International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 12-02-2024, Accepted: 08-03-2024, Published: 30-03-2024
Volume 10, Issue 2, 2024, Page No. 92-97

The rise of cyberwarfare: The applicability of international humanitarian law for the protection of civilians and civilian objects

Chukwudumebi O Joseph-Asoh[1], Nkechinyere Worluh-Okolie[1], Jojo Ebibode[2]
[1] Lecturer, Faculty of Law, Benson Idahosa University, benin City, Edo State, Nigeria
[2] Research Assisstant, Faculty of Law, benson Idahosa University, Benin City, Edo State, Nigeria

Abstract
This Article examines the nature of Cyber warfare in relation to the existing rules of IHL on the protection of civilians in armed conflicts, their applicability or otherwise to cyber warfare, the existing gap in the law, with a view to making recommendations on more effective ways to protect civilians and civilian objects. In doing this, the research methodology adopted is the doctrinal approach. Both primary and secondary sources of information were consulted and utilized in the course of this work. The primary sources include the third Geneva Convention and their Additional Protocol I, the UN Charter etc. The secondary sources include textbooks, journals, articles, newspaper, and online material retrieved from the ICRC website and other relevant websites. This paper finds that although International Humanitarian Law provides for rules aimed at the protection of civilians and civilian objects in armed conflicts, these rules do not sufficiently afford protection to civilians in Cyber warfare as the complexity brought about by these new means and methods of warfare were not captured at the time the rules were made. This work identifies some of the challenges posed to the protection of civilians in cyber warfare and therefore recommends that it is essential to recognize the distinct nature of the cyberspace and establish a legal framework that comprehensively discusses its complexities. The work concludes that a specific legislation that comprehensively addresses its intricacies of cyber warfare is a step in the right direction to protecting civilians and civilian objects.

Keywords: Cyber warfare, international humanitarian law, civilians, armed conflict

Introduction

This Article examines the expansive nature of cyber warfare and the legal protection that International Humanitarian Law can provide to civilians and civilian objects, as well as its limitations in an era when the use of cyber technologies in situations of armed conflict are so prevalent. Warfare is widely defined as the use of military force to achieve political, economic, or territorial objectives [1]. The elements that typically characterize warfare include; the use of force, political objectives, organized conflict, governmental authorization & significant impact.

Cyber warfare refers to the use of digital technologies such as computers and networks, to conduct military operations. Examples of cyber warfare include the use of malware to disable an adversary's computer systems or the use of denial-of-service attacks to disrupt communication networks. The use of cyber warfare as a military strategy has become increasingly common. In armed conflicts in recent years, several states have publicly acknowledged the use of cyber operations alongside kinetic operations. It has been estimated that 140 nations are in the process of developing the capacity to wage cyber warfare [2].

The assertion that cyber warfare is actually warfare has been a point of contention for many scholars. However, the International Committee of the Red Cross (ICRC) in a 2016 report [3] noted that "cyber-attacks may constitute a means or method of warfare" and that "the principles of International Humanitarian Law apply to cyber operations during armed conflict". Additionally, prominent scholars have also posited that cyber warfare is a form of warfare. Mary Kaldor [4], a prominent scholar has argued that cyber warfare should be considered "a new form of war" which involves "networked actors who use violence to achieve their political aims". Likewise, Michael Schmitt [5], an expert in the field of international law and armed conflict has argued that the use of cyber-attacks that cause significant harm could be considered a violation of the principles of proportionality and distinction under international law. Thus, while cyber warfare differs from conventional warfare as a result of its nature, it is generally recognized as a form of warfare by both legal and academic authorities because it involves the use of force to achieve military objectives and has significant impact. As a result, the international legal frameworks that regulate warfare also apply to cyber warfare.

Originally, International Humanitarian Law in its development considered land, sea and air as the domains of warfare, however, due to the advent of the cyberspace, a new domain of warfare has come into existence. This leaves room for legal questions regarding its nature and regulation. The development of IHL in the pre-digital age means that its regulations were not formed with the vision of cyber operations. This makes it difficult to determine how its provisions apply to cyber warfare.

For purposes of this analysis, the paper is structured in parts. Part one will examine the nature of cyber attack, part two provides an analysis of International Humanitarian Law on protection of Civilians and civilian objects especially the principles of International Humanitarian Law to cyber warfare and part three reveals the challenges of applying IHL principles to cyber warfare. The paper concludes by providing recommendations for regulating war in the cyberspace.

Can a cyber-attack be regarded as armed attack?

In order to apply the principles of IHL to protect civilian lives in a situation of cyber conflict, it is to be first determined whether cyber-attacks fall under the threshold

for armed force. Article 2 common to all Geneva conventions provides that;

"The present Convention shall apply to all cases of declared war or of any other armed conflict *which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."*

The definition for "attack" is provided for in Article 49(1) of API, which defines it as "acts of violence against the adversary, whether in offence or in defence [6]." Violence, in this sense, is denoted to mean physical violence [7]. In addition, the ICRC is of the view that the term "attack" means "combat action," which denotes a physical act. On the basis of this understanding, the Tallinn Manual 2.0 proposes the following definition: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" [8]

Following an examination of the UN charter state practice and interpretation of the text over time, It can be concluded that the proper test of when a cyber-attack can be considered an armed attack is when the attack results in physical destruction comparable to a conventional attack. However, some experts hold that a cyber attack amounts to an attack if it is expected to interfere with the functionality and if restoration of functionality requires replacement of physical materials and the reinstallation of the operating system or of particular data [9].

Analysis of International Humanitarian Law Rules For the Protection of Civilians and Civilian Objects in Armed Conflicts.

1. Protection of the Civilian Population in Cyber warfare

Protection of civilians is an essential objective of IHL. The civilian population and individual civilians "enjoy general protection against dangers arising from military operations" [10]. According to Additional Protocol I, where a person is in the power of a Party to the conflict and who do not benefit from more favorable treatment under the conventions or under the protocol shall be treated humanely in all circumstances and shall enjoy, as a minimum, the protection. provided by this article without any discrimination [11]. Additionally, the law provides that protected persons are entitled in all circumstances to protection of their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs [12]. The IHL principles on distinction, proportionality and precautions are fundamental to the protection of civilians during hostilities.

2. Protection of objects indispensable to the survival of the civilian population

IHL aims to protect the civilian population during armed conflicts by ensuring that their survival is not compromised. As such, it prohibits the use of starvation as a method of warfare [13]. Parties involved in a conflict are prohibited from attacking, destroying, removing or rendering essential objects necessary for civilian survival, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse party, whatever the motive [14], whether in order to starve out civilians, to cause them to move away, or for any other motive. However, there is an exception if these objects are used solely by the opposing party's armed forces or for direct military support. In such cases, actions against these objects are permissible but only if they do not leave the civilian population with inadequate food or water that would result in starvation or forced displacement [15]. It is also important to know that these objects should not be targeted as a form of reprisal [16].

Civilian hospitals organized to give care to the wounded and sick, the infirm and maternity cases are not to be the object of attack, but must at all times be respected and protected by the Parties to the conflict [17]. Hospitals are to be located as far as possible from military objectives. The protection is extended to the members of staff of the hospital. Additionally, Convoys of vehicles or hospital trains on land or specially provided vessels on sea, conveying wounded and sick civilians, the infirm and maternity cases, shall be respected and protected [18]. Also, aircraft exclusively employed for the removal of wounded and sick civilians, the infirm and maternity cases, or for the transport of medical personnel and equipment, shall not be attacked, but shall be respected while flying at heights, times and on routes specifically agreed upon between all the Parties to the conflict [19] concerned. Parties to the conflict are also required to allow the free passage of all consignments of medical and hospital stores and objects necessary for religious worship intended only for civilians. They shall likewise permit the free passage of all consignments of essential foodstuffs, clothing and tonics intended for children under fifteen, expectant mothers and maternity cases.

The implication of the aforementioned provisions is that in cyber warfare, the protection of objects indispensable to the survival of the civilian population is of utmost importance. These objects can include critical infrastructure systems such as healthcare facilities, water supply facilities, healthcare facilities and transportation systems.

3. Protection of works and installations containing dangerous forces

Attacks on works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations are prohibited by IHL, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population [20].

However, the special protection against attack stated above ceases: for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support [21] of military operations and if such attack is the only feasible way to terminate such support; [22] for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations [23] and if such attack is the only feasible way to terminate such support; for other military objectives located at or in the vicinity of these works or installations only if they are used in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support. Where the protection ceases and any of the works, installations or military objectives is attacked, civilians remain entitled to all the protection accorded them and all practical precautions shall be taken to avoid the release of the dangerous forces. Attacks by way of reprisals on works, installations or military objectives are prohibited.

The cyber space enables attackers to infiltrate into the control systems of critical infrastructures like dams, dykes and other installations. For instance, in 1998, Arizona's Roosevelt Dam, gaining control 1.5 million acre-feet of water was broken into. Federal authorities said the attacker had total command of the Supervisory Control and Data Acquisition Systems (SCADA) that controlled the dam's massive floodgates [24]. This particular instance may serve as an indication of the danger that civilians are in in their physical environment as a result of actions which are carried out in the cyberspace. If the principles and regulations of IHL are not adhered to in cyber warfare, civilian lives would be put in further harm.

4. The Protection of Data as a Civilian Object

The protection of civilian data as a civilian object has been subject to significant debate. It is however becoming increasingly important because data is a cornerstone of everyday life in any modern society. Data such as; social security data, tax records, medical data and bank accounts are necessary for the functioning of a large percentage of civilian life [25].

In some aspects, IHL covers certain categories of data as civilian data which enjoys protection. For example, the need to protect medical facilities and humanitarian operations can be extended to the data belonging to these facilities and operations. Similarly, tampering with data in manner that renders objects, which are indispensable to the survival of the human population (such as water installations and irrigation systems) useless is prohibited by IHL [26]

5. The Principles of International Humanitarian Law in Application

IHL is a set of rules that aim to limit the effects of armed conflict and protect individuals who are not taking part in hostilities. While IHL was originally developed with traditional warfare, although with a significant difference in its specific application, the principles of IHL can be applied to cyber warfare in the absence of a specific legal framework.

a. The Principle of Distinction

The principle of distinction is set out in Article 48 of API, which provides: "The Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives" [27]

Similarly, in its *Nuclear Weapons Advisory Opinion* [28] the ICJ held that the principle of distinction is the "cardinal principle contained in the texts constituting the fabric of humanitarian law." A literal interpretation of Article 48 would mean that, attacks may only be directed against military objectives. To translate this to the cyberspace, attacks which are directed at civilian cyber infrastructures would amount to a breach of Article 48. Conversely, a "lawful" cyber-attack is one which only attacks military cyber infrastructures which would confer a "definite military advantage [29]."As a result of the dual-use nature of the cyberspace, the distinction between civilian and military cyber infrastructure is not as pronounced, this makes the determination of legal targets difficult. The principle of distinction, which requires states to distinguish civilian and military personnel and restrict attacks to military objectives [30], obliges parties to cyber conflict to restrain from acts that would result in excessive collateral damage. In this sense, military commanders must use weapons that can target accurately and must use this capability to distinguish between civilian and military objectives [31]. By extension, IHL prohibits cyber-attacks that are uncontrollable, unpredictable, or do not discriminate between civilian and military objectives. Furthermore, Additional Protocol I prohibits attacks that deny the civilian population indispensable objects, such as food or water supplies [32].

There are situations where the principle of distinction is easily applied to cyber-attacks. For example, a cyber-attack that targets a military air traffic control system and only causes a troop transport to crash would comply with the principle of distinction. Other cyber-attacks would clearly violate the principle of distinction, for example, an attack on the civilian banking sector or on hospitals, museums, or places of worship. Cyber-attacks against the networks that manage these targets, like any other attack on these objects, would be unlawful.

Admittedly, application of the principle of distinction in the cyberspace will prove to be complicated because it is highly probable that the targets are used by both military and civilian actors at once. Because much of cyberspace is dual use, used by both the military and civilians, upholding the distinction requirement in cyberspace can be more challenging than it is in a conventional context. This therefore brings about the question of who may be lawfully targeted in a cyber-attack as opposed to those who are to be protected from cyber-attacks. It is important to such time as, they directly participate in hostilities. Article 58 of API provides the need to segregate "civilian objects from the vicinity of military objectives." The same can be said for cyber infrastructures. All States shall endeavor to segregate military cyber infrastructures from civilian cyber infrastructures. This approach is the best way to distinguish between civilian and military cyber objects.

b. The Principle of Proportionality

Due to the fact that civilian deaths and or destruction to civilian objects are unavoidable in wartime, the principle of proportionality is one of the most disputed principles of IHL. While the application of the proportionality principle is easier when it comes to traditional kinetic warfare [33] the same cannot be said for cyber operations. Given the dual-use nature of most cyber infrastructures, the principle of proportionality is essential in protecting civilians and civilian objects in the cyber domain. The proportionality principle is found in Article 51(5)(b) of API, which also reflects customary international law applicable in both International Armed Conflicts (IAC) and Non International Armed Conflicts (NIAC). Under Article 51(5)(b), an attack is prohibited if it "may be expected to cause incidental loss of civilian life, injury to civilians, *damage to civilian objects*, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

There has been universal acceptance that the proportionality principle applies to cyber conflicts that constitute attacks [34], but *how* it is to be applied remains subject to controversy For cyber operations that utilize the proportionality principle, two major elements of the principle deserve a more nuanced understanding and

approach: the "damage to civilian objects" threshold in Article 51(5)(b); and the issue of indirect effects.

Due to the nature of harm they inflict, the proportionality of cyber-attacks poses unique challenges. It can be difficult to evaluate whether an attack would be proportional according to the relevant categories of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," as the typical direct effects of cyber-attacks may be nonlethal or temporary, yet severe. In particular, how should the temporary incapacity of critical systems be evaluated? A cyber-attack that effectively stops the transmission of information through the Internet might merely inconvenience the populace, but it might also have more severe consequences. For example, it might cause hospitals to be unable to communicate vital information, leading to loss of life. Thus, cyber-attacks may change the weight given to temporary consequences, and may force states to confront more uncertainty than they typically face in making decisions about the legality of planned attacks. Nevertheless, Military Commanders must distinguish between legitimate military targets and civilian objects including the civilian population.

c. The Principle of Precaution

The principle of Precaution is a principle within the framework of jus in bello that requires parties involved in cyber warfare to take measures to minimize harm to civilians and civilian infrastructure. This principle aims to reduce the potential humanitarian impact of military operations. In the context of cyber warfare the principle of precaution can be adhered to by carrying out thorough risk assessment, taking into consideration, potential risks and consequences of their cyber-attacks. This includes evaluating the likelihood of collateral damage to civilian infrastructure, disruption of essential services and harm to non-combatants. The principle of proportionality also requires parties to weigh the anticipated military advantage in their response to an attack by an adversary, against the potential harm to civilians and civilian infrastructure. That is, the expected benefits of a cyber-operation must justify any potential collateral damage.

4. Issues and Challenges in the Application of International Humanitarian Law During Cyber Warfare

In regard to the new type of warfare, in particular its more and more developed forms and rising popularity, the international community, or at least some of its members, along with international law experts begun to look for options how to include cyber warfare into the Laws of War.

As a result, and possibly also the easiest solution, the current mainstream opinion on the legal rules applicable to cyber warfare is that the currently valid Laws of War, especially the IHL Conventions, apply to cyber warfare and cyber weapons accordingly.

Notwithstanding the lack of any agreement amongst the international community on such approach, let alone the lack of existence of any official document that would set rules which authority or according to which parameters the IHL Conventions should be interpreted when applied on cyber warfare, some interpretation efforts have already started on regional levels and amongst legal scholars.

a. Interconnectivity and Dual Use Nature of the Cyberspace

The cyber space is of a dual use nature and the implication of this is that both civilian and military objects are interconnected. This poses as a challenge in the application of the principle of distinction. Distinction is applicable to the cyberspace where the only target permissible are computer systems that are making an effective contribution to military operations. A cyber-attack would violate the principle of distinction if aimed directly at a computer system serving exclusively civilian purposes. Civilian computers are more than often using the same software, code or type of data, hence making them vulnerable to the same cyber-attack but civilian computer networks usually possess less capabilities for counter measures, they are therefore weaker and more easily targetable. With the risk for collateral damages in the cyberspace being as high as in the physical space, it appears essential to inquire how distinction operates in cyber warfare. The key issue here is the inherent "interconnectivity" of the cyberspace [35] In fact, it is not the whole range of different computer systems what we should define as the "cyberspace" but the interconnection between them which makes it a global network. The interconnectedness of civilian and military in cyber-space poses a challenge to the protection of civilians and civilian objects in cyber-space. IHL allows attacks to be made on combatants and military objectives and prohibits attacks on civilians and civilian objects. Compliance with this in cyber warfare is difficult as military and civilian infrastructures in cyber-space are interwoven. Military infrastructures are military objectives and therefore legitimate objects of attack. Since most military networks rely on civilian cyber infrastructure, and it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures, attacks on such military networks will occasion incidental damage on the civilian infrastructure.

The position in IHL is that when a particular object is used for both civilian and military purposes, it becomes a military objective, except for the separable parts thereof, and therefore a legitimate object of attack. Applying this strictly to cyber warfare could lead to the conclusion that many objects forming part of the cyber-space infrastructure would constitute military objectives and would not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ensuing impact that such a loss of protection could have in terms of disruption of the ever-increasing concomitant civilian usage of the cyberspace. IHL even permits a certain level of collateral damage on civilians and civilian objects provided that such damage is not in excess of the actual military advantage gained from the attack. The military advantage has to be assessed and measured against the incidental harm to civilians. The protection of civilians in this situation hangs on the result of the assessment. In cyber-warfare, a proper assessment will first entail knowing enough about the connection between the sending computer and the targeted computer to be sufficiently assured that the attack will in fact engage the intended target [36]. The operator will also need to know enough about the characteristics of the particular cyber capability that is being used to undertake the attack to be assured that it will engage the target in the intended way. Secondly, he will need to know enough about

the targeted computer system, its dependencies, and associated networks to be able to assess the proportionality of the planned attack. Finally, if the cyber capability to be used in the attack is liable to affect other networks as it travels to the targeted system, the expected effects on those other networks will need to be assessed as, to the extent that those networks do not themselves consist of military objectives. Damage to them, and consequential damage or injury to their users will have to be factored into the proportionality assessment that is made in advance of the decision to mount the cyber-attack [37]. This assessment is particularly difficult because civilian and military networks are so critically interconnected that incidental civilian harm must be expected in most cases, and it is almost impossible to foresee all possible harm including incidental harm indirectly caused by the reverberating effects of the attack. It is difficult to limit the effects of attacks, as required by IHL. A lot will depend on the particular cyber tool that is planned to use, on the characteristics of that tool, on whether the damaging effect of the cyber tool can be reasonably limited to the intended target of attack, and on whether enough is known about the target computer system to enable proper precautionary judgments of the sort discussed above to be made. AP I requires that *'in the study, development, acquisition or adoption of a new weapon, means or method ofwarfare, a High Contracting Party is under an obligation todetermine whether its employment would, in some or allcircumstances, be prohibited by [API] or by any other rule ofinternational law applicable to the High ContractingParty'*. [38] In line with this provision, a review of cyber capabilities that are to be used to cause death, injury, damage or destruction to an opposing party to a conflict is required.

b. Attribution and Anonymity of Actors

In cyber warfare, anonymity becomes a different notion than during kinetic attacks. The issue of anonymity of cyber-attacks is in fact closely linked to the impossibility to trace down the original source of such an attack, since it is usually located in an absolutely different location than the one of its targets.

Even in the instance, where the location is discovered, attribution is still an issue because the identity of the attacker is hard to unveil. For instance, the series of Denial-of-Service attacks on Estonia in 2007 constitutes an exemplary situation when a state entity, the Russian Federation, denied its responsibility for the attacks and blamed it on a group of independent individuals. [39]

Attribution is a very cogent factor in the enforcement of IHL. To attribute responsibility in IHL, the source of the attack must be identified. Cyber-warfare raises a number of issues with regards to attribution of responsibility. The identification of attackers is difficult as many cyber-operators are located far from the armed conflict and a cyber-attack can be carried out from any part of the world. The remoteness of the cyber operator from the consequences of his or her activity makes it difficult to determine; first, who undertook the cyber-operation in question. Second, on behalf of which state or organization, if any, the operation was undertaken and, third, its purpose. In the absence of information on the cyber-operator, it is difficult to attribute responsibility or even establish that the attack was carried out in furtherance of an armed conflict.

Recommendations

In view of the above challenges associated with cyber warfare, This Article provides the following recommendations;

1. To ensure the protection of civilians from the consequences of cyber-attacks, it is essential to recognize the distinct nature of the cyber domain and establish a legal framework that comprehensively discusses its complexities. By doing so, the shortcomings of the current regime will be overcome. The development of a comprehensive and internationally recognized legal framework, which specifically addresses cyberwarfare and its impact on civilians and civilian objects.
2. Education and training initiatives to raise awareness, not only in the field of cybersecurity but also in the field of International Humanitarian Law. This education and awareness creation ought to involve relevant stakeholders, including governments, military personnel and even members of the private sector. This is to ensure a better understanding of the better understanding of the legal and technical aspects of cyber conflicts.
3. The strengthening of international institutions and organizations such as the United Nations and its specialized agencies in order to enhance their capacity to address cyber threats and enforce International Humanitarian Law in the cyberspace.
4. The recognition of the role of private sector entities in critical infrastructure and digital services and encourage public-private partnerships to develop guidelines and standards for protecting civilian infrastructure and facilitating the sharing of threat intelligence.
5. Continuous research and analysis by academic institutions and research organizations in order to keep pace with evolving landscape of cyberwarfare and propose updates or amendments to legal frameworks as new challenges arise.

Conclusion

In conclusion, the rise of cyberwarfare has presented significant challenges regarding the applicability of international humanitarian law for the protection of civilians. Not only do cyber-attacks represent a fundamentally different method of warfare, they come at a time when the laws of armed conflict are struggling to meet the challenges of greater than ever civilian participation in conflict, increased asymmetry and technological advance. The general rules and principles of IHL were not originally designed to address the unique characteristics and complexities of cyberwarfare. A pressing concern which this project has brought to the fore is the absence of provisions in IHL to protect data and information in the cyberspace. Similarly, the interconnectivity of the cyber space and the potential of cyber attacks to cause significant harm to civilians in critical infrastructure and demand an urgent response.

To safeguard civilians in the face of cyber threats, it is essential to recognize the cyber space as distinct and develop specific legislation that comprehensively addresses its intricacies. This legislation should extend the protection provided to physical civilian data to include data, information and critical cyber infrastructure. Furthermore, a thorough legal review of cyber weapons, means and methods of cyberwarfare should be conducted to ensure compliance with IHL.

References

1. Kaldor M. *New and Old Wars: Organized Violence in a Global Era.* (Stanford: Stanford University Press, 1999.)
2. Kevin C. The Cyber Arms Race Has Begun https://www.csoonline.com/article/2122353/coleman--the-cyber-arms-race-has-begun.html [Accessed 20/11/2022]
3. Kevin C. The Cyber Arms Race Has Begun https://www.csoonline.com/article/2122353/coleman--the-cyber-arms-race-has-begun.html [Accessed 20/11/2022]
4. International Committee of the Red Cross. "The Roots of Behaviour in War 3: Cyber Operations and International Law." in https://www.icrc.org/en/doc/assets/files/other/icrc-002-4603.pdf [Accessed 01/04/2023]
5. Kaldor M. In Defence of New Wars." International Journal of Security and Development,2013:2(1):1-16.
6. Schmitt MN. yber warfare and the concept of jus ad bellum." *NATO Legal Gazette*,2012:34:1-17.
7. Commentary On The Fourth Geneva Convention Relative To The Protection Of Civilian Persons In Time Of War 59 (Jean S Pictet ed., 1958).
8. Schmitt MN. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2013)
9. Gisel L, *et al*. 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*,2020:102(913):287-334
10. Article 51(1) of AP I.
11. Article 75 of AP I
12. Article 27 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War (herein after GC IV)
13. AP I Article 54(1)
14. Article 54(2) of AP I
15. Article 54(3)(a) and (b) of AP I
16. Article 54(4) of AP I
17. rticle 18 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War (herein after GC IV)
18. Article 21 of GC IV
19. Article 56(1) of AP I
20. Article 56(2)(a) of AP I
21. Article 56(2)(b) of AP I
22. Article 56(2)(c) of AP I
23. Gellman, B., "Cyber-attacks by Al Qaeda feared. Washington Post" in https://www.washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/ [Accessed 20/10/2022]
24. Gisel. L., *et al*., "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* (2020) Vol. 102, No. 913 pp. 287-334
25. Article 54 of AP I
26. Article 48 of AP I
27. Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 256 (July 8).
28. Chang Z. Cyberwarfare and International Humanitarian Law", *Creighton International and Comparative Law Journal*,2017: 9:1.
29. Louise Doswald-Beck, "Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*", Computer Network Attack And International Law*,2002:76:163-185.
30. Hathaway AO, Crootof C, *et al*. The Law of Cyber-Attack", *California Law Review*,2012:100:817-886.
31. Article 54(2) of AP I
32. Eric T. Jensen, "Cyber Attacks: Proportionality and Precautions in Attack"*International Law Studies*,2013:89(198):205-206
33. Tsagourias N, Russell B. Research Handbook on International Law and Cyberspace"(Cheltenham: Edward Elgar Publishing, 2015, 130.
34. Boothby W. Some Legal Challenges posed by Remote Attack *International Review of the Red Cross*,2012:94:886-587
35. AP I Article 36
36. Richards J. Denial-of-Service The Estonian Cyberwar and Its Implications for U.S. National Security, International Affairs Review", *The Elliot School of International Affairs at George Washington University*, 2009, 18(1).