The Impact of Cyber Warfare on International Humanitarian Law

Mr Tirtha Dutta Biswas*

Mrs.Vidya Nair**

Contents

* Research Scholar at Maharashtra National Law University Mumbai.
** Research Scholar at Symbiosis International (Deemed University).

1. Introduction

Cyber warfare refers to the practice of conducting warfare in cyberspace through cyber means. Whereas the term warfare is mostly used to understand as a reference to conducting military hostilities during the armed conflict.[1] Cyberspace, which is an interconnected global digital information and communication source that includes telecommunication networks, the internet, computer systems, etc, plays an important role in cyber warfare.[2] Therefore, if we consider an example that is an act of infecting the computer network of a belligerent,[3] it will amount to an act of cyber warfare, but an act of aerial bombardment by a military group using the cyber command will not amount to cyber warfare.[4]

An act of cyber warfare usually takes place in cyberspace, but that doesn't mean cyber warfare cannot create a kinetic effect outside the domain of cyberspace. Cyberwar attackers can be aimed directly at a person whose object and functionality of existence depend fully on the computer system, including military, medical and life support systems.

2. Objectives of the study

The research paper will determine -

a) Under what circumstances, if any, a cyber operation has taken place, it can amount to a wrongful threat under the international law regime

b) To what extent is an armed attack in proportionate forces necessary and justified in self-defence

c) Breach of peace or a significant threat to international peace and security, subject to resolution by the United Nations Security Council

d)Under the laws related to neutrality, to what extent can the belligerents make the lawful use of the telecom infrastructure of neutral states in case a cyber-attack happens, and what are the specific responsibilities of the neutral states against the non-state belligerents conducting an attack on their territory

[1] On The Notion Of "Armed Conflict" See Section V.1.
[2] U.S. Joint Chiefs Of Staff, Department Of Defence Dictionary Of Military And Associated Terms 41 (U.S. Govt 2001)
[3] Eastwest Institute, The Russia–US Bilateral On Cybersecurity—Critical Terminology Foundations 11 (Moscow State University 2011)
[4] Armin Bogdany And Rüdiger Wolfrum (Eds), Max Planck Yearbook Of United Nations Law 96 (Vol. 14 Mpil 2010)

e)An approach to distinguish the law of armed conflict and cyber warfare is going to be taken in this paper, including the scope of cyber criminality and cyber terrorism, which may fall outside the purview of International Humanitarian Law in certain situations.

3. Scope of the study

The areas in which international humanitarian law applies will be clarified to what extent the rules and principles of International Humanitarian Law are applicable, which is designed to govern the methods of warfare by traditional means and how it can be switched to cyber warfare. The focus here is primarily on the fundamental rule that regulates state conduct and the principles that define hostile action by the states, rather than on the laws concerning the treatment and protection of individuals during armed conflict. It is important to note that, to date, there has been no definitive application or interpretation of existing international legal principles specifically related to cyber warfare. Furthermore, the technological and military aspects of cyber operations have yet to be fully explored. Being stringent about the sapplication of cyber warfare law is not an economically productive approach, even though such warfare may not take place outside of the scope of law. Important international organisations, such as NATO, have taken significant steps to define the legal frameworks related to international laws and cyber warfare. For example, the Manual on the International Law of Cyber Warfare is significant with regard to such efforts.

4. The Unique Cyberspace

In the area of cyber warfare, the implementation and understanding of current international law is very important. Cyberspace is the only environment completely generated by man. Public and private mutual stakeholders across the globe sustain, create, own and run it, and it continues to evolve over time as a result of technical progress. Since cyberspace has no natural or geopolitical boundaries, electronic payloads and information are frequently deployed Cyberspace is also readily available to the government for access including the non-state organizations and individuals and as a result it makes easy to trace the origin of operational activities thus making it an attribution and identification of activities related to cyberspace very

difficult.[5] All these elements of cyberspace make it a unique entity, and therefore, it requires special attention.

5. Cyber Operations, Attacks, Exploitation and Defence

Cyber operation, popularly known as Computer Network Operation (CNO), is considered a broad term. It has applications in the civilian and military arenas. It is a reduction of information in terms of electronic format, and it includes the actual movement of such information related to cyber infrastructural elements.[6] Computer network attacks (CNA), on the other hand, comprise a specific category of cyber operations aiming to deny, disrupt, destroy and degrade the information that is present in a computer.[7]

Computer Network Exploitation (CNE) refers to the reconnaissance and espionage operation. The purpose of such kind of operation is to steal data from a particular system, or more specifically, to understand the configuration and operational activity of a computer, whereas CND or Computer network defence is nothing but a form of cybersecurity which is utilised for securing the systems of Military and Government organisations. It includes protection, monitoring, analysis and detection of unauthorised activity within the network and the system. Computer network defence helps to prevent Computer network attacks and Computer Network Exploitation by means of law enforcement, counterintelligence and military activities.

6. Cyber Operations and Jus Ad Bellum

In general, the term Jus Ad Bellum refers to the circumstances or situations under which a state may have a tendency to resort to war or is obliged to use military force. The most major element of Jus Ad Bellum is the Charter of the United Nations, although it is important to remember that some legal elements, especially the modalities regulated by the use of force at the time of self-defence, are not protected by the UN Charter. The derivation of these modalities is mainly based on the customary laws that can be found in state practices that are predominantly characterised as opinio juris.To understand whether cyber operations constitute the right to go to war, it must be considered if the following conditions had also taken place –

1. An unlawful use of force
2. A form of justifiable armed assault, such as that for self-defence

[5] U.S. Department Of Defence, The National Military Strategy For Cyberspace Operations 3-4 (U.S. Gov 2006)
[6] NATO, Tallinn Manual (CCDOE 2017)
[7] U.S. Department Of Defense, The National Military Strategy For Cyberspace Operations Gl-1 (Us Gov 2006)

3. A breach of the peace of a state to the extent that intervention from the UN Security Council becomes necessary.

The first condition holds great importance. State-funded cyber operations that also fulfil the first condition are considered to be the cause of international war. The general prohibitions in the Charter of the United Nations are not applicable here.[8]

While cyber operations that fulfil the first condition are not allowed as per the non-intervention framework of customary international law, they can be considered as legally valid countermeasures. This occurs when the cyber operations take place as a response to an internationally unlawful activity. [9] This is allowed because each state has an intrinsic right to defend itself, including through the use of force. With regard to the third condition, the threats to peace and aggression against the state would allow the UN Security Council to interfere between the involved parties forcefully for the purpose of preserving global peace. This happens when the UN Charter's articles 2(4) and 51 are not complied to by the involved parties.

7. Restrictions on Interstate Force with Regard to Cyber Operations

Under Article 2(4) of the UN Charter, all the member states of the UN are forbidden from making the use of force and similar actions against any other state.[10] In accordance with this, it should be considered whether cyberspace operations can also fall within the scope of the article and within the framework of "use of force".[11] The ordinary meaning of "force" is a broad term, and the question of whether any non-coercive action can amount to force or not must be dealt with strictly.[12] Many observers and legal theorists in the present International Law System interpret "force" to be synonymous with military force or armed war, although this does not mean that the use of chemical, biochemical, kinetic or nuclear weapons is limited to the prohibition of force. [13]

There is a restriction on the use of any power, according to many International Court of Justice rulings. Whether or not the power was produced by the means of an arm or not is immaterial.

---

[8] United Nations Charter, June 26, 1945, U.N. Doc. A/5/1 Art. 2(4)
[9] Georg Ress, The Interpretation Of The Charter 18 (Bruno Simma (Ed.), The Charter Of The United Nations: A Commentary, Vol. I, 2002)
[10] Vienna Convention On The Law Of Treaties, 1969 Art. 31(1)
[11] Marco Roscini, Cyber Operations And The Use Of Force In International Law 17 (Oxford University Press 2014).
[12] Ian Brownlie, International Law And The Use Of Force By States 362 (OUP 1963)
[13] Yoram Dinstein, War, Aggression And Self-Defence 80 (4th Ed. Cambridge University Press 2005)

[14] Therefore, the inclusion of cyber operations should not be disputed in some direction whether such activity has been used as an offensive or as a defensive weapon intended to inflict harm or death to individuals or whether it leads to destruction of facilities and artefacts irrespective of the extent of such devastation including technical harm, physical damage or a mixture of both.[15]

Any of the cyber-operations falling under the meaning of force referred to in Article 2(4) of the United Nations Charter involve the exploitation of computer networks intentionally intended for the meltdown of a nuclear power plant or the opening of dam floodgates located over a densely populated area by controlling the system of air traffic control.[16] However, the real difficulty arises regarding the activity which do not cause injury, death or destruction can be placed under Art. 2(4) as use of "force" or not.[17]

With respect to the definition of a use of force, the real challenge appears. Cyber activities that do not cause death, damage or devastation, or do not explicitly cause them. [18] Article 41 of the Charter of the United Nations applies to the "interruption of... communication" as a measure which does not require armed conflict, indicating that such denial-of-service assault operations will not be subject to Art 2 (4). [19] However, it doesn't mean that due to the absence of a violating effect, all cyber operations are excluded from the purview of armed conflict.

8. The "Interstate" Dimension of Cyber Operations

Article 2(4) of the Charter of the United Nations refers only to states. Under this dimension, such a threatening force is used by one state towards another.[20] When individuals also act through the approval of a state, their actions are equivalent to the state's actions to which the individual belongs. To this extent, Article 2(4) is also not applicable to individual entities that are acting without the authorisation of their specific state, and such entities would be considered

[14] Ibid 81
[15] Ian Brownlie, International Law And The Use Of Force By States 362 (OUP 1963)
[16] Albrecht Randelzhofer, The Charter Of The United Nations: A Commentary 117 (Vol. I, Oxford 2002)
[17] International Court Of Justice, Corfu Channel (United Kingdom Of Great Britain And Northern Ireland Albania) (Merits), Separate Opinion By Judge Alvarez 47 (Icj 1949)
[18] Alfred Verdross And Bruno Simma, Universelles Völkerrecht: Theorie Und Praxis 469,476 (Duncker Und Humblot 1984)
[19] Marco Roscini, World Wide Warfare—Jus Ad Bellum And The Use Of Cyber Force 105 Ff (Armin Bogdany And Rüdiger Wolfrum (Eds), Max Planck Yearbook Of United Nations Law, Vol. 14, 2010)
[20] Yoram Dinstein, War, Aggression And Self-Defence 175ff (4th Ed., Cambridge University Press 2005)

non-state actors. The authorities within the state that handle such individual actions would be considered with regard to the international law principle of state liability. [21]

This area has been comprehensively reaffirmed by the International Law Commission in Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001) by the International Law Commission and it can be expected that the individual liability of the non-state actors will soon be under scrutiny. However, at present, the individual hackers engaging in the use of force, including the cyber operations, cannot escape as they are being prosecuted under the International Criminal Law and International Humanitarian Law, but to date, they are being exempted from being a subject under Art. 2(4)

9. Negative Effects of Cyber Attacks on "Critical Infrastructures"

Critical infrastructures can be understood on the basis of the interpretation of the term "scale and effects". When there is no direct impact in the form of physical injuries and death, the reference would be to the "critical infrastructures" of the state.[22] The protection of these critical infrastructures by means of cybersecurity has been the key concern for the states from time to time. The following examples explain that certain consistencies must have to be provided for the proper functioning of these mechanisms.[23]

UN General Assembly: The UN General Assembly has defined the types of infrastructure that fall within the category of critical infrastructures. These include services related to food and water distribution, services related to maritime transportation, e-commerce activities, finance and banking, public health services, IT infrastructures, and services related to energy transmission.[24]

United States: Here, the meaning of critical infrastructure is inclusive of any cyber operations that are necessary for the economic activities of the U.S. This refers to activities related to banking, finance, energy, and telecommunication operations. [25] Critical infrastructure can also be virtual assets that would deliberately impact national security, public health or safety.[26]

---

[21] D.W. Bowett, Self-Defence in International Law 12 (Brill 1958)
[22] Marco Roscini, World Wide Warfare—Jus Ad Bellum And The Use Of Cyber Force 96 (In Armin Bogdany And Rüdiger Wolfrum (Eds) Max Planck Yearbook Of United Nations Law Vol. 14 2010)
[23] Loyola Of Los Angeles International And Comparative Law Review Vol. 32 306 (Loyola Marymount University 2010)
[24] UN General Assembly Resolution 58/199, 30 January 2004.
[25] Critical Infrastructure Protection (Us Presidential Directive) – 63,1998, [§ I. 55]
[26] Us Patriot Act, 42 U.S.C. 5195c (E), § 1016(E) (2001).

European Union: In the EU, this refers to those infrastructures that, if destroyed, would affect the health and security of the citizens of the EU. However, as per the UN General Assembly, it should be on the basis of the discretion of a state that the meaning of critical infrastructures for the state should be considered, though such considerations must include national security.[27]

10. Cyber Operations and UN Security Council Enforcement

In preserving international stability and stability, the UN Security Council plays a significant role. There should be no question that the responsibility of the United Nations Security Council indeed applies to the preservation of stability and security in cyberspace, since cyber operations mostly impact foreign state relations. The UN Security Council may make suggestions whether there is a violation of peace or a danger to peace, call for the parties involved to cooperate with the provisional steps and may also call for action, which may be armed or unarmed compliance. UN Charter specifies certain unarmed enforcement measures, including the partial or complete interruption of radio, telegraphic and other means of communication, thereby creating a cyber blockade as per the provisions of the UN Charter.[28]

Art 42 of the UN Charter, on the other hand, empowers the UN Security Council to provide a basis of action by means of armed enforcement by sea, air or land forces. However, irrespective of the threat to peace, it does not provide full discretion to the Council for evaluating the impact of single cyber operational activities. The Council is expected to take action in compliance with the principles of the Charter of the United Nations and, most specifically, in accordance with the principles of international law and justice. For this reason, it is important that the Security Council follow the practice of permitting compliance action that allows the use of military force to tackle cyber threats. However, such force should be under the levels of the criteria that determine self-defensive action. The discretion of the Security Council is not entirely unrestricted when deciding if a single cyber activity poses a threat to security. At a minimum, the Council is obliged to act in compliance with the aims and principles of the Charter and, more broadly, with the "principles of justice and international law".[29]

---

[27] The White House, The National Strategy For The Physical Protection Of Critical Infrastructures And Key Assets Annex2, 24 (Dhs Gov 2003)
[28] United Nations Charter, June 26, 1945, U.N. Doc. A/5/1 Art. 24
[29] United Nations Charter, June 26, 1945, U.N. Doc. A/5/1 Chap. Vii

11. Cyber Operations and the Law of Neutrality

There can be no doubt regarding the validity of the core principles of neutrality in the case of an armed conflict where traditional weapons have been used. However, the application of neutrality to hostilities and hostile acts conducted in cyberspace has to be taken care of in a separate manner. The main purpose of law of neutrality in the cyber space domain is to protect the cyber infrastructure which is located within the neutral state and hence there is an obligation to the belligerents with respect to the inviolability and sovereignty of States not getting involved into any harmful interference related to the cyber infrastructure of the neutral state's territory. On the other hand, neutral States must act in an impartial manner and they must not engage in any kind of Cyber activities that are the military action of belligerents and that are detrimental to other belligerents. Moreover, their obligation is to take all the necessary measures to eradicate the abuse of cyber infrastructure located within their territory by any belligerent. For example the US Department of Defence (DOD) has taken a step long-standing International norm that are the guiding principles of state behaviour in respect of peace and conflict software applied in cyber also the DOD on the basis of the cyber space police report emphasis that the application of the law of armed conflict cyber space is really critical. It must be added in this context that the application of the law of neutrality to Cyberspace has recently been acknowledged in the HPCR manual.[30]

12. Cyber Operations and Jus in Bello

International Humanitarian Law (IHL), which is popularly referred to as jus in bellum, or the "law of armed conflict", is applicable exclusively in regulating armed conflict situations and for the regulation of the conduct in terms of hostilities between the belligerents. The most important source of IHL is the Geneva Conventions, two additional protocols of 1977 and the Provisions of the Fourth Hague Convention and a number of conventions limiting or prohibiting the use of such weapons. The cyberwarfare domain is not necessarily governed by international humanitarian law, especially since the subject of Cyber criminality and cyber terrorism has been kept outside the purview of IHL. In this chapter, an examination shall be made of the extent the traditional methods of warfare can successfully be transposed to cyber warfare.

[30] International Court Of Justice, Legality Of The Threat Or Use Of Nuclear Weapons, Advisory Opinion § 89 (Icj 1996)

Cyber Operations as "Warfare"

The answer to the question of whether cyber operations can result in armed conflict, warfare or hostilities can be found by raising the preliminary question of definition and terminology. It is important to remember that the term cyber war. Cyber hostilities and cyber conflict have not been specified for the purposes of international law. The Shanghai Cooperation Organisation is the only treaty that outlines the general definition of information warfare. It states that an information war is nothing but when two or more States damage information systems, critical infrastructure, political, social and economic systems, including the process and resources for the betterment of the opposing party. As several leading analysts have pointed out, the term information warfare is very much misused as an information operation. The key distinction between these two words is that the latter exists during the Periods of War and Peace, both when, as the former suggests, solely the intelligence operations carried out during military conflict and explicitly prohibits information operations that take place during peacetime. This suggests that in the pre-existing wars today, the usage of the words cyber warfare, cyber conflict and cyber hostilities can be limited to the definition of IHL under the topic of armed conflict. IHL seems to have been relevant in the sense of military non-international armed conflict. It is pertinent to note that cyber operations existed during the time of adoption and drafting of the leading instruments of international humanitarian laws, but IHL does not exclude their application to such operations.

Cyber Operations as "Attacks"

The term attack is technical in nature, as it can be in various forms; for example, the individual civilians and civilian populations are not going to be the object of an attack. Indiscriminate attacks are entirely prohibited, and attacks are limited to military targets only. The same refers to the concept of assault and precautions as a consequence of the effects of the attack, including those covered by medical units. Article 49(1) of Additional Protocol 1 states that an attack an act of violence against the adversary is considered either as a defence or as an offence. This precise definition has sparked an important controversy about what degree of an act of aggression should be called in terms of non-kinetic aggression. Currently, kinetic violence is not taken into account as a commonly accepted concept of violence, but it can also be seen that the resultant consequences are associated with Kinetic violence, such as the death or disability of individuals or that it results in physical damage to objects. This precise approach does not apply the principle of attack in the strict sense, but merely considers whether the cyber-related

triggering mechanism is likely to cause death, damage or damage equivalent to, but represents an act of aggression within the context of the Additional Protocol's 49(1). Cyber operations aimed at capturing rather than injuring, destroying or killing the target, this extreme difference is very common as to whether the simple notion of attack is often utilised. Even though an 'attack' forms some of the fundamental principles in international humanitarian law, cyber hostilities cannot be solely limited to the frameworks related to the term. Therefore, while the attack represents the prevailing military activity, it would be very misleading to assume that cyber operations are not categorised as an attack under IHL that governs the conduct of hostilities.

Cyber Operations as "Hostilities" and "Direct Participation" therein

The definition of hostilities as a joint resort by the parties engaged in the war, according to the International Committee of the Red Cross, requires the aggregate total of all hostile actions by individuals carried out as a result of hostilities requiring direct involvement. Under international humanitarian law, direct involvement in hostilities also requires conduct which, if carried out by civilians, results in suspension in order to protect against direct attacks. The direct intervention of the principle of hostility goes beyond the notion of attack, according to the report of the International Red Cross Committee, and it not only involves the use of harm, death and destruction, but also implies any act that is likely to impact the military capability or military activity of the belligerent group. In addition to constituting hostilities in the field of international humanitarian law, the problem of cyber operations must lead directly to damage and must also be structured to support belligerent actions and to the detriment of other activities. The question of whether the damage is direct or indirect depends entirely on the ability of the belligerent party and the extent of the damage to the enemy. Accordingly, circumstances in which a belligerent is responsible for cyber operations are intended to damage either by directly causing injury, death or destruction or by directly affecting the military capability of the military operations. The nature of such an operation must be regarded as hostilities and would be subjected to all kinds of restrictions imposed by international humanitarian law. Therefore, the cyber operations that has been aimed to incapacitate or disrupt the computer-controlled weapon system, radar, logistic supply of an adversary may not result in causing any physical damage directly but it will definitely be qualified as a part of hostility and would be subjected to the rules and principles of international humanitarian law that are governed related to the conduct of hostilities. On the other hand, cyber operations that

do not cause death or destruction by injury or military damage would not be protected by the IHL and would not be regulated by it.

13. Non-State Actors in Cyber Warfare

Conflicts are fought not only by nation-states but also by a wide range of non-state players in the age of international conflicts and the developing digital sphere. A paradigm shift in the way that conflict is understood in the twenty-first century has been brought about by the emergence of non-state actors in cyberwarfare.

In the realm of cyberspace, numerous actors beyond state oversight actively engage in activities, impacting religion and global politics, financial stability and public welfare. The spectrum of non-state players in cyberspace is vast and varied, encompassing hacktivist groups driven by ideology and highly skilled cybercrime syndicates seeking financial gain.

States hire non-state actors primarily for self-defence purposes. States hire non-state actors primarily for self-defence purposes. Creating accountability in cyberspace is difficult, as being secretive about one's identity is easy in the realm of cyberspace. States are able to ensure they are not prosecuted due to cyberattacks with the help of non-state actors. Such actors can avoid responsibility and also help the states in denying their role in such attacks. Thus, cyber warfare, which takes place with the help of contractors, allows states to profit while taking zero responsibility under the eyes of international law enforcement. The use of non-state actors is most likely to occur when the cyber operations are of an unlawful nature. For example, North Korea has used the hacker group Bureau 121 to engage in cyber attacks against other countries, particularly South Korea.[31]

With the rise of global connectivity, it is important for security experts and the public to consider policies that reflect the strategies of non-state actors in cyber warfare activities. Warfare is developing and changing with the evolving technologies, and so it is important to focus on issues related to national security with regard to cyberspace.

14. Cyber Warfare and the Role of Hacktivists

[31] Walter De Gruyter, Military Studies (Brill 2020)

Hacktivists are an important group that should be considered when evaluating the role of non-state actors in cyber warfare activities. Such actors will use their advanced digital tools and skills to push their political agendas. Such groups are not properly organised and can also be considered to be decentralised organisations. Their primary focus is to illustrate their disapproval for certain societal norms and injustices through digital means. Examples are the Syrian Electronic Army, Anonymous, and the Lizard Squad. [32]

Some of the illegal activities that such groups engage in include data dumps, cyberespionage, distributed denial-of-service attacks, etc. Such groups will usually not follow the laws and policies related to digital networks and will also frequently steal information from such networks. Furthermore, such groups also take advantage of social media platforms to reach a larger audience.

With regard to cyberwar and the changing nature of global aggression between countries, hacktivist groups are important actors. They use the digital world and networks as a form of battlefield. While their importance has been highlighted by policymakers and researchers, it is also important to consider the difficulties in recognising these actors as well as associating them with a specific state.

15. Role of Extremist Groups in Cyberspace

Extremist groups have varying technical skills and capacities with regard to cyber warfare. However, they pose a significant threat, particularly in relation to terrorist activities on the global level.

The threat of extremist groups is high, and the US Government used the Red Team to improve its technical capabilities and defence systems. This involved 35 hackers attempting to interfere and hack into the US National Security Network while pretending to be a part of the North Korean Intelligence with permission to target the US Pacific Command and penetrate any Pentagon network. They had the permits to use any openly downloadable tools from the internet. Through the use of "brute force cracking", they were able to decode encrypted data,

[32] Stefano Baldi, Eduardo Gelbstein, Jovan Kur Balija, Hacktivism, Cyber-Terrorism And Cyberwar The Activities Of The Uncivil Society In Cyberspace (The Information Society Library 2003)

map networks and even acquire passwords.[33]This reflects the real threat that extremist organisations can also pose to the US or any other national security system simply by using openly available hacking tools on the internet.

It is very important that the extremist views and mindsets in the state must be subjected to certain actions, and those actions must be focused on mixed approaches, specifically towards exclusion of extremist mindsets especially, in the domain of cyberspace. Some of the approaches which can be taken in this regard are the rehabilitation of the individuals under the influence of the extremist view by digital means. The governments can also emphasise developing strict laws that help to deter the creation of extremist groups. It is very important for the state to have a technological infrastructure that is very strong and secure so that it can prevent attacks from extremist groups.

16. Negative Impact of Cyber Warfare on Human Rights

There are several negative effects as a result of cyber warfare, especially related to human rights. The fact that cyber warfare has become a tactical practice which is common among states cannot be ignored. This damage not only creates an impact on the critical resources of the state, but it also impacts the human rights of the citizens of that states. For example, in the year 2022, an attack was inflicted on the Ukrainian e-governance platform, Diia, which specifically caused the shutdown of various critical resources of the state. For example, the Healthcare services, National Banks, etc. Along with this issue, the human rights of the citizens were also affected, for example, their inability to access the information related to Healthcare as well as their privacy. It is very important to find ways to manage such attacks because if there is a shutdown of important infrastructure like the public health care system, human lives can be affected.[34]

In order to prevent such attacks, which create negative impact on the effect of human rights of the citizens various steps should be taken by the states for preventing the attacks. It is also very important to protect the activists as well as the groups which work towards the protection of

[33] Dan Verton, Black Ice (Computerworld, 2003)
[34] Online Cambridge University, Ukraine, Cyber-Attacks And Lessons For International Law (Cambridge University Press 2022)

human rights as their advocacy specifically protect many persons in the state who are at the disadvantaged position.

17. Distortion of Information and Cyberspace

Cyber warfare can also take place on the basis of spreading misinformation. This is considered a commonly used tactic to create chaos, as well as false narratives and panic within democracies. As most democracies ensure free speech, this particular technique is considered an effective mechanism for impacting the results of the election. In recent times, everyone has constant access to various digital spaces like X (formerly known as Twitter). False information on such platforms can severely affect the entire community within the democracy. It can also significantly affect the opinions of the individuals as well. The governments of different states are able to control the narrative put by different countries by means of this Warfare technique. To overcome this problem, the government must engage in censorship activities, which will help in protecting its citizens from false information. The government should restrict the social media platform or limit their access to a certain source of misinformation.

A memo issued by the Pentagon General Counsel's office which considered the concept of military cyber attacks. information operations are excluded to be a part of such attack. However, operations like spreading of logic bombs were noted as a form of warfare the to make the citizens vulnerable to misinformation. Various morphing tools and techniques are also found that spread misinformation and are included in the forms of warfare.[35]

These specific types of attacks are considered to be the major threat to the democratic states. The reason is their ability to impact the election outcomes. It also impacts the operations and process of Democratic institutions. Debates and public opinions are also affected in this process. Therefore, it is very important for the democratic Nations to ensure that their citizens are protected from false digital information.

18. Recommendations and Suggestions

The incidences of cyber warfare are increasing in modern times. The current International humanitarian Law (IHL) is not found to be adequate for protecting states from such attacks. It is very important for the IHL principles to be amended by the different policymakers. The various ingredients of cyber warfare must be considered in those principles, then they should be adopted and fit into the domain of IHL. ICJ has also specifically stated that future Warfare

[35] Pentagon General Counsel Office, Assessment Of International Legal Issues In Information Operations, (The Guardian, November 8, 1999)

weapons can also be made a part of the domain of IHL. There are several reasons why the present International Humanitarian Law is difficult to apply in the digital space. The most challenging task in identifying the party behind the attacks is the ease with which anonymity can be maintained digitally.

Furthermore, it can also be challenging to determine the difference between military objects of the cyber operation and civilian objects, as this also affects the assessment of 'proportionality' in the context of IHL. These challenges also make it difficult to enforce IHL due to the evolving nature of cyber operations.

It is also important to note the complementary nature of the UN Charter and IHL. While the Charter restricts the use of force by countries, IHL provides complementary mechanisms for handling such events. International humanitarian law, on the other hand, comes into play in the event that an armed conflict arises and provides crucial safeguards for both civilian property and individuals who choose not to participate in hostilities (such as injured troops or captives).[36] IHL provides an extra layer of protection for all victims of war in the tragic event that hostilities break out, without replacing or nullifying the UN Charter.

19. Conclusion

An adaptable and efficient legal structure capable of addressing the complexities of modern warfare is crucial, particularly given the intersection of cyber warfare and international humanitarian law. As the nature of warfare is constantly being redefined by technological advancements, it is crucial for the international community to establish strong norms and mechanisms that can regulate state behaviour in cyberspace and uphold the fundamental principles of humanitarian law. These laws are meant to protect human dignity and lessen the impact of armed conflicts on civilian populations.

As far as International Law is concerned, it has been found from time to time that the phenomenon of cyberwarfare is non-existent in a legal vacuum, but it is always subject to the established rules and principles of International Law. Therefore, pre-existing principles and rules that can be found in the cyberspace domain have encountered a lot of difficulties and have certainly raised a number of questions. Some of these concerns can be effectively tackled by interpretative means of certain existing treaties, while others are aimed at a unanimous policy decision by international law scholars and the international community. An attempt in this

[36] United Nations Charter, June 26, 1945, U.N. Doc. A/5/1 Art. 2(4)

paper has been made to identify some of the most important questions and initiatives, in terms of suggestive measures are also being discussed for their resolution. As of now, the domain of cyberwarfare has achieved a humanitarian consequence, and it can be hoped that the present state of affairs is not going to change the future. The field of cyberwarfare has reached a humanitarian impact from now on, and it is hoped that the current state of affairs will not change the future. It is therefore very important for states to be aware not only of the fulfilment of their legal responsibilities, but also to examine and analyse the information on modern weapons and the methods used to operate in cyberwarfare, towards fulfilling the responsibility of the upcoming future generations.

20. References

1. Albrecht Randelzhofer, The Charter Of The United Nations: A Commentary 117 (Vol. I, Oxford 2002)
2. Armin Bogdany And Rüdiger Wolfrum (Eds), Max Planck Yearbook Of United Nations Law 96 (Vol. 14 Mpil 2010)
3. Critical Infrastructure Protection (Us Presidential Directive) – 63,1998, [§ I. 55]
4. D.W. Bowett, Self-Defence in International Law 12 (Brill 1958)
5. Dan Verton, Black Ice (Computerworld, 2003)
6. Eastwest Institute, The Russia–US Bilateral On Cybersecurity—Critical Terminology Foundations 11 (Moscow State University 2011)
7. Georg Ress, The Interpretation Of The Charter 18 (Bruno Simma (Ed.), The Charter Of The United Nations: A Commentary, Vol. I, 2002)
8. Ian Brownlie, International Law And The Use Of Force By States 362 (OUP 1963)
9. International Court Of Justice, Corfu Channel (United Kingdom Of Great Britain And Northern Ireland Albania) (Merits), Separate Opinion By Judge Alvarez 47 (Icj 1949)
10. International Court Of Justice, Legality Of The Threat Or Use Of Nuclear Weapons, Advisory Opinion § 89 (Icj 1996)
11. Loyola Of Los Angeles International And Comparative Law Review Vol. 32 306 (Loyola Marymount University 2010)
12. Mačák And Vignati, Civilianization Of Digital Operations: A Risky Trend (Asia Pacific Journal Of International Humanitarian Law, 2023)
13. Marco Roscini, World Wide Warfare—Jus Ad Bellum And The Use Of Cyber Force 105 Ff (Armin Bogdany And Rüdiger Wolfrum (Eds), Max Planck Yearbook Of United Nations Law, Vol. 14, 2010)
14. Marco Roscini, Cyber Operations And The Use Of Force In International Law 17 (Oxford University Press 2014).
15. NATO, Tallinn Manual (CCDOE 2017)
16. Online Cambridge University, Ukraine, Cyber-Attacks And Lessons For International Law (Cambridge University Press 2022)
17. Pentagon General Counsel Office, Assessment Of International Legal Issues In Information Operations, (The Guardian, November 8, 1999)

18. Stefano Baldi, Eduardo Gelbstein, Jovan Kur Balija, Hacktivism, Cyber-Terrorism And Cyberwar The Activities Of The Uncivil Society In Cyberspace (The Information Society Library 2003)
19. The White House, The National Strategy For The Physical Protection Of Critical Infrastructures And Key Assets Annex 2, 24 (Dhs Gov 2003)
20. UN General Assembly Resolution 58/199, 30 January 2004.
21. United Nations Charter, June 26, 1945, U.N. Doc. A/5/1
22. U.S. Department Of Defense, The National Military Strategy For Cyberspace Operations Gl-1 (Us Gov 2006)
23. U.S. Joint Chiefs Of Staff, Department Of Defence Dictionary Of Military And Associated Terms 41 (U.S. Govt 2001)
24. Us Patriot Act, 42 U.S.C. 5195c (E), § 1016(E) (2001).
25. Vienna Convention On The Law Of Treaties, 1969 Art. 31(1)
26. Walter De Gruyter, Military Studies (Brill 2020)
27. Yoram Dinstein, War, Aggression And Self-Defence 175ff (4th Ed., Cambridge University Press 2005)