INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERWARFARE AND LAW OF ARMED CONFLICT: UNDERSTANDING THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAW IN CYBERWAR

AUTHORED BY - K. ASWATHA

ABSTRACT:

In Modern times, information technology plays a significant role in every aspect of civilian life as well as military operations which is known as 'cyber space'. This cyber technology will benefit to us as well as it provides opportunities for exploitation too. Attacking the other state by means of cyber technology results as cyber attack. Cyberwarfare is an emerging form of warfare but it is not addressed by existing International law. This paper discusses about the application of International Humanitarian Law rules and its principle to the cyberwarfare. The author trying to find out the lacuna based upon the challenges that IHL faces while taking cyberwarfare into consideration. Moreover, the paper also analysis about the application of IHL in various cases of cyber warfare. Therefore, the main motto of the author the acceptance of IHL in cyberwarfare to prevent the harm caused to the civilians in the near future.

Keywords: Cyberwar, Tallinn Manuals, Sovereignty, Challenges, Intervention

1. INTRODUCTION:

From Gun powder to cyber war, the advancement of technology led to different forms of warfare. In this Century, Cyber space plays a major role. It is the notional environment in which digitized information is stored or communicated over information systems and networks.[1] There are several vulnerabilities in cyberspace, which allow malicious actors to make cyber systems function in ways that they weren't designed to. Vulnerabilities can be caused by design flaws or inherent in the systems' design, and they can coexist with "bugs," which are flaws that may result in accidents. Governments are also aware of the situation and need to take action in order to prevent the harm from cyber space. In 2004, General S. Padmanabhan, former chief of the Indian Army envisioned that the future where wars would be fought not just with soldiers

[1] Graeme P Herd and John Kriendler (eds), Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance (Routledge 2013) https://dokumen.pub/understanding-nato-in-the-21st-century-alliance-strategies-security-and-global-governance-9780415436335-9780203076002-9781138831889.html

 ISSN: 2582-6433

and tanks but with invisible weapons, cyber systems embedded in everyday devices.[2] Today, the people are living in the cyber space.

Cyberwar is one of the newest frontiers of warfare, extending the known universe of land, sea, air and space.[3] Cyberspace and information technology are drastically altering the character of the contemporary battlefield. The employment of satellites on the battlefield, autonomous tools, intelligence systems, information exchange and fusion systems, real-time integration of target seeking sensors with firing systems, and more are a few examples of the cutting-edge technology present on the battlefield. The public are not aware about the consequence of cyberwar and how it will affect the society. It is one of the far worse wars like nuclear weapon. Whereas nuclear war and other war crime, there will be physical consequences, unlike cyber war. In recent year, it is shown that the cyber operation will seriously affect the civilian infrastructure which results in harm. The 2010 National Security Strategy emphasized that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[4] Various countries concern over the cyber war so they take measures and establish numerous international conventions and protocols to address the issue on the legalities of cyberwarfare which includes the Tallinn Manuals, the Singapore Norms Package, the Paris Call, the Budapest Convention, International Code of Conduct for Information Security, and International Strategy of Cyberspace on the International Law for the IHL applicability in cyberwar. But unfortunately, it is still in controversy. In order to avoid unforeseen consequences of an attack, new rules for limiting cyberconflict must be developed.

2. LITERATURE REVIEW:

2.1. Cyberwar- an emerging new form of warfare:

The term 'Cyberwar' does not have the exact definition in International law. However, many experts describe that cyberwarfare as cyber operations conducted in or amounting to an armed conflict. Such cyber operations, which involve the development and dispatch of computer code from one or more computers to target computers, can be aimed at either infiltrating a computer system to collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise

[2] Ananth Krishnan, 'Lebanon: Hezbollah cyber attack, pager explosions, warfare, Israel-Gaza' (Frontline, 19 September 2024) https://frontline.thehindu.com/news/lebanon-hezbollah-cyber-attack-pager-explosions-warfare-israel-gaza/article68654302.ece
[3] Sinan Ulgen, 'Cyberwar' (2010) <https://www.jstor.org/stable/resrep26924.12>
[4] Lieutenant Colonel Scott W. Beidleman, 'Defining and Deterring Cyber War' (2010) National Security Strategy 21 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795>

 ISSN: 2582-6433

manipulate processes controlled by the infiltrated system.[5] It involves the use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyberattacks, espionage and sabotage.

"Cyberwarfare" has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"[6], but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.[7]

2.2. Importance of framing rules in respect to cyberwarfare:

Cyberwar not only cause harm to computers networks and communication system but also to military operation, which eventually led physical harm to the public. One of many cyberwar cases, which is popularly known as WannaCry. This ransomware attack in May 2017 affects both government and civilian infrastructures including hospitals, transport, and energy services around the world. Followed by NotPetya ransomware in June 2017 targets companies (Maersk, FedEx, and Merck) in Ukraine attacking its government, financial, and energy institutions which results in $300 million financial loss (Wong & Solon 2017).[8] The cyberwar eventually develop from economic loss to such government to target nuclear facilities; oil pipelines or power grids; breach on sensitive information, control system of critical facilities etc., some of such cases will be listed in the following paper.

This cyberwar could be used as an ultimate weapon to strike down the air defence system.[9] If an attack has been executed through cyberspace, the attacker can accomplish upon controlling the air defence system in their hands, without causing physical destruction, and military or civilian casualties.[10] Likewise, in 1990s, NATO air war planners devised a cyber attack to insert false messages and targets into the Serbian military's centralized air-defense command

[5] Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 886 International Review of the Red Cross 533, 538.
[6] Richard A. Clarke, *Cyber War* (HarperCollins 2010) ISBN 9780061962233.
[7] Sean Collins, 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications' (April 2012) 7 Journal of Policing, Intelligence and Counter Terrorism 1 <https://doi.org/10.1080/18335330.2012.677032>
[8] T Ramluckan, 'International Humanitarian Law and its Applicability to the South African Cyber Environment' (2020) 19 No. 3 102.
[9] Bradley Graham, 'Cyberwar: A New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal' (Washington Post).
[10] Brian T. O'Donnell & James C. Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8 Journal of Conflict & Security Law 133, 149.

 ISSN: 2582-6433

network, but the NATO did not launch this cyber attack.[11] Cyberwar not only disable military operation but also such civilian infrastructure which serves both military and civilian functions namely power plants, telecommunication, transport infrastructure. Destruction of such civilian infrastructure results in loss of power supply until the war is over which will made it difficult for the hospital for saving people's life.[12]

2.3. Application of International Humanitarian Law rules and its principle in cyberwarfare:

International Humanitarian Law applies to both International Armed Conflict and Non-International Armed Conflict in order to limit the effects of the war and to minimise the sufferings of the victim of the war. This law applies to combatants, non-combatants, civilians, Hors de combat. The cyberwar has not been included in IHL.

A) Additional Protocol I: Inclusion of new weapon

To adopt cyberwar as a new weapon under IHL, the High Contracting party has an obligation under Art 36 of Additional Protocol I to decide whether such weapon is prohibited under IHL or any other rules of IHL.[13] A key information in regard to make an informed evaluation of cyber operations compatibility with IHL which is often lacking. They are: (a) the technology available, (b) the attacks conducted, (c) the identity of the parties conducting the attacks, and (d) the policies, guidelines, and rules that states apply in relation to cyber warfare, along with their reading of the applicable rules of IHL.[14]

B) International Armed Conflict:

IHL applies only to the armed conflict.[15] 'An international armed conflict occurs whenever there is a resort to armed force between states. Cyber war will only be considered as an international armed conflict if it satisfies that a) the cyber operation involved are in attribution to the state; and b) they amounted to a resort to armed force against another state.[16] The classification of a situation as an armed conflict under International Humanitarian Law (IHL)

[11]William M. Arkin, 'The Cyber Bomb in Yugoslavia' (Washington Post, 25 October 1999) <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm> accessed 8 March 2008.
[12] DOD, Assessment, (discussing the war crime allegations sur- rounding the coalition bombing of the electrical power system in Baghdad).
[13] International Committee of The Red Cross, 'Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)' (8 June 1977).
[14]'Applying International Humanitarian Law to Cyber Warfare' <http://www.jstor.com/stable/resrep08957.8>
[15] See, Common Article 2 of the four Geneva Conventions of 1949: 'An international armed conflict occurs whenever there is a resort to armed force between states.
[16] *Ibid*

 ISSN: 2582-6433

has significant implications, allowing for the use of lethal force against enemy combatants and the targeting of military objectives. However, it also protects civilians and civilian objects from indiscriminate harm. Cyber warfare complicates this legal framework, as it can cause significant damage without direct physical destruction, raising questions about whether such actions constitute armed force under IHL. A more restrictive interpretation could limit the conditions for applying IHL to cyber operations. Currently, the lack of clear state practice and consensus on cyber warfare's legal status leaves its classification under IHL uncertain, highlighting the need for ongoing discussion and potential legal developments.[17]

C) Non-international Armed Conflict:

For the existence of cyberwar in non-international armed conflict, it must entail armed violence involving at least one non-state actor where (a) the parties involved satisfy a minimum level of organization and (b) the armed violence reaches a minimum level of intensity. However, applying these criteria to cyber warfare raises a number of difficulties.[18] However, applying these criteria to cyber warfare presents challenges. While cyber operations that disrupt physical objects can clearly be seen as attacks, it is less straightforward to categorize operations that solely disrupt communication in cyberspace. This ambiguity complicates the classification of cyber warfare within the context of non-international armed conflict.[19]

D) Principles of IHL:

The norms in international humanitarian law covering such issues as the use of indiscriminate weapons, distinction between military targets and civilians, proportionality and perfidy, can and must be applied also to cyber warfare.[20] Principle of Distinction, Principle of Proportionality and Principle of Precaution are some cardinal principles used to distinguish between civil and military personnel and to ensure protection under IHL accordingly.[21]

***Firstly,* Principle of distinction** has been articulated in Art 48 of Additional Protocol I and Rule 93 of Tallinn Manual 2.0. (Schmitt, 2017, p. 420). This principle highlights that the attack

[17] Nishat Subah Maliha, 'Cyber Warfare: Challenges in the Application of International Humanitarian Law to Virtual Conflict' (2020)
[18] Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' in *Law and National Security: Selected Issues* (2020) 83
[19] *Supra 15*
[20] International Committee of the Red Cross, 'Cyber Warfare' (2010) <https://www.icrc.org/en/document/cyber-warfare>
[21] *Supra 1*

 ISSN: 2582-6433

should be distinguished between civilian objective and military objective (Droege, 2012, p. 539). According to this principle, attack should only be against military objective not the civilian objective. Sometimes, state has dual-use objects in cyberspace, such as part of the civilian infrastructure that supplies the military for their operations such as power plants or electrical grids. Military use some data to store in civilian database, in such times entire network turned as military objective.[22] According to the Commentary in respect to Art. 52 of AP I, it provides that there must be a definite military advantage for every military objective that is attacked.[23]

In the context of cyber warfare, commanders must ensure that their operations target military objectives rather than civilians or civilian objects. This distinction is important, as military and civilian computer systems are not entirely the same. (Droege, 2012, p. 539). IHL provides special protections for certain categories, such as medical personnel and facilities, which are often marked by visible symbols. (ICRC), 2011, p. 25). The concept of distinctive emblems or digital markings for identification in cyberspace has emerged as a potential protective measure. This could involve digital symbols or signals, like light or electronic signals, to signify protected entities. However, this idea is still under discussion and requires further development and testing to be effective. (Rodenhauser et al., 2021).

Secondly, **Principle of Proportionality** has been manifested under Arts. 51 (5) (b) and 57 (2) (iii) of Additional Protocol I, Art. 52 (5) (b)., and rule 113 of Tallinn Manual 2.0. (Schmitt, 2017, p. 471). Proportionality determined the degree and kind of force used to archive a military objective by comparing the predicted military advantage gained to the expected incidental damage inflicted on civilians and civilian property (Pascucci, 2017, p. 445). To determine if an attack was proportionate, one must evaluate whether a reasonable person, given the information available to the attacker, could foresee excessive civilian casualties resulting from the operation (International Criminal Tribunal for the Former Yugoslavia 1993-1998, para. 58).

Thirdly, **Principle of Precaution** has two approaches namely Precautions in attack and Precaution against the effect of attack based upon Art 48 and 49 of AP I. IHL emphasizes keeping military and civilian uses distinct, prohibiting dual-use systems in this context. It

[22] Amalia Zuhra & Laila Almira, 'The Limitation of Cyber Warfare Under Humanitarian Law' (2021) 3 Nomor 1 1-10 <http://dx.doi.org/10.25105/teras-lrev.v3i1.10741>
[23] Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 52 (1) (2)

 ISSN: 2582-6433

requires to verify that their targets are legitimately military objectives not the civilian objectives. If an attack is likely to cause significant collateral damage, it must be cancelled or suspended. Upon choosing military objectives, constant care and reasonable precautions must be taken upon keeping in mind the impact of their action and simultaneously to protect the civilians. Additionally, The Tallinn Manual outlines specific precautions for cyber warfare, such as Segregating military and civilian cyber infrastructure; Ensuring critical civilian systems are isolated from the Internet; Backing up vital civilian data; Preparing for timely repairs of essential systems; Digitally recording cultural and spiritual artifacts to aid in reconstruction; Using antivirus measures to protect civilian systems during military attacks.

3. RESEARCH GAP:

The aim of this research paper is to deal with the problem in respect to cyberwarfare which will be arising in the near future. This paper identifies the lacunae, challenges, and gaps present in the above comprehensive literature studies and helps to address such gaps for development of a legal framework. As cyberwarfare evolves, it's essential to assess whether current IHL adequately governs cyber operations, particularly regarding gaps like unclear definitions of cyber attacks, challenges in attributing actions to specific actors, and ambiguities in protecting civilians. Addressing these shortcomings is crucial for maintaining civilian protections and accountability in modern conflicts, making your findings vital for policymakers, military strategists, and legal experts. Your methodology could involve analysing existing IHL texts, reviewing case studies of cyber incidents, and proposing legal reforms to enhance clarity and effectiveness in regulating cyberwarfare. This approach underscores the need for IHL to adapt to the complexities of contemporary warfare.

4. RESEARCH QUESTIONS:

This paper seeks to explore the following research questions:

1. Does a non-consensual cyber operation that intervenes in another state’s military or civilian operation violates such state's sovereignty and potentially trigger a cyberwar?
2. Whether the IHL rules and principles is compatible and effective with cyberwarfare or new legal framework is needed for such emerging warfare?

 ISSN: 2582-6433

5. CHALLENGES FACED UPON APPLYING IHL IN CYBERWAR:

The nature of warfare is changing according to the technological development. Modern warfare causes significant impact than the conventional warfare. Thus, there is a need for code of conduct to control and safeguard the civilians from such war crime. The National Strategy to Secure Cyberspace acknowledges that cybersecurity is a real issue and sets several goals for improvement.[24]

Various cyber attacks happened during recent times and many countries were affected due to such incidence. Recently, in the Israel pager attack, cyber war were initiated which causes physical destruction to the communication technologies. Likewise, there were many incidents such as Russian-Ukraine war occurred but still there were no implementation of cyberwar in IHL or form any other rules. There are many lacuna upon implementing cyberwar in IHL. IHL only deals with international armed conflict and non-international armed conflict.[25] However, there are still lack of understanding upon applying cyberwar in International law due to complexity. Even though, there is a provision for adding new weapon in IHL, likewise nuclear weapon is added. But adding cyberwar in IHL is still in controversy.

Based upon the author's understanding, the application of International Humanitarian Law to cyberwar can be summarized as follows:

- Cyberattacks as Armed Conflict- Cyber operations must reach a threshold of severity to be classified as armed attacks under international law.
- Criteria for Interference- Specific criteria are needed to define what constitutes "interference," focusing on the scale and impact of the attacks.
- Sovereignty in Cyberspace- The concept of territorial sovereignty in cyberspace is complex and requires clearer definitions to determine when an attack occurs in another state's territory.

5.1. Anonymity of kinetic attack in cyberwar:

According to IHL, they need to satisfy the criteria of attack in cyberwar. It need to be the involvement of kinetic force in such attack. There will be kinetic force of attack in conventional

[24] Office of the President, *The National Strategy to Secure Cyberspace* (2003) <http://www.us-cert.gov/reading-room/cyberspace-strategy.pdf>
[25] Rona G, 'Interesting Times for International Humanitarian Law: Challenges from the "War on Terror"' (2005) 17(1–2) Terrorism and Political Violence 157 https://doi.org/10.1080/09546550590520645

 ISSN: 2582-6433

war unlike cyberwar. In cyberwar, it is impossible to track down the actual address of the original source of the attacker because the attack can able to hide the origin of the attack and also able to multiple detour the attack in various countries symbolising the attack originated from that country. IHL do not have a clear term about the stipulation and origin of attack in cyberwar.[26]

5.2. Criteria for Assessing Interference in Cyber Warfare:

Based upon the observation of applying IHL rules, during an armed conflict, there need to differentiate between military and civilian objects. The threat to computer information systems presents a substantial danger to the military, the civilian government, industry, academia, and the general public.[27] In accordance with Article 13 (2) of Geneva Conventions: '(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war.[28]

Whereas the Tallinn Manual do not provide clear detail how it is actually works in cyberwar. Because the impact of the cyber attacks is not predicted. Even though there was no physical harm in cyber war but a mere disruption, interference, and permanent loss of functionality or destruction may cause a severe harm to both military and civilians if not targeted accurately. Nevertheless, this act of violence is not embedded in IHL. Lack of endurances of cyberwar in IHL, it suffer greater damage.

Cyber law expert Dinniss points out: 'Viruses and worms are two methods of computer network attack, which are particularly likely to fall into this category as their effects are often not limited by their creators.'[29]

5.3. The Ambiguities of Sovereignty in Cyber Warfare:

There is no clear definition about sovereignty over cyberwar. In respect with Article 2(4) of UN Charter, it prohibits the "threat or use of force against the territorial integrity or political independence of any State." Cyberspace includes all of the integrated command, control, and

[26] *Supra 1*
[27] Mathew Borton, Samuel Liles & Sydney Liles, 'Cyberwar Policy' (2010) 27 Journal of Marshall Journal of Computer & Information Law 303.
[28] See Article 13(2) of the Geneva Conventions I and II
[29] H. Heather Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 203.

 ISSN: 2582-6433

communication networks throughout the world.[30] Thus, cyber space is different from order physical space, so it is difficult for state to claim sovereign responsibility for the cyber act. The issue arise from the cyberwar is from 'where' the attack reach their targets because the attack can take place anywhere even from the targeted country. As already elaborated, the cyber attack cannot be traced. It can pass through within the civilian's database of the targeted country, other third country database etc. Since the IHL does not prohibit restriction on passing the data, the cyber weapon can pass through legally without any territorial interference. The manual suggests to take off the responsibility from the transmitting countries.[31] Under international law, state are prohibited to intervene the internal and external sovereignty of another state. ICJ recognized non-intervention as "a corollary of the principle of the sovereign equality of States."[32] Although state have the responsibility over the international wrongful act which is committed within its territory if the state controls the individuals or entities that committed the Act.[33] In today's world, we cannot confine the cyber operation within a country but we can limit the cyber operations which cause physical harm. There is indeterminate sovereignty rule over cyber war in IHL. Without clear prohibition of cyber operation in another state territory, it will cause some chaos which ultimately leads to cyberwar.

6. RECOMMENDATIONS:

1. To constitute a specific code of conduct to regulate cyberwar. The means and methods of cyber war should be established in the said code. Although, the cyber operation which performs in another state territory which leads to physical harm should be implemented with restrictions. It should provide a determinate sovereignty rule over cyberwar.
2. There is need for reconstruction in Tallinn Manual upon applying International Humanitarian Law in cyberwarfare for clearer guidelines on civilian protection and critical infrastructure.
3. To provide a clear standard definition in respect to international law. Without such standardised definition, the state can interpret the term in their own perspective with leads to differentiation.

[30] Mathew Borton, Samuel Liles & Sydney Liles, 'Cyberwar Policy' (2010) 27 J Marshall J Computer & Info L 303
[31] Rule 7 & 8 of the Tallinn Manual
[32] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) (Merits) [1986] ICJ 14, 106, ¶ 202 (27 June 1986) (holding that "[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference ... parcel of customary international law.").
[33] Art 7 of Draft Articles on Responsibility of States for Internationally Wrongful Act, 2001

 ISSN: 2582-6433

4. There needs to be target assessment upon the way the cyber attack reaches the target. A mechanism has to be instituted to evaluate the targets based on military necessity, ensuring they are legitimate military objectives, and weighing potential civilian harm against military gains. This careful evaluation promotes responsible and ethical conduct in cyber operations.
5. A principle has to establish to separate the civilians and military objects which mandates clear distinction between combatants and non-combatants. This involves identifying military targets to ensure operations focus solely on legitimate military objectives while protecting civilians and civilian infrastructure from attacks.
6. Develop training programs for military personnel, policymakers, and cyber operators that incorporate IHL principles as they apply to cyber operations. Training should include case studies and simulations of potential scenarios. Continuous Learning: Implement mechanisms for ongoing education and adaptation as the technology and landscape of cyber warfare evolve. This could include regular updates and refresher courses.
7. Participate in international dialogues to create shared norms and standards for cyber warfare that adhere to IHL. This may involve treaties, declarations, or joint statements among states. Furthermore, Work with non-governmental organizations and international bodies to promote adherence to IHL in cyberspace and provide platforms for dialogue and understanding.
8. Recognize the intersection of IHL and international human rights law, ensuring that cyber operations respect fundamental human rights such as the right to life, privacy, and freedom of expression. Conduct human rights impact assessments prior to cyber operations to identify potential risks to civilians and ensure measures are in place to mitigate those risks.
9. Engage in regular discussions with other states about best practices and challenges related to cyber operations and IHL compliance. Workshops and Conferences: Organize workshops and conferences that bring together military leaders, legal experts, and technologists to discuss the implications of cyber warfare under IHL.

7. CONCLUSION:

As warfare has evolved over time, cyber warfare has emerged as a novel dimension influenced by technological advancements. The intersection of International Humanitarian Law (IHL) and cyber warfare presents substantial challenges, necessitating careful interpretation and

 ISSN: 2582-6433

adaptation of established principles such as distinction, proportionality, and necessity. In cyberwar, it is not the means of attack is detrimental but the consequences of attack. Since IHL drafters did not foresee these new methods of warfare, it is vital to reinterpret existing principles to protect civilians and preserve infrastructure. However, the current IHL conventions cannot constitute an efficient solution to the implementation of cyber warfare into the IHL framework. Therefore, there is need to produce new set of rules in regard to cyberwar.

8. BIBILOGRAPHY:

1. 'Applying International Humanitarian Law to Cyber Warfare' <http://www.jstor.com/stable/resrep08957.8>
2. 19. Office of the President, *The National Strategy to Secure Cyberspace* (2003) <http://www.us-cert.gov/reading-room/cyberspace-strategy.pdf>
3. Amalia Zuhra & Laila Almira, 'The Limitation of Cyber Warfare Under Humanitarian Law' (2021) 3 Nomor 1 1-10 <http://dx.doi.org/10.25105/teras-lrev.v3i1.10741>
4. Bradley Graham, 'Cyberwar: A New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal' (Washington Post).
5. Brian T. O'Donnell & James C. Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8 Journal of Conflict & Security Law 133, 149.
6. CLARKE, Richard A. Cyber War, Harpercollins (2010) ISBN 9780061962233.
7. Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 886 International Review of the Red Cross 533, 538.
8. Diamond, EItan. "Applying International Humanitarian Law to Cyber Warfare." Pnina Sharvit Baruch and Anat Kurz, Editors. Law and National Security: Selected Issues, Containing: Applying International Humanitarian Law to Cyber Warfare. Ramat Aviv: Institute for National Security Service, July, 2014. 67, 70. Article.
9. Dinstein, Y. "The Principle of Distinction and Cyber War in International Arm
10. Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' in *Law and National Security: Selected Issues* (2020) 83.
11. Elya Taichman, 'Defend Forward & Sovereignty: How America's Cyberwar Strategy Upholds International Law' (2021) 53 U Miami Inter-Am L Rev 53
12. H. Heather Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 203.

 ISSN: 2582-6433

13. International Committee of the Red Cross, 'Cyber Warfare' (2010) <https://www.icrc.org/en/document/cyber-warfare>
14. Lieutenant Colonel Scott W. Beidleman, 'Defining and Deterring Cyber War' (2010) National Security Strategy 21 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA500795>
15. Mathew Borton, Samuel Liles & Sydney Liles, 'Cyberwar Policy' (2010) 27 Journal of Marshall Journal of Computer & Information Law 303.
16. Nishat Subah Maliha, 'Cyber Warfare: Challenges in the Application of International Humanitarian Law to Virtual Conflict' (2020).
17. Richard A. Clarke, *Cyber War* (HarperCollins 2010) ISBN 9780061962233.
18. Sean Collins, 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications' (April 2012) 7 Journal of Policing, Intelligence and Counter Terrorism 1 <https://doi.org/10.1080/18335330.2012.677032> accessed 6 June 2015.
19. Sinan Ulgen, *Cyberwar* (2021) https://www.jstor.org/stable/resrep26924.12
20. T Ramluckan, 'International Humanitarian Law and its Applicability to the South African Cyber Environment' (2020) 19 No. 3 102.
21. T Ramluckan, International Humanitarian Law and its Applicability to the South African Cyber Environment, (2020) 19, No. 3 102.
22. William M. Arkin, 'The Cyber Bomb in Yugoslavia' (Washington Post, 25 October 1999) <http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm> accessed 8 March 2008.