*Page 1112 - 1115* **DOI:** *https://doij.org/10.10000/IJLMH.112009*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 4 | Issue 5**

**2021**

# Cyber-warfare: A Challenge for International Law

PRADYUMN AMIT SHARMA[1]

## ABSTRACT

*War and conflict have become synonymous with humanity. They have existed since even before human civilization, as we know it, came into being. As time passes by and civilization evolves, the means of war and conflict evolve with it simultaneously and increase their capacity to cause destruction and chaos. One such means, which has developed over the last few decades, is cyber-warfare and it is growing at an unprecedented rate to become something which was hitherto unheard of. In the such circumstances, when there is a lot of ambiguity and nescience with respect to formation of laws which efficiently cater to cyber-space, the question before us is to analyze how can the existing international legal framework be applied to effectively deal with cyber-warfare.*

## I. INTRODUCTION

It is an undeniable fact that over the last 3 decades internet has cemented itself as one of the most revolutionary innovations in the entire history of humankind, and for most of us, has become an indispensable part of our everyday lives. As compared to 1995, when the number of individuals actively using internet stood at a mere 16 million, it now stands at a colossal figure of 1.7 billion, as of late 2010.[2] However, as the reliance on internet, and the cyber-network it entails, grows on to be stronger than ever in all walks of life, it has rapidly opened up the horizon of creating an entirely unique battlefield for warfare which is unlike anything that humans as a collective have witnessed or imagined till now. This raises an inevitable thought that how would cyber-space, a place where trans-continental boundaries don't exist, be regulated and would the conventional principles of international law, which keeps in check traditional warfare, be applicable to this domain.

## II. WHAT IS CYBER-SPACE?

As Cyber-space is a domain created out of globally interconnected network of digital information, it is sometimes hard to imagine the repercussions of cyber-warfare out of that

[1] Author is a student at Symbiosis Law School, Noida, India.
[2] UK government, "A Strong Britain in an Age of Uncertainty: The National Security Strategy", 2010, p. 29.

 [ISSN 2581-5369]

specific domain. However, the targets of cyber-warfare might also include systems whose functionality depends upon computers, such as nuclear missiles, intrinsic transport facilities, the healthcare system, etc. which makes it as real a threat as an act of traditional warfare. However, when the question of interpreting existing international law in context of cyberwarfare arises, due considerations has to be given to the unique nature of this domain, which is that it is completely man-made and does not exist and does not have a tangible presence, but is maintained and operated collectively by a series of stakeholders, from private companies to state owned enterprises. Further, due weightage has to be given to the fact that it's constantly in a state of evolution due to rapid technological innovations.

## III. APPLICABILITY OF INTERNATIONAL LAW ON CYBER-WARFARE

International law, as it primarily exists, was created and implemented to maintain peace and order among states and their bodies. As discussed earlier, cyber-space and the issues with respect to its governance are not solely confined to the purview of states, as several non-state actors also have considerable stake when it comes to cyber-domains such as, for instance the internet. However, when it comes cyber-warfare and conflict, the existing legal framework can be applicable on both state actors and non-state actors.

When it comes to the application of international law on cyber warfare, two theories would be applicable while analyzing it, namely *Jus ad bellum* and *Jus in bello*.

### (A) jus ad bellum

*Jus ad bellum* can be described as that body of law which governs a state's resort to force when it comes to their international relations.[3] In the contemporary times, the most relevant source of *jus ad bellum* is the charter of the United Nations. As the UN charter is not precise on the explanation of the use of force as self-defense, then as per the customary law in opinio juris and state practice, it has to be perused whether cyber warfare can lead to an internationally wrongful use of force or threat, an armed attack which can justify the resort to use of force for self-defense, and a threat to the peace/breach of peace.[4] In case a cyber warfare operation fulfills any of the above conditions, then depending upon the circumstances of their action, they can fall under the prohibition under Clause 2(4) of the UN charter, which states that:

"*All member shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner*

[3] Melzer, N. (2011). Cyberwarfare and International Law. Retrieved from unidir.org: https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.
[4] Ibid 2.

*inconsistent with the purposes of the UN*."[5]

Further, if cyber operations lead to "threat to the peace", "breach of peace" or an "act of aggression", then it can also warrant the use of military force and other actions by the UN Security Council, as well as a state's inherent right to defend itself, as laid under Article 51 of the UN Charter.[6]

**(B) Jus in Bello**

*Jus in bello*, on the other hand, is synonymous with International Humanitarian Law ("**IHL**"). *Jus in bello*, also referred to as the "Law of Armed Conflict", is usually derived from international treaties and conventions, such as the Geneva and Hague conventions, and from practices which are recognized as part of the customary international law. The principles which are derived from them are used to govern the use of force during armed conflict.[7] The three main guiding principles used to establish a framework for determining the legality of conducting a cyber warfare operation during an armed conflict are:

- The Principle of distinction which states that attacks should be limited to achieving military objectives and that civilians should not be an object of attack.
- The Principle of proportionality which states that the use of force shall be limited to the objective which is essential to meet an armed attack, while exercising the right to self-defense, and should be proportionate to the danger faced.
- The Principle of Discriminate Attack which mandates the prohibition of attacks that cannot be limited to specific military objectives, and result in civilian causalities.

This suggests that irrespective of whether engagement in conflict is through the means of cyber-space, or through a traditional approach such as kinetic weapons, similar restrictions would entail when the principles of *Jus in bello* or IHL are applied on the same.

## IV. CONCLUSION

As far as cyber warfare is concerned, it is quite evident that it does not exist in a legal void, as it is subjected to established principles of international law, similar to traditional warfare. However, apart from some rare exceptions, such as the African Union Convention and the Budapest Convention on Cybercrime, there are not many regulations in the field of

[5] Charter of the United Nations and Statute of the International Court of Justice . (1945). Retrieved from treaties.un.org: https://treaties.un.org/doc/publication/ctc/uncharter.pdf.
[6] Ibid 4.
[7] Lewis, J. A. (2010, April). A Note on the Laws of War in Cyberspace. Retrieved from Center for strategic & International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.

international law which are specifically created to tackle the issue of cyber warfare and cyber-crime.[8] Even today, there have been demands to create, what some call as the "digital Geneva Convention", to regulate state behavior in the cyber-space. Going forward, it would be important to determine whether the existing framework of international law would be enough to regulate the growing use of cyber-warfare, and if not, then how can effective regulatory system be implemented in this ever-changing arena.

*****

[8] Hollis, D. (2021, June 14). A Brief Primer on International Law and Cyberspace. Retrieved from https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.

 [ISSN 2581-5369]