BLOGS

Applicability of the Principles of International Humanitarian Law to Cyberwarfare Operations

Adtiya Aryan · 01 May 2026

International Humanitarian Law is a branch of Public International Law. It aims to limit the effects of armed conflict by protecting the concerned people. It protects victims of such conflicts such as prisoners of war, civilians, aid workers, and medical helpers. Its primary objective is to protect and prohibit attacks on sick, wounded, and surrendered victims of armed conflict.

One of the prime aspects of International Humanitarian Law is that it puts limits on the weapons and the type of warfare with which the conflict is approached. The two branches of IHL are the Geneva Conventions, 1949, and the Hague Conventions, 1907.

The aspect which needs to be understood here is that IHL aims to limit the violence committed during a conflict, but it does not try to prohibit all violence during the conflict. Moreover, International Humanitarian Law falls short of defining the legality of war. When it comes to cyberwarfare and the application of the principles of IHL, it acts as a challenge due to the dynamic nature of cyberwarfare.

Outlining the Principles of International Humanitarian Law

The principles of International Humanitarian Law surround distinction, proportionality, and attribution.

Principle of Distinction

This principle aims to protect civilians and reduce their suffering during an armed conflict. The same has been codified under Article 48 of Additional Protocol I to the Geneva Conventions, where civilian objectives are distinguished from military objectives.

The principle of distinction of IHL is violated when civilian objectives are intentionally targeted instead of military objectives during an armed conflict. The military objectives are mentioned in Article 52(2) of Additional Protocol I of the Geneva Conventions. It includes all those objectives

which, by virtue of their nature, location, and purpose, make a significant contribution to military action, and this applies to non-international armed conflict as well.

Now, when it comes to the application of this principle to cyberspace in the context of cyberwarfare, it becomes a tedious task. As ‘data’ plays a prime role in any cyberwarfare activity, the question arises whether that data is a civilian object or a military object from the perspective of IHL.

Accordingly, it can be derived that ‘objects’ are those entities that are visible and tangible, that is, which can be attributed with physical properties. Thus, the principle of distinction of IHL cannot be easily applied to cyberspace.

Principle of Proportionality

When it comes to armed conflict, it needs to be understood that civilians and civilian objects cannot be targeted, and if done so, then the principle of proportionality comes into the picture.

It can be conceived through the notion that if, during armed conflict, damage is caused to civilians or to civilian objects, the damage cannot be such which will provide military advantage to the other as per Article 51(5)(b) and 57(2)(iii) of Additional Protocol I of the Geneva Conventions.

If it does so, then it violates the principles of military necessity and proportionality under IHL. It needs to be determined that during armed conflicts, if civilians or civilian objects are attacked, it should not be in disproportionate form.

When it comes to cyberspace, it is important to understand that the principle of proportionality is taken into consideration such that the attacks committed do not violate the notions of IHL.

There exist systems of dual use such that they can be used for military and civilian purposes as well, such as power plant systems, which have the responsibility to supply power to both military and civilian setups.

But when such dual systems are attacked, the application of the principle of proportionality poses a challenge, as there is no distinction between dual systems and their distinct use for civilians and military is not differentiated.

Therefore, the application of the principle of proportionality to cyberwarfare becomes a tedious task.

Principle of Attribution

The principle of attribution can be easily applied in the traditional warfare setup, where all the principles of International Humanitarian Law are applicable altogether.

But when it comes to cyberwarfare, the application of the principle of attribution is not easy. This is because, due to rapid advancement in technology and the ability to hide original identity behind a veil, perpetrators can escape the attribution loop and commit crimes in cyberspace.

There are certain conducts mentioned by the Draft Article for Responsibility of States for Internationally Wrongful Act, 2001, which are attributed to the state, and for such conduct they can be held liable under International Humanitarian Law.

Such conduct is attributed to the following:

1. State organs
2. Persons or entities upon which the State exercises governmental authority
3. Persons or groups acting under the State's control
4. Private persons or groups whose conduct the State adopts as its own

Thus, cyberwarfare committed in cyberspace by any entities or subjects of a particular state will be considered as a cyber activity committed by the state itself.

Subsequently, the state can also be held accountable for violations of International Humanitarian Law.

But there lie certain challenges when it comes to the application of the principle of attribution to cyberwarfare activities. Cyberwarfare is initiated by hiding identity and is committed in different stages, thus making it difficult to establish a link between the line of command and the actions committed in response by one state to another state.

Therefore, the principle of attribution of International Humanitarian Law falls short in dealing with cyberwarfare.

Thus, the principles of International Humanitarian Law fall short of effectively regulating cyberwarfare operations.

Existing Legal Framework

When it comes to understanding cyberwarfare from the lens of International Humanitarian Law, it needs to be viewed from the existing legal framework as well, such as Tallinn Manual (1.0 and 2.0), Geneva Conventions, and their Additional Protocols.

Tallinn Manual (1.0 and 2.0)

The Tallinn Manual is considered to be the first comprehensive effort at the international level to apply IHL to cyber conflicts.

It was commissioned by the NATO Cooperative Cyber Defence Centre of Excellence. However, this manual does not have a binding effect, but it comprises expert opinion to deal with the application of IHL to cyber conflicts.

The Tallinn Manual 1.0 was produced in the year 2013 and exclusively dealt with the topics of sovereignty, state responsibility, and International Humanitarian Law.

However, this manual failed to include military cyber operations which occur outside the purview of armed conflict.

It states that the use of force by cyber conflicts qualifies to be recognized within Article 2(4) of the UN Charter when their effects are comparable to a traditional warfare setup.

The manual provides a scale and effects test, which puts forward that if cyberattacks cause large-scale destruction, death, or injury, then they would fall within the arena of armed attacks.

This motion will trigger the right of self-defense as mentioned under Article 51 of the UN Charter.

Apart from this, Tallinn Manual 1.0 puts emphasis on the principles of proportionality and distinction of IHL.

On the other hand, Tallinn Manual 2.0, produced in 2017, made an effort to engage with the peacetime regime and governing issues of cyber operations, sovereignty issues, state responsibility, and human rights.

Thus, Tallinn Manual provides a comprehensive outlook on how cyberwarfare operations are handled under the purview of international law.

It discusses how the principle of sovereignty and non-intervention applies to cyber operations.

Geneva Conventions

The Geneva Conventions of 1949 apply to cyber operations that take place during an armed conflict.

The First and Second Geneva Conventions protect the sick and wounded, and shipwrecked members of armed forces respectively.

Thus, during cyber conflicts, when such medical units and facilities are targeted, they violate the above-mentioned conventions.

When it comes to the application of the Third Geneva Convention, it applies in the case of treatment of prisoners of war.

Article 4 of the Third Geneva Convention will be applicable if cyber operations were conducted openly and under command, and while doing the same the individual gets caught by the adverse party.

Lastly, the Fourth Geneva Convention governs the comprehensive protection of civilians in times of conflict.

Cyber operations that deliberately target civilians, their infrastructure, and cause distress and panic violate the Fourth Geneva Convention.

Additional Protocols

Additional Protocol I to the Geneva Conventions was adopted in 1977 and acts as a supplement to articulate the principles of IHL to cyber operations and deal with them in a specific manner.

Article 49 of Additional Protocol I talks about attacks and states that they are acts of violence whether committed in offence or defense.

But whether such acts of violence must be physical or not has been left open to interpretation.

Moreover, Article 52(2) defines military objectives as distinct from civilian objectives.

Lastly, Article 51(4) states that indiscriminate attacks need to be prohibited as they inevitably destroy civilian infrastructure.

When it comes to Additional Protocol II, it applies to non-international armed conflict.

It acts as a guarantee of protection for persons who are not part of hostilities.

It can be seen that the existing legal framework tries to bridge the gap between cyberwarfare and the principles of International Humanitarian Law.

This can be understood in the following ways:

Article 2 of the Geneva Conventions: There is no mention of any specific form of force which can be opted for during armed conflict. Thus, this opens space for nation-states to opt for cyberwarfare.

Article 36 of Additional Protocol I to the Geneva Convention, 1977: This states that parties must ensure that any deployment of new weapons is in line with International Humanitarian Law.

Thus, it makes it mandatory for nation-states to be vocal and transparent about the use of cyberwarfare tactics.

Conclusion

There has been rampant advancement in cyberspace, and one such development is cyberwarfare.

The lack of a comprehensive legal framework and the inadequacy of the principles of International Humanitarian Law to deal with cyberwarfare act as limitations in protecting civilians and infrastructure during armed conflict.