Volume 13, December 2020 ISSN 2581-5504

"The Efficacy of International Humanitarian Law in the Era of Cyber Warfare: A Legal Appraisal"

R. Chandrasekar
Assistant Professor
Saveetha School of Law,
Saveetha Institute of Medical and Technical Sciences (SIMATS),
Chennai

ABSTRACT

Cyber technology has witnessed tremendous developments in recent times. It has posed a jurisprudential and technological challenge in the field of International Humanitarian Law (IHL). For instance, the men fighting in the land had moved to fight on the Chariots; stirrups are replaced with the horsemen; the invention of gunpowder and cannon. In this line, cyber armed conflict is a new phenomenon in the field of IHL. The study that deals with the internet-based warfare is known as cyber warfare. This method of warfare, if not regulated, would cause severe damage to every quarter. For instance, the Hiroshima and Nagasaki incidents (considered to be an innovation during those times) have proved how notorious an invention could turn. Robotic technology could be in those lines. These robots could harm the civilians due to its weak-reasoning capacity. Similarly, the application of technology to harm the internet facilities of another State could amounts to armed attack (2008 South Ossetia War). This would amounts to the violation of the principle of the prohibition of use of force. However the IHL is capable to function effectively with the already existing instruments, it still requires proper regulatory mechanism. The reason could be that, for instance, the issues of jurisdiction and attribution in the cyber warfare place a notable challenge in the IHL. Therefore, this paper deals with the challenges that are prevailing in the IHL, in order to find out whether the IHL possessed the capability to coup up with the recent technologies or not.

Key words: International Humanitarian Law, Cyber Armed Conflict/Warfare, Changing Technologies in IHL, Tallinn Manual, Issues of Jurisdiction and Attribution.

INTRODUCTION

Cyber technology has witnessed tremendous developments in recent times. Due to a distinct low-cost advantage, States are much interested in developing it. For instance, technologies related to domestic appliances are changing rapidly. The old ones are outdated, and it is replaced with highly urbane machines.[1] Likewise, since ancient times, the technologies in armed conflicts

* This piece of work is an improvised version of a unit from Chapter V of the author's PhD thesis titled, "Normative Status of the Principles of International Humanitarian Law: A Critical Legal Appraisal".

Volume 13, December 2020 ISSN 2581-5504

have witnessed massive changes, such as the men fighting in the land had moved to fight on the Chariots; stirrups are replaced with the horsemen; the invention of gunpowder and cannon – also, these changes had marked the place for the rise of the nation-States.[2]

Another grave innovation in the technology of warfare is the atom bomb, through which the effects have been marked deadliest ever in the history of modern warfare. Similar to the atom bombs are nuclear weapons that could be bowed through different means - land, air and sea. At present, numerous technologies have emerged which are not easily understood by a lay person. Those changes or innovations are expected to develop constantly until the existence of human beings, which, in turn, could even question the future of mankind. Notably, IHL at present tend to face jurisprudential and technological challenges to cope up with these innovations.

Primarily, the developments in the technology of warfare, *i.e.*, robots and artificial intelligence in the warfield, have posed a threat to the "principle of distinction" in the first phase. It is unclear whether robots could identify or differentiate the non-combatants from combatants due to its artificial reasoning capacity. In addition, the technology employed for civil purposes is worth capable to be used for military purposes. This intertwined use of the technology could question the very aspect of the legitimization on the status of the Parties to the war. For instance, the 2008 South Ossetia War between Russia and Georgia had declared the criminal hacker organization - Russian Business Network - as combatants for the reason that they had attacked the internet facilities of Georgia.[3] In the present digitalized world, such attacks could happen even in the absence of declared war. Similar attacks on the internet facilities would serve as a major factor to cause conflict/war. In this situation, there arises series of questions - whether hackers being civilians, could be considered combatants? Whether they could be punished for their acts? And, would not be the principle of distinction stand violated, in case an attack taking place? This technological-play occurring during peacetime would likely be resulting in war.[4]

[1] For instance, the television used before three decades had to be fixed with antennae on the roof of the house. Later, it was replaced with the portable antennae on the top of the television itself. Nowadays, there is no need for antennae and it is replaced with a set-top box. It is expected that in future, this would also be changed. The technology of the television has been changing day by day according to the needs of the society. Infact, even in smart phones the features showing programs of television are available. People are watching television serials, movies, hearing songs, etc., in smart phone itself.

[2] Empires, who had got emerged with the help of gunpowder and cannon, were the Turkish Ottoman Empire; the Safavid Empire of Persia; the Mughal Empire in India; the Russian State; Spain, the Spanish New World; etc. These nations-States were known as the 'gunpowder empires'. *See*, Allenby, Braden R. (2014), "Are New Technologies Undermining the Laws of War?", *Bulletin of the Atomic Scientists*, Sage Publications, Vol. 70, No. 1, p. 21; available at: https://journals.sagepub.com/doi/abs/10.1177/0096340213516741 (accessed on 11 February 2017).

[3] *Ibid*. p. 27.

[4] There are also chances of negotiations. But in the context of political relations between the two States, Russia and Georgia, there are minimal chances for negotiations. States may contest that these hacking attacks would amount to the violation of sovereignty.

Volume 13, December 2020 ISSN 2581-5504

Also, it amounts to the violation of Article 2 (4) of the UN Charter.[5] The result would obviously lead to serious ramifications in the international relations.

The study that deals with such internet-based warfare is known as cyber warfare. To understand the cyber warfare, firstly, it is pertinent to look primarily at what cyberspace would mean. This paper would, in the first phase, address the law on cyber space, the emergence of norms and the role of scholarly institutions; secondly, the efficacy of the existing principles of the IHL that includes the definition of the cyber attack, *Tallinn Manual* and the principle of distinction; thirdly, Challenges in the identification of the perpetrators, such as the issue of jurisdiction and cyber attribution in the event of cyber attack taking place; finally, this paper concludes with the findings of the paper.

TOWARDS INTERNATIONAL CYBER LAW

States are engaged to enact laws to curb the threats caused by cyber attack, cyber crimes and cyber espionage.[6] To note, internet-related crimes are increasing rapidly. Among others, one significant reason for such increase could be the viability. It has become easy to commit an offence abroad without being present physically. The cybercriminals not only perpetrate crimes locally but also internationally, which could cross beyond the boundary of one State. Apart from the material damage caused, it hinders the relationship between States. For instance, an individual in Asia could wage a potential *virus* thus attacking any communication system in Europe. Such cyber-activities require strict prosecution and punishment. In international law, there is a lack of certainty about the application of international legal paradigms that, in turn, causes difficulties in adopting a concrete set of rules.[7] Therefore, there is a need for regulating the conduct of internet-related affairs worldwide. Such regulations could be made possible through the intervention of the United Nations (UN) or by concluding multilateral agreements between States.

Every field in international law is operated through computer-based technology. Hence there is a need to regulate the affairs of cyber technology under the domain of IHL. In this regard, whether there is a need to revitalize the instruments of IHL due to the changing technology? Or the existing norms are sufficient to tackle the situations?

[5] Article 2 (4) of the UN Charter read as: "All Members 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 inconsistent with the Purposes of the United Nations."

[6] Weissbrodt, David (Summer 2013), "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage", *Minnesota Journal of International Law*, Vol. 22, No. 2, p. 347; available at: https://heinonline.org/HOL/P?h=hein.journals/m jgt22&i=36 3 (accessed on 30 May 2019).

[7] *Ibid*. pp. 348-349.

Volume 13, December 2020 ISSN 2581-5504

Cyber Space Law and the Emergence of Norms

Cyber Space law is the recently emerged notion in domestic as well as in international arena. An increasing number of States have legislated laws to regulate the affairs of internet-based activities. Parallelly, in international law, cyber law is still seen as an evolving jurisprudence. As a result, there prevails no concrete solution to punish the culprits committing crimes from other States. Often the situation results in the rival relationship between the States concerned. International regulatory mechanism is the need of the hour. In the international forum, efforts have been initiated to put the cyber-related affairs under the ambit of international law. These efforts or evolution could be divided into four stages. Ma Xinmin has mentioned the growth of cyberspace law into four distinct stages.

The first stage could be traced through the foundation of the formulation of legal strictures. The groundwork is laid down through the "World Summit on the Information Society" (WSIS). The United Nations General Assembly (UNGA) on 21st December 2001, had authorized the convening of the WSIS in two stages *viz.*, the Geneva Phase (2003) and the Tunis Phase (2005) in which four significant documents had been discussed namely, "Geneva Declaration of Principles, the Geneva Plan of Action, the Tunis Commitment and Tunis Agenda for the Information Society".[8] These instruments have marked the initial stage of the evolution of cyberspace in international law.

The second stage is said to have attempted to bring the issues related to cyberspace under the purview of general international law. To be noted, until this stage, the laws of cyberspace had been considered within the State's internal jurisdiction. Therefore, the UNGA First Committee had set up the "Groups of Government Experts" (GGE) to fix the cyberspace related issues under the ambit of the general international law. So far, the UNGA had formed four GGEs to look into the issues of cyberspace, such as the threats from cybersphere and the practical measures to address them.[9] The forth GGE had made clear that "states must observe, among other principles

[8] Xinmin, Ma (2016), "Key Issues and Future Development of International Cyberspace Law", *China Quarterly of International Strategic Studies*, Vol. 2, No. 1, pp. 120-121; available at: https://www.worldscientific.com/doi/pd f/10.1142/S2377740016500068 (accessed on 10 September 2018). These four documents specifically mention that the, "[p]olicy authority for internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international internet-related public policy issues". On December 2015, a high-level meeting had been conducted by the UNGA to review the implementation of the four documents. Again it is expected that the UNGA will conduct similar meeting in 2025.

[9] To be noted the third GGE has been concluded with the statement that the UN Charter would be applicable to the cyberspace. Also, the third GGE has held that "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to the conduct of states – ICT related (Information and Communications Technology) activities and to their jurisdiction over ICT infrastructure - within their territory". Though the committee had submitted their report in 2013, it has been brought under the UNGA resolution in July 2015 only; *Ibid*. p. 121. For this purpose the UNGA has adopted a resolution. *See, The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res. (2015), UN Doc.

of international law, state sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States".[10] The principles mentioned above are already taken place in the UN Charter. However the UN Charter speaks mostly on the principles of general international law, observations derived by the fourth GGE are considered a viable jurisprudence to which States do respect. Moreover, bringing the cyberspace under the ambit of the UN Charter is considered an essential requirement.

The third stage is crucial for the implementation and enforcement of cyberspace laws. On the request of the UNGA (UNGA Resolution 46/152), the Economic and Social Council (ECOSOC) through its resolution 1992/1 has established "The Commission on Crime Prevention and Criminal Justice" (CCPCJ).[11] Through this commission, the "United Nations Expert Group on combating Cybercrime" has been formulated according to the "Salvador Declaration". This got adopted in April 2010 at the 12th "United Nations Congress on Crime Prevention and Criminal Justice". Its primary function is to study the cyber-related crimes.[12] Since this digital era could produce increasing number of criminal activities that turn to be the reason for the conflicts, it has become necessary to lay down strict measures against those crimes. This stage is considered reaching a milestone to curb internet-related crimes.

The fourth stage is considered a controversial step in the evolution of the cyberspace law. On December 2012, The International Telecommunication Union (ITU) has convened the "World Conference on International Telecommunications" (WCIT) at Dubai to amend the "International Telecommunications Regulations" (ITRs).[13] In this regard, WCIT had been faced with the proposal by the developing countries for amending the treaty concerning the "internet governance and cybersecurity" to promote equal internet management by national Governments irrespective of being developing or developed countries.[14] The above proposal is considered to be the reason behind the controversy prevailing among the developed countries. The developed countries had felt that there will be unnecessary interference of the cyberspace regime into their national jurisdiction. This had halted the socialization of the cyberspace governance to some extent. Still, unprivileged States strive constantly to bring the entire cyberspace under the ambit

A/70/174, pp. 1-17; available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed on 14 November 2018).

[10] Xinmin, Ma (2016), at *note n.* 8, at p.121.

[11] *Ibid*. p. 122.

[12] *Ibid*.

[13] *Ibid*. To be noted that, ITR, a binding treaty, was incorporated in 1988.

[14] Despite the opposition from the US and other Western Countries the amendment has been adopted and came into force on January 2015. Apart from these four major stages, the cyberspace law has witnessed an increasing number of other developments through other sources. Other institutions that have been working in cyberspace related issues are ICRC, United Nations Institute for Disarmament Research, Shanghai Cooperation Organisation (SCO), Asian-African Legal Consultative Organization (AALCO), etc. The Group of Twenty (G20) for the first time has witnessed the agenda brought up before it by Turkey in relation to the cyberspace issues. The agenda has discussed issues that include cyber espionage, the applicability of international law in cyberspace and the United Nation's role in the cyber rule-making process; *Ibid*. pp.122-123.

Volume 13, December 2020 ISSN 2581-5504

of a single regulatory mechanism. Even though the claims of developed countries are worth measurable, such cyber-related crimes, when it could perpetrate from one corner of the world to other causing severe consequences, must be tackled effectively. It becomes necessary to bring the cyberspace regime under an inter-Governmental organization.

Role of Scholarly Institutions

Scholarly institutions are among those who have also contributed to the development of the law of cyberspace. Academicians who contributed for the law of cyberspace, also, have a close scrutiny on the Law of Armed Conflict (LOAC). The noted work of the scholars are: (1) after convening several rounds of round table conferences by the International Institute of Humanitarian Law, the group of naval experts had concluded the "San Remo Manual on International Law Applicable to Armed Conflicts at Sea" (1988-1994); (2) The Harvard University's Program on Humanitarian Policy and Conflict Research has contributed "the 2008 Draft Manual on International Humanitarian Law in Air and Missile Warfare"; (3) The McGill University (Canada) has come up with the "Manual on Armed Conflicts in Outer Space"; (4) the influential document of "Tallinn Manual on the International Law Applicable to Cyber Warfare" has marked the presence of armed conflict-related issues in the cyberspace law.[15]

Above all, the noteworthy contribution is the *Tallinn Manual* (2013), which was developed by a group of independent legal scholars or experts and coordinated by the "NATO Cooperative Cyber Defense Centre of Excellence".[16] This manual deals with issues, to mention few, the law of State responsibility and definitions pertaining to it that include the definition for cyber-attack.[17] Again in February 2016, *Tallinn 2.0* was launched with the assistance and participation of legal experts belonged to various continents and Governments, which focused on the peacetime cyber activities.[18] Having those instruments prepared by the international scholars on the subject of armed conflict-related cyberspace law, they are considered only a soft law. However, it serves as a guiding factor for the States in understanding the concept of armed conflict with reference to the cyber law. Also, the significant contribution of the scholars is considered remarkable towards the development in both the cyber law as well as in the LOAC.

EFFICACY OF THE EXISTING PRINCIPLES

One of the significant reasons for why the cyberspace law is emerging would be the gradual rising of the internet-related crimes, *i.e.*, cybercrimes or attacks. To curb these crimes,

[15] *Ibid*. p. 123-124.
[16] Camino Kavanagh (2017), "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century", *The United Nations Institute for Disarmament Research (UNIDIR)*, p. 33; available at: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (accessed on 01 July 2019).
[17] *Ibid*. pp. 33-34.
[18] *Ibid*. p. 34.

Volume 13, December 2020 ISSN 2581-5504

increasing researches have been conducted by the UN agencies, non-Governmental organisations (NGOs), and so on. This part deals with the development of the cyber laws that have relevance in the field of IHL.

Definition of the Cyber-Attack

Hathaway has defined the cyber-attacks as the activities performed to destabilize the operations of a computer network for political and national security.[19] In view of the above, cyber-attacks are perpetrated to seek political gain or to protect one's national security. Such attacks can be performed by series of actors, such as the States, non-State actors, individual citizen, or programmed automated robots. Those attacks are considered capable to strike the information and communication systems of a State, either military or civilian facilities. Similarly, in 2009, the US National Research Council has defined the cyber-attack as they are "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks".[20]

It appears apparent from the above connotations that the cyber-attacks could happen within a State or beyond thus interfering in one's territorial integrity. In this regard, Article 2 (4) and 51 of the UN Charter is considered applicable to cyber-attacks even it has not been explicitly mentioned.[21] However, there is a conflicting view on the application of Article 2 (4) of the UN Charter to the concept of cyber-attack. This is due to the fact that the concept of cyber-attack has emerged during the late half of the 20th century (turned to be an *Ex-Post Facto Law*).

Tallinn Manual and Use of Force

Though framed by the international group of experts, the *Tallinn Manual* is considered as a guiding factor for the cyber-related issues in international law.

Rule 11 of the 2013 *Tallinn Manual* provides that:

> "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".

At the same time, Kosmas Pipyros raised the issue, in case, any death, injury or damage to the property had not taken place. For this, the majority of the international cyber specialists in the field have stated that Article 2 (4) of the UN Charter could be applied to any category of the use

[19] Pipyros, Kosmas et al. (2016), "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare", *Information & Computer Security*, Vol. 24, No. 1, p. 39; available at: http://dx.doi.org/10.1108/ICS-12-2014-0081 (accessed on 24 February 2017).
[20] *Ibid*.
[21] In May 2011, the United States Department of Defense has held that the LOAC could be made applicable to cyber-warfare (or attack) thus would attract both Article 2(4) and Article 51 respectively of the UN Charter. *See*, Weissbrodt, David (Summer 2013), at *note n*. 6, at p. 356.

Volume 13, December 2020 ISSN 2581-5504

of force that has not approved by the UN Charter; also the phrase "other manner" would specify the cyber-attacks.[22] But the above interpretation is considered untenable. During the time of negotiation of the UN Charter, there was no such concept of cyberspace existed. This branch of law had emerged approximately only after thirty years from the establishment of the UN Charter. There prevails chaos that the drafters would have had any idea regarding the cyberspace during the time of drafting Article 2 (4) of the UN Charter. If this is considered in affirmation, punishing the culprits on the basis of UN Charter is against the fundamental precepts of the criminal justice system, *i.e.,* one should not be punished for the non-established rules at the time of occurrence of the crime. The so-called offender cannot be punished retrospectively. The alternative way to prosecute the attackers could be made possible through having a separate treaty between the States (or) concluding binding treaty and establishing an independent tribunal. Or else, amendment has to be made to Article 2 (4) of the UN Charter to bring cyber related crimes under its ambit.

It is also pertinent to look into the instruments of IHL to curb cyber-related crimes. For instance, as per the Geneva Conventions, killing civilians are prohibited. In the strict sense, by whatsoever manner it may be, either through cyber warfare or conventional warfare, the killing of civilians is considered a prohibited act. While the deaths of the civilians are caused due to the cyber-attack, it amounts to the violation of IHL. But, it is difficult to prove the involvement of the alleged State due to the lack of mechanism. There is a need to establish a concrete regulatory mechanism to deal with the cyber warfare.

Striking the opponent through the means of cyber-weapons would cause severe damage to every quarter. These attacks can affect not only the military facilities but also the facilities of civilians. Such attacks would violate the principles of IHL, such as principles of distinction, humanity, necessity and proportionality. As a precaution every State must prohibit such attacks.

Principle of Distinction

An ample example would be the penetration of *malware* or *virus* into the targeted communication facilities. These *malware* or *virus* could be perpetrated into the computers belonging to sensitive or confidential departments (for example, defence) of the enemy State through the internet. This act tends even to collapse the entire communication system of a State. The act of attacking the whole communication network of a State's sensitive internet facilities is considered as a violation of IHL principles, *i.e.,* it violates the principle of "the prohibition of perfidy", especially the principle of distinction. The origin of the place of attack and its perpetrator could not be traced as it might have been waged from any corner of the world. Likewise, the target is not accurate as it might kill the non-combatants. Therefore, the technologies that are invented in every walks of human life turn to be the reasons for war.

[22] Pipyros, Kosmas et al. (2016), at *note n.* 19, at p. 44.

Volume 13, December 2020 ISSN 2581-5504

For instance, State A possesses nuclear-capacitated facility where researches are conducted. Considering, for the sake of civil purpose, the facility has been constructed with the latest communication technology. Now State B has an aggressive relationship with State A and the former needs to destroy the nuclear facilities of the latter as revenge. To this effect, State B employed its officers or hired an individual who is highly capable of handling the complex technology. He, then, attacked on State A's facilities, and finally, he succeeded. As a consequence, the said nuclear facility is exposed to the cyber-attack. This case would be a clear case of cyber-attack. The issues here appear to be whether individual acts would amount to armed attack? Whether the concerned individual who causes the attack would be considered as a combatant? Whether he could be identified? (Or) Is there any advanced technology to find the perpetrator from where he had attacked? To find out whether a concerted attack amounts to a cyber-attack, the above said issues have to be resolved.

In general, a simple cyber-attack will not constitute an armed attack. To constitute a cyber armed attack, it has to satisfy the requirements of the principle of distinction. Article 48 of the Additional Protocol - I (AP-I) to the four Geneva Conventions, 1949 read as follows:

> "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations against military objectives."

The basic requirement of the principle of distinction is that the Parties should distinguish the civilian population from the combatants. In case if the civilians are attacked, then this provision is considered as violated. Whenever an attack is carried out against the military objectives and, in consequence, if the civilians are attacked, it is regarded as a violation. To be noted, a computer *virus* attacking the military internet-facilities could affect the civilians too.[23] The said attack is considered a cyber armed attack. Another issue could be the 'individual found to be a combatant' or not. Article 50 (1) of the AP-I mentions that if in case a doubt arises as to a person caught in the hands of the adversary is whether a civilian or not, such person has to be considered as a civilian only. Similarly, for civilian objects used for military purposes, Article 52 (3) of the AP-I states that

> "In case of doubt whether an object which is normally dedicated to civilian purposed, … it shall be presumed not to be so used" (Emphasis omitted).

[23] Dinstein, Yoram (2012), "The Principle of Distinction and Cyber War in International Armed Conflicts", *Journal of Conflict & Security Law*, Vol. 17, Issue 2, p. 262; available at: https://heinonline.org/HOL/P?h=hein.journals/jcsl17&i=265 (accessed on 30 May 2019).

Volume 13, December 2020 ISSN 2581-5504

Yoram has rightly pointed out that "in any event, the presumption can be rebutted when additional information is factored in".[24] In the above circumstances, an individual, even though considered to be a civilian, uses his personal computer or laptop around the military facilities for the purpose of military engagements he could be regarded as a combatant.[25] Therefore, all the cyber-attacks would not constitute an armed attack. To satisfy the requirements of a cyber-attack, the said attack should attract the principle of distinction. In case, if there found the violation of the principle of distinction, subsequently, similar breaches could follow, such as the principles of proportionality, discrimination, perfidy, etc.

CHALLENGES IN THE IDENTIFICATION OF THE PERPETRATORS

On the above-mentioned incident, other challenges are identified. Firstly, the facilities are filled with nuclear energy. Secondly, if any leakage appears as a result of such attack, then it causes severe damages to State A. Even, such attacks could impact neighbouring States or spread across continents.

The occurrences of the cyber-attack could produce victims of all kind ranging from civilians, Governmental institutions, hospitals, courts, education and research institutions, etc. Since the impact of the exposed nuclear facility seems to be colossal, primarily, it seems difficult to identify from where the attack is initiated. Though identifying the place of attack (the exact location of a cyber-attack), there exist no proper forum to complain. Even though there exist implicit understanding of the culprits, those cybercriminals could not be punished as any definitive evidence could not be produced. Even, the judges who know this particular branch of law are scarce. For instance, considering it has happened between the States that were already engaged in an armed conflict, then there arises, in particular, two challenges as to how the culprit could be tried before the courts (issue of jurisdiction), and how could the culprit be found (issue of attribution).

The Issue of Jurisdiction

The jurisdictional issue places a difficult challenge while an attack is committed. This jurisdictional issue has put the enforcing mechanism of a State into a complicated situation. As a result, States are handicapped to prosecute those criminals who performed such cyber-attacks from other States. For instance, considering a cybercrime committed from one State against other. Purposefully, a separate Agreement is required to be concluded between the States. Since the issue is considered universal, there is a need for every State to conclude a multilateral-treaty on this jurisdictional issue.

[24] *Ibid*. p. 264.
[25] *Ibid*.

Volume 13, December 2020 ISSN 2581-5504

Cyber-attack related to the armed conflict creates a major jurisdictional issue among the States. Even to say, a concerned State may be held responsible for an attack committed by an individual or a non-State actor found under its jurisdiction, it is difficult to prove such involvement accurately.

The first *Tallinn Manual*[26] is considered as the only instrument that serves as a guiding factor to take cognizance of the extra-territorial jurisdiction. Rule 2 of the said Manual mentions as:

> "Without prejudice to applicable international obligations, a State may exercise its jurisdiction: over persons engaged in cyber activities on its territory; over cyber infrastructure located on its territory; and extraterritorially, in accordance with international law."[27]

Though this rule has paved the way for the extraterritorial jurisdiction, still it has to receive wide recognition from States.

The Issue of Cyber Attribution

Cyber Attribution has been defined as, "… the process of tracking, identifying and laying blame on the perpetrators of a cyber attack or other hacking exploit".[28] States could initiate this process of attribution to investigate and extract the complete picture of the attack, thus producing the perpetrators before justice.[29] However, the attackers may not be identified as they could even hide their source of operation.[30] Identifying the perpetrators and producing them before the court of law is complex in nature. The cyber-attackers who are highly capable in handling the cyber activities could deceive the source of attack. The culprits may hide their place of attack and could place evidence as if the attack is perpetrated from other State. This, in turn, could attract the provision related to the prohibition of perfidy. In such a situation, it has become difficult to trace the source of crime. Even in case if caught, the assistance to share the information regarding the crimes would be a complex issue. For instance, a bilateral "Mutual Legal Assistant Treaty" concluded between Estonia and Russia in assisting each other with the information had proved to be inadequate.

[26] Though both the *Tallinn Manuals* are not binding on the States (as it is prepared by the international experts on the subject), it is expected that in the future, would turn to be an authoritative source for international cyberspace law. Notably, they are prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

[27] Schmitt, Michael N. (ed.) (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press, p. 18.

[28] Rosencrance, Linda and Haughn, Matthew (last updated: October 2017), "Definition: Cyber Attribution", *SearchSecurity*; available at: https://searchsecurity.techtarget.com/definition/cyber-attribution (accessed on 20 November 2018).

[29] *Ibid*.

[30] Also, the attackers would use another computer (IP Address) to commit the crime. In fact, there is no definitive or accurate cyber attribution possible till date; *Ibid*.

Volume 13, December 2020 ISSN 2581-5504

On 27 April 2007, computer facilities of the Estonian Government, such as banking, media and other businesses had been hacked and attacked (cyber-attack) which caused huge loss and damage.[31] Estonia could however manage to identify the perpetrators, such as the "bot net herders", individuals and the involvement of Russia behind the attack.[32] Having concluded a "Mutual Legal Assistance Treaty" between the two States, Russia refused to provide assistance or information to Estonia to conduct investigation.[33] The above-said incident could set an example of how the cyber-attack cases have been proved inadequate (in spite of having a bilateral treaty between the States). In 2013, Atlantic Council has proposed the convening of a "Multilateral Attribution and Adjudication Council" as an international agency that could tackle the issues of illegal cyber-attacks by States as well as "adjudicating associated interstate disputes".[34] Due to the fact that it requires intelligence and forensics reports, States were reluctant towards the proposal.

States need to take precautionary measures to tackle this situation at the domestic level. In the advanced cyber-legal order, each State has a moral responsibility to curtail these attacks, and if not checked, the consequences would be severe.

CONCLUSION

IHL is highly capable to face the contemporary challenges in an effective way. However, it is not a denial that there exists jurisprudential gap. In order to cope up with the changing technologies, this branch of international law is required to travel more to find a concrete solution to the issues, such as cyber terrorism, cyber crimes, cyber warfare, etc. In this regard, the WSIS, GEEs, CCPCJ and WCIT under the ambit of UNGA are earnestly working towards the development of the norms of cyberspace law. It has to be noticed that an increasing number of treaties have got recognized after several years of discussions, even, more than a decade. For example, the debates on the instruments, such as Vienna Convention on the Law of Treaties, International Covenant on Civil and Political Rights, International Covenant on Economic Social and Cultural Rights, United Nations Convention on the Law of the Sea, World Trade Organization, etc., had taken place for several years. In view of the above, jurisprudence of cyberspace related to armed attack/conflict is expected in the near future to serve as a guiding factor for the IHL.

[31] Goodman, Will (Fall 2010), "Cyber Deterrence: Tougher in Theory than in Practice?", *Strategic Studies Quarterly*, Vol. 4, No. 3, p. 110; available at: https://www.jstor.org/stable/10.2307/26269789 (accessed on 01 July 2019).
[32] *Ibid*. p. 111.
[33] *Ibid*.
[34] Camino Kavanagh (2017), at *note n*. 16, at p. 34.