MSB-INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH
Associating Researchers; Nourishing Innovation
Peer Reviewed
Vol. 2, Issue 3, March 2024-July 2024
22-30, MSB-IJIR

An Approach Towards Applicability of International Humanitarian Law on Cyber Attacks: A Critical Appraisal

Siddharth Sanjay
B.A. LL. B
Amity Law school
Amity University, Lucknow
Dr. Axita Srivastava, Ph.D.
Assistant Professor
Amity Law School,
Amity University, Lucknow

Abstract

The digital and technology era has given rise to a variety of interdisciplinary perspectives on how innovations affect lifestyles due to the capabilities for communication, particularly through social media. Digital technology does provide advantages, but there are also disadvantages, most notably the risk of cybercrime. This study attempts to systematically comprehend cybercrimes, their effects on society, and the difficulties they present. It is based on secondary data. The scholars will talk about the growing ways that cybercrimes are committed as well as the benefits and drawbacks of the digital age. In this study paper, several facets of cybercrimes will be covered in detail.

Keywords: Cyber-crime, Digital criminology, Digital society, Cyber space.

Introduction:

Crime in today's time is a growing social and legal problem around the world that we live in and growing population is an essential factor that influences the rate of crime across the globe. Constantly developing science and technology has endless advantages for the people of developing cities and countries, throughout the world however, there are darker sides of it too. The criminal activity such as misuse of the Technologies and playing with someone's data and privacy is also increasing day by day with the population growth. The number of Cyber-crimes is also increasing day after day in a larger quantity. The Rate of Cyber Crime has shown a big increase during and after the pandemic period as almost every work was done on the internet. Work from home has also given opportunity to the hackers to be active and work on their internet servers by hacking the network of people working online 24x7.

Cyber Offenses are the Offenses that are committed by an individual or group of people against anyone using the internet facility across the world. The criminal intention of harming the reputation of someone, defamation, or any kind of mental torture or physical harm to any individual directly or indirectly, using the internet mode or telecommunication network services may it be Internet, SMS, MMS, Emails, Phone calls, etc, comes under cyber-crimes. Cyber-crime search as fraud, hacking, phishing, identity theft, etc, has increased dramatically a lot in last few years. India had a 50 percent increase in the number of cyber-attacks last year during the pandemic period.

Cyber Crime Definition

A general definition of cyber-crime maybe as below:

'An unethical/unlawful act where did computer is involved or any internet source is involved which can harm any individual, groups or community by any illegal criminal activity is known as cyber-crime.' (Roshan,N., 2008)

Reasons behind the cyber crimes

There are various reasons why the cyber-crimes getting so much increase across the world, few of them are mentioned below:

For the sake of money

For the sake of popularity

No concrete regulatory measures on cyber crimes

Limited coverage of Media

Corporate cyber-crimes are done mostly committed by the group not by an individual person.

Classification of Cyber Crimes

There are number of types of Cyber-crimes prevailing in the cyber space, (Ashabhari Thakur, 2019) here the researcher will discuss few of the major categories of Cyber-crime which are given as below:

Crime against individuals

Cyber-crime that are committed against an individual person using internet or any source of Cyber space against whom the type of crimes such as harassment of any use user by the mode of email or not extractions fishing credit card or debit card for traffic in cyber definition hacking the private chats and social media IDs such as Instagram, Facebook, or telegram come under the category of the crime against individuals.

Crime Against Property

Another category of Cyber-crime classification is the crime against property these includes intellectual property crimes or computer vandalism or threatening etc kind of crimes is mostly seen in the financial institutions and an important feature of this crime is that there is very little law available in the cyber laws of India due to which normally go unobserved.

Crime Against Organization

This type of Cyber-crime relates to the cyber-crime against organization. Cyber terrorism is one of the very famous examples of such kind of crime in the world the crime explains that when are human being hats or cracks into the cyber space of government of any country or the military intelligence website of any countries intelligence department cyber terrorism takes birth. This type of crime can be seen in any country across the globe and any system of any intelligence around the world can be cracked due to number of crackers and cyber terrace available in our society.

Crime Against Society

The last classification of crimes in cyber space is the crime against society, in this category cyber forgery web jacking sale of legal articles extortion of data drilling and polluting the youth through various criminal sources available on internet which brain washers the youth and cyber contraband etc, are included in this category.

Mostly the web checkers and hackers game access over the sites and personal data of the youth through the gaming websites and online job fraudulent cases are mostly heard in the society nowadays for the fulfilment of the pockets of hackers due to unemployment in the country.

An Insight of Cyber Laws in India

Digital guidelines are particularly significant in countries like India, where the web is generally used. Digital regulations are set up to control the advanced trade of data, programming, data security, online business, and financial exchanges. India's digital regulations have prepared for e-trading purposes and electronic administration in the country, as well as expanded the extension and utilization of advanced media, by guaranteeing ideal association and diminishing online protection gambles. (Solomon & Co. 2017)

In any case, there are a few hindrances that stroll alongside the current regulations too. There are prevalently four digital regulations that India embraces:

Information and Technology Act, 2000

The IT act, which was enacted in the year 2000, takes care of the Indian Cyber Cell department. The aim of this act is to protect E-commerce trading and networking with legal protection by making it suitable to register real time information with the Government of India.

However, with the generation being technology freak, cyber criminals (hackers & Crackers) being very smart have other ways to misuse this technology, and so amendments are always been made by the government in this act for the improvement.

Companies Act, 2013

This act gave SFIO (Serious Frauds Investigation Office) the whole responsibility to run the Software of Indian Corporate department and protect them from Cyber Frauds.

And they have very strict rules and regulations against the regulations and cyber security to protect Companies from any kind of cyber-attacks.

Indian Penal Code, 1860

IPC along with IT act, 2000 both works together to identify theft or crimes relating to cyber space. The main provisions relating to cyber-crimes seen in general are as under:

False documentation (S-464),

Forgery (S-465),

Defamation (S-469), Etc

Cyber security Framework (NCFS)

This provides standardized approach to the cyber security and includes all the necessary guidelines and regulations for effectively managing the Cyber Related Issues and solves them with the required solutions.

Among all the above-mentioned cyber laws in India, The IT Act, 2000 remains a lot in the discussion when data protection law is being talked about in India.

Dispute Resolution Mechanism under IT Act, 2000

The Information Technology Act, 2000 lays out semi legal bodies, for example, mediating authorities, to determine questions (offenses of a common sort as well as criminal offenses). The mediating official has the locale to grant remuneration as a common cure as well as force fines for disregarding the Act, giving them common and criminal court-like powers. The Cyber Appellate Tribunal is the principal level of allure, with a chairperson and any extra individuals selected by the Central Government. A subsequent allure might be stopped with a High Court having purview in no less than 60 days after the Cyber Appellate Tribunal's decision has been imparted.

Issues with the Dispute Resolution Framework under IT act

The system might look encouraging in principle; however, it has not been as successful practically speaking. There is not really any reportage on a digital question and there is no information accessible on the quantity of cases mediated upon by officials or the court. We have recognized specific issues that feature the lacunae in the framework:

Possibility of orders passed by the Adjudicating officers

They AOs appreciate wide powers. They can settle on infringement of any arrangement, rule, guideline or bearing passed under the IT Act. AOs have some of the time elapsed orders with huge implications. For instance, in one case, an AO expected a bank to take responsibility for

not practicing a reasonable level of effort to forestall phishing. The AO alluded to the overarching RBI guidelines on web banking to come to this end result. In this manner, AOs can assume a critical part in deciphering the IT Act.

There are numerous AOs, who address comparable sort of issues, simultaneously. This outcomes in the issue of clashing feelings on a similar issue. For example, in a case, the AO had held that Section 43 of the IT Act was not relevant to the bank as it was a body corporate. In any case, AOs in different states had held in any case. In different cases, Section 43 has been summoned against body corporates. This can make it challenging for a substance to follow the IT Act, as it might need to consider the assessment of different AOs to work across India.

Need for building capacities for adjudicating cyber offences

There is a need to fabricate the limit of AOs. The Crown Prosecution Service of the United Kingdom has given Cybercrime-arraignment direction This direction has characterized significant sorts of cybercrimes like hacking, virtual entertainment related offenses, and so forth. They give fundamental standards to the settlement of cybercrimes. A direction of a comparative sort ought to be acquainted in India with guarantee better treatment of objections.

Investigation & appreciation of evidences during the process of adjudication

Examination concerning infringement is directed by an official in the Office of Controller of Certifying Authorities or CERT-IN; or by the Deputy Superintendent of Police. Be that as it may, the limit of these bodies to direct digital examinations is problematic.

Most digital offenses are accounted for to the police divisions, as the National Cyber Crime Portal capacities under the space of the Ministry of Home Affairs. Grumblings on this entry are alluded to the police branch of the state in which the claimed digital offense **was** committed. The police staff are not furnished to manage cybercrimes; they might not have the imperative aptitude in regions like digital legal sciences and examination. They frequently designate confidential firms to explore into such matters.

There is no directing report under the Indian administrative system on digital examination or digital criminology. The Information Technology (Amendment) Act, 2008 has laid out a body called the Examiner of Electronic Evidence. This body gives well-qualified assessment on electronic proof. The Meity has delegated different measurable science research centres as the inspector. These research facilities hold mastery in directing digital examination. Be that as it may, the Holding of Enquiry Rules, 2003 have not been refreshed post the approaching of the 2008 revision act. The principles should be altered to empower AOs to request such inspectors to explore into the issues before them. There ought to be rules or standards on the examination of digital offenses to all the more likely prepare the police and other exploring organizations to deal with such cases. For example, the United States Department of Justice had given an aide on 'Electronic Crime Scene Investigation' in 2001. This is an exhaustive aide which sets out examination strategies for various types of digital infringement like fakes, wholesale fraud and so on. A comparable public rule on digital examinations should be given in India. A cybercrime examination manual was sent off by the Data Security Council of India. Steps should be taken by the focal government to inform such rules.

Jurisdiction Issues

Jurisdiction is one of the questionable issues on account of digital wrongdoing because of the exceptionally widespread nature of the digital wrongdoing. With the steadily developing arm of the internet the regional idea appears to evaporate. New Methods debate goal ought to give

way to the customary strategies. Subsequently, the Information Technology Act, 2000 is quiet on these issues. However, Section 75 accommodates extra-regional activities of this regulation, yet they could be significant just when supported with arrangements perceiving requests and warrants for Information gave by capable specialists outside their locale and measure for collaborations for trade of material and proof of PCs wrongdoings between policing. (Ikigai law, 2000)

Applicability Of IHL (International Humanitarian Law) On Cyber Warfare and Its Challenges

The current IHL regime does not specifically address cyber weapons in the way it has banned certain conventional weapons, biological weapons and chemical weapons. However, IHL is an adaptive body of law, which can be deduced from Article 36 of Additional Protocol I to the Geneva Conventions ("API"). This provision, also known as the 'weapons review' clause, requires States to conduct a legal review of a new weapon, means or method of warfare to determine if its employment would be prohibited under international law. It is clear from Article 36 that IHL is not restricted to weapons that were developed at the time when these laws were made. Hence, new and emerging technologies are also bound by the regime regardless of whether they have been directly addressed in the provisions of law or not. So, when States adopt IHL treaties, they agree for these treaties to regulate their present and future conflicts. The International Court of Justice's ("ICJ") Advisory Opinion on the *Legality of the Threat or Use of nuclear weapons* supports this notion, where the court affirmed that the rules and principles of IHL apply to "*all forms of warfare and to all kinds of weapons, including those of the future*". Therefore, as a new means and method of warfare, States are required to conduct a legal review of all "cyber weapons" to ensure compliance with IHL before using them in operations.

It is essential to establish the applicability of IHL to cyber operations as this regime accords various obligations as well as protections during armed conflicts. IHL is only applicable to cyber operations which occur during or in connection with an armed conflict. These conflicts are categorised into international armed conflicts ("IAC") or non-international armed conflicts ("NIAC"). The category of armed conflict determines the rules applicable under IHL, therefore, it is necessary to consider what elements are required for each to determine which rules apply. Moreover, when it comes to cyber operations there are various challenges in determining when either an IAC or a NIAC exists with respect to the application of IHL.

International Armed Conflict

According to Common Article 2 to the Geneva Conventions of 1949, "*the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them*." The Commentary of the Geneva Conventions of 1949 further elaborates that whenever there is a resort to hostile armed force between two states, there is an international armed conflict. However brief or intense this resort to armed forces between States is, it would trigger the application of IHL. Moreover, the law has not prescribed any specific form for the resort to force, therefore hostilities between States may involve cyber operations or any combination of both cyber and kinetic operations. The issue arises when operations by non-state actors or private individuals can be attributed to a State which would render the conflict international. During cyber operations, States often act through private entities in order to preclude direct responsibility. In such situations it is crucial to establish "effective control" of the State over the cyber operation. Therefore, whenever two or more States are involved,

having “effective control” over such entities, it would amount to an IAC, and thus the protections and obligations provided under the Geneva Conventions would be applicable. Such control is more difficult to establish in cyberspace as the location of the perpetrators or the machine from which the attack is launched all may be in different jurisdictions, with responsibility all the harder to establish.

Non-International Armed Conflict

When it comes to a NIAC, the following criteria needs to be satisfied as entailed in the *Tadic case* whereby i) the hostilities must reach a minimum level of intensity; and ii) non-governmental groups involved in the conflict must possess a sufficient level of organisation.

It appears that no cyber-attack by a non-State actor has ever risen to meet the required intensity of violence to trigger a NIAC. Singular and isolated cyber-attacks such as data deft, network intrusions would not launch a NIAC as the requisite threshold of “protracted armed violence” would not be satisfied in such attacks. However, they may occur once a NIAC is already established when they would be part of the hostilities. Another element that needs to be fulfilled is that a NIAC can exist only between parties that are sufficiently “organised” and have the capacity to sustain military operations. For this reason, there must be a distinct armed group with a visible and verifiable organizational structure. This is difficult in cyberoperations which may be conducted through a disorganised group of hackers with little coordination or cooperation with each other.

Regulation of 'Cyber-Attacks' under IHL

As discussed in the previous section, IHL is applicable to cyber operations that take place during armed conflicts, this section will now delve into how IHL regulates cyber operations to ensure that there is no violation of international law. IHL consists of a set of rules and principles, in light of which, various protections are available during armed conflicts. According to the criteria described above to qualify for an armed conflict, either of an international or non-international nature, there must be an attack. Article 49 of API defines ‘attacks’ as “*acts of violence against adversary, whether in offence or defence*”. According to the Tallinn Manual, a cyber-attack is a “*cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*”. There is a general notion that an attack consists of some form of physical damage, however in cyber operations the rights of others may be violated without causing any physical damage. Would this amount to an ‘attack’ in its true sense? According to the ICRC, an operation that leads to disabling a computer or a computer network would constitute an ‘attack’ within the ambit of IHL. Therefore, destruction caused by cyber operations would amount to an ‘attack’ and enable the applicability of IHL on cyber operations. However, some argue that there must be extinguished or reduced functionality due to such an operation for it to amount to an ‘attack’. For instance, the temporary disruption of functionality of cyber infrastructure can lead to death, injury, destruction or damage, such as leading to the crash of an aircraft. As it stands, there is not yet consensus as to whether an attack entails injury, death, damage or destruction or whether the broad approach requiring a loss of functionality would suffice.

Conclusion

As discussed, IHL is applicable to new means and methods of warfare, thus these sets of rules would be applicable to cyber warfare during both IAC and NIAC. Keeping in mind the laws of armed conflict, it is essential to respect the three core principles of IHL i.e. the principles of distinction, proportionality and precaution in an attack. However, when the laws of armed conflict were made, such advanced technologies were not in place, which is why it is the need of the hour to introduce new laws that deal directly with cyber warfare as there persists certain complications with the applicability of the three cardinal principles of IHL during cyber operations.

While IHL is applicable to cyber warfare, its scope is very limited whereby the current IHL regime only requires a legal review to be conducted of such weapons and requires for these 'new means and methods of warfare' to be in compliance with the three cardinal principles of IHL i.e. principle of distinction, proportionality and precautions in attack, the law does not focus on other areas, such as attribution of cyber-attacks. In addition to this, the current war law regime protects civilians and civilian objects from atrocities during armed conflicts, however the same becomes ambiguous when it comes to cyber operations as military and civilian cyber infrastructure are interlinked with each other which makes it difficult to accord protection to civilian cyber infrastructure. Hence, there is a need to introduce a special treaty that deals with cyber warfare in detail while focusing on the findings of the Tallinn Manual regarding the analysis and applicability of IHL on cyber warfare for the purposes of improving cyber security.

Furthermore, focusing on the limitation of the applicability of the principle of proportionality during cyber operations, it is crucial to develop a proportionality standard in a unified international treaty that needs to be observed by parties to a cyber operation in order to avoid lethal cyber consequences. Militaries need to conduct a proportionality analysis before any cyber-attack that may cause incidental damage to civilians or civilian objections. Moreover, militaries must exercise the 'constant care standard' as stipulated in the API when conducting cyber operations even when these operations are not categorized as 'attacks' to protect civilians and civilian infrastructure. Militaries should also consult cyber experts to be aware of the impact of their attacks or operations on a particular system. This will help them determine the level or degree of anticipated harm incidental to the life of civilians or civilian objects. Moreover, nations should take precautionary measures such as providing systems with warning of attacks, training civil defense forces and monitoring networks in order to segregate between civilian objects and military objectives during cyber operations.

References

Ashabhari Thakur, 'Determination of jurisdiction in cyber-crimes- issues & classification', 2019, available at: www.legalpedia.in

Roshan, N., What is cyber-Crime. Asian School of Cyber Law,2008: Access at-http:// www.http://www.asclonline.com/index.php?title=Rohas_Nagpal,

Ikigai law, 'DRM framework of cyber-crimes under IT act, 2000,' available at: www.ikigailaw.com

www.mondaq.com/india/securty/623820/cyber-laws-in-india

Ashabhari Thakur, 'Determination of jurisdiction in cyber-crimes- issues & classification', 2019, available at: www.legalpedia.in

www.cybercrimes.gov.in

www.legalservicesindia.com

www.researchgate.net

Dr. Gregory Laidlaw, "cyber criminology, and cyber-crime: towards an academic discipline", Centre of cyber security and intelligence studies

Shameek Mukhopadhyay, 2015, "cyber law: countermeasure of cyber-crime"
R.R. Choudhary, 2020, "cybercrimes: challenges and solutions" available at: www.researchgate.net
IT act, 2000