THE ROLE OF INTERNATIONAL LAW IN ADDRESSING CYBERCRIME

Legal Upanishad Journal (LUJournal.com)

Vol 1 Issue 3 | November 2023 | pp. 114-123

Vedang Sharma, Law Student, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore

ABSTRACT

The world has connected more than ever in the twenty-first century because of the internet's and technology's rapid advancements. Although there are many advantages to being interconnected, there are also new difficulties as a result, with cybersecurity and criminality being the most pressing. Crimes committed on the internet are no longer limited to a nation's borders, just as the world of the internet has no boundaries. The application of international law to cyberspace has been a hot topic of discussion among nations worldwide in an effort to counter this threat, particularly in light of the difficulty in establishing guidelines for appropriate online conduct. In this article, we shall emphasize how important international law is for cyberspace and understand two areas of international law that show how countries engage themselves in various debates and discussions to reach an agreement. It shall also explore the evolution of cybercrime, its challenges, and its potential to shape the future of digital security.

Keywords: *Crimes, Cyberspace, Digital Security, Internet and Technology.*

1. INTRODUCTION

The United Nations Group of Governmental Experts (UN-GGE) and the Open-Ended Working Group (UN-OEWG) are two entities investigating how international rules can apply to cyberspace, however, there are many conflicts among various governments on these matters. For example, can a cyberattack by one country violate the sovereignty of another country, and if so, how does this work? Is there a rule that says countries should not let their territory be used for bad actions in cyberspace? Can countries take action in response to a violation of international law in cyberspace, and when is this allowed? To answer all of these questions, it is crucial to reach a consensus on important issues to avoid the risk of people exploiting the lack of rules. It's difficult to create an effective legal framework to regulate cyberspace because of constant disagreement and tension. Despite the challenges, the process of countries agreeing on international rules for cyberspace is valuable. The discussions at the UN, even if they are divided, show that many countries are getting involved in a process that is becoming more open, inclusive, and global. It will take time to figure out what counts as customary international law for cyberspace. However, by getting many countries involved in the UN processes, having them share their views, and building their legal expertise in this area, the debate is making some progress. It's like building important building blocks that will eventually help create specific rules for cyberspace in international law.

2. INTERNATIONAL LAW: MEANING AND CONCEPT

The domain of international law is intricate and ever-changing, regulating the interactions between independent nations and other global entities. It provides a framework for upholding harmony, settling disputes, and encouraging collaboration on a worldwide level. Treaties, customary international law, general legal principles, rulings by international organisations and judicial authorities, and general principles of law are the main sources of international law[1]. One of the main features of international law is its decentralized nature. Unlike domestic legal systems, international law does not have a centralized legislative authority that it derives its power from, nor does this type of law have a global court with a universal jurisdiction around the world. Instead, the states voluntarily enter into agreements or treaties to regulate the interactions and behaviour they have with other nations, these treaties form an

[1] Rabeea Alqamoudi, *The concept of international law,* 11(4) INT'L J. SCI. & RSCH. PUBL'N (2021)

essential component of international law and can cover a wide range of subjects from human rights and environmental protection, to trade and security.

Customary law is another aspect of international law and is a significant source. Customary law is the result of governments' regular, consistent practises that they view as legally obligatory. The idea that these practises must be followed by law in order to establish customary norms is associated with these practises. International legal norms are also shaped by general legal concepts that are acknowledged by nation-states[2].

International law also plays a crucial role in fostering peaceful relations among states. It provides a framework for the resolution of disputes through peaceful means, such as negotiation, mediation, and arbitration. The International Court of Justice (ICJ), is said to be the principal judicial organ of the United Nations and has the power to adjudicate legal disputes between states and issue advisory opinions on legal questions referred to it by the UN General Assembly, the UN Security Council, or other specialized agencies and authorized bodies.

One of the most prominent aspects of international law is human rights. In the international arena, various treaties such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, establish fundamental rights and freedoms that states are expected to uphold. International human rights law creates a standard for evaluating the conduct of states, and international organizations often monitor and report on compliance.

International law also governs the use of force and the maintenance of international peace and security. The United Nations Charter is a foundational document that prohibits the use of force except in self-defence or when authorized by the UN Security Council. The Security Council, with its five permanent members and ten elected members, has the authority to take measures, including the use of force, to maintain or restore international peace and security.

While international law provides a framework for global governance, its effectiveness is contingent on state compliance and enforcement mechanisms. States voluntarily adhere to international legal obligations, and non-compliance can lead to diplomatic, economic, or even military consequences. International law, therefore, reflects the delicate balance between the sovereign interests of states and the collective pursuit of a more just and peaceful world order.

[2] *Id.*

3. CYBERCRIME: MEANING AND TYPES

Cybercrime refers to any illegal activity that involves the use of digital devices and computer networks, and it encompasses a wide range of malicious actions, we shall explore various types of cybercrimes, their impact on individuals and organizations, and the importance of cybersecurity measures to combat them[3].

- Phishing

Phishing is a type of cybercrime that involves fooling individuals into revealing their personal information, such as login credentials and financial details. Perpetrators often pose as trusted entities, sending deceptive emails or creating fraudulent websites that mimic legitimate sources. Once the victim falls for the bait, their sensitive data is stolen and can be used for identity theft, financial fraud, or further cyberattacks.

- Malware

Malware, short for malicious software, is a broad category of cyber threats that includes viruses, worms, Trojans, and ransomware. Malware is designed to infiltrate a computer system, either to disrupt its operations or to steal sensitive information. Ransomware, for example, encrypts a victim's files and demands a ransom for the decryption key, leading to financial losses and data breaches[4].

- Identity Theft

Identity theft involves the use of someone's personal information, such as their name, social security number, or financial data, to commit fraudulent activities without their permission. Cybercriminals obtain this information through data breaches, phishing, or by hacking into databases. The consequences of identity theft can be long-lasting, leading to financial ruin and reputational damage for the victim.

- Online Harassment and Cyberbullying

[3] Dr. R Mangoli, *Cyber Crime: A Threat to Indian Society*, SSRN ELEC. J. (2016)
[4] Apoorva Bhangla & Jahanvi Tuli, *A Study on Cyber Crime and its Legal Framework in India*, 4(2) INT'L J. L. MGMT & HUMAN. (2021)

Online harassment and cyberbullying involve the use of digital platforms to harass, threaten, or humiliate individuals. These acts often occur on social media, in chat rooms, or through instant messaging apps. Cyberbullying can have severe psychological and emotional effects on its victims, and it can lead to real-world consequences.

- Hacking

Hacking is the act of gaining unauthorized access to computer systems or networks. Hackers may infiltrate systems to steal information, disrupt operations, or simply for the thrill of breaching security measures. State-sponsored hacking, also known as cyber espionage, is another form of hacking where nation-states engage in cyberattacks to steal sensitive information or gain a strategic advantage[5].

- DDoS Attacks

Distributed Denial of Service (DDoS) attacks involve overwhelming a target website or online service with a massive amount of traffic, rendering it inaccessible to users. Cybercriminals use botnets (networks of compromised computers) to launch these attacks. The motives behind DDoS attacks can vary from financial gain to ideological or political reasons.

- Online Scams

Online scams encompass a wide range of fraudulent activities designed to deceive victims into parting with their money or personal information. These scams can take the form of fake online auctions, lottery scams, romance scams, or tech support scams. Victims are lured by promises of easy money or assistance with non-existent problems[6].

- Child Exploitation

Child exploitation refers to the use of technology to produce, distribute, or access explicit content involving minors. Offenders may use the internet to groom and exploit children, leading to long-term emotional and psychological trauma for the victims. Law enforcement agencies worldwide work tirelessly to combat these heinous acts.

- Doxing:

[5] *Id.*
[6] Vijaykumar Shrikrushna Chowbe, *The Concept of Cyber-Crime: Nature & Scope*, SSRN ELEC. J. (2015)

Doxing or "dropping documents" is a practice of revealing an individual's personal and private information publicly without their consent. It involves an individual's phone number, home address, email address, workplace, etc. The information of the victim is gathered through means of hacking and research. It is used as a form of revenge, and intimidation, and can also be used to encourage others to harm the victim both online and offline. In some cases, doxing may also lead to identity theft or stalking. Many jurisdictions consider doxing to be illegal, especially if it results in harm to the victim.

- Hate Speech

Online hate speech refers to the use of discriminatory, offensive, or derogatory language, often targeting a person or a group based on attributes like race, religion, gender, or ethnicity. It can occur on various digital platforms, including social media, forums, and comment sections. Hate speech not only perpetuates prejudice but can also incite real-world harm, fostering a toxic online environment.[7]

- Revenge Porn:

Revenge porn, also known as non-consensual pornography, involves the distribution or sharing of explicit or intimate images or videos of a person without their consent, typically intending to cause embarrassment, humiliation, or harm. This malicious act is often carried out by a former partner or someone seeking revenge, control, or leverage over the victim. Revenge porn can have devastating consequences, leading to emotional distress, reputational damage, and even legal implications.

3.1 Impact of Cybercrimes

The effects of cybercrimes are extensive. Its victims can include people, companies, or even the government. One of the main goals of cybercrimes is to harm a person or organisation financially. This can be accomplished by extortion, fraud, threats, and other means. Instead of the reputation of the perpetrator, an institution's reputation suffers long-term harm along with a decline in public confidence and credibility when a government or organisation is the target of cybercrime. Cybercrime can also result in data breaches that compromise the confidentiality of sensitive information, such as government secrets, personal details, and

[7] Showkat Ahmad Dar & Dr. Naseer Ahmad Lone, *Cyber Crime in India*, 43(4) SAMBODHI (2020)

intellectual property, in addition to financial losses. Consequently, there may be ramifications for national security.

The effects of cybercrime on an individual are significant and frequently result in serious psychological repercussions[8]. Stress, anxiety, and sadness can be experienced by those who are the victims of identity theft, cyberbullying, or online abuse. One's everyday routine and emotional health may be negatively impacted by the dread of being targeted online.

4. ROLE OF INTERNATIONAL LAW IN CYBERCRIME

When it comes to cybercrime or any cyber-related operations, there has always been a silent consensus among the States that the existing principles of international law shall apply to cyberspace just like how they are applied to the physical realm. This consensus was reached until there was a legal obligation on a state to suggest otherwise. Therefore, in the year 2013, the UN General Assembly adopted the consensus reports of the UN GGE wherein the participating nations had agreed to maintain peace and stability, and also promote an open, secure, and accessible IT environment. In the year 2015, states agreed to follow the principles of the UN Charter, which included the obligation to observe State sovereignty, sovereign equality, peaceful dispute resolution, and non-interference in other States' internal affairs when using ICTs. This has been recognized by several international bodies, such as NATO (2014, 2020), the OSCE (2016), the G7 (2017), the EU (2017), and the Commonwealth (2018), who have all affirmed that existing international law applies to states' activities in cyberspace.

International law provides standards of conduct that states should follow to ensure that their territory is not knowingly used for acts that violate other states' rights. The principle of "due diligence" is one of the UN GGE Reports' series of measures that states should take to prevent and mitigate cyberattacks. Article 33 of the UN Charter on the peaceful settlement of disputes also applies to disputes in the cyber domain, as it does to other areas of state activity. Therefore, international law provides a framework for states to deal with grievances in the cyber realm. Here are a few international legal frameworks that contribute to the fight against cybercrimes around the world.

[8] Dr. R Mangoli, *supra* note 1

4.1 The Budapest Convention

The Budapest Convention or the European Convention on Cybercrime is considered to be one of the most significant steps towards tackling the issue of cybercrimes around the world. Held in Budapest in November 2001, the multilateral treaty outlined various procedures and provisions to criminalize offences through the use of computers. It was drafted by the Council of Europe along with various countries like Canada, Japan, the United States of America and South Africa. The convention comprises four chapters and forty-eight articles in total and provides states with the following provisions[9]:

- To criminalize certain acts or actions done through the means of computers and the internet.
- To establish a proper procedure to investigate cybercrimes and use electronic devices as evidence for the said crime.
- To have the international judiciary and police cooperate in mitigating cybercrimes.

The convention was signed by 67 nations together with international organizations such as the EU, Interpol, the International Communication Union, etc. These signatories were to be participating members or observers of the convention and the Cybercrime Convention Committee[10].

The Convention on Cybercrime is an agreement signed by several countries, but India is not one of them. As a result, India is not required to adjust its laws or adopt the Convention's guidelines. However, the Convention has been instrumental in shaping global and national cybercrime laws, as well as preventative measures and electronic evidence practices.

4.2 Model Law on Computer and Computer-Related Crime

The Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" in October 2002, specifically for the 53 member countries of the

[9] Sandeep Mittal & Prof. Priyanka Sharma, *A Review of International Legal Framework to Combat Cybercrime*, 8(5) INT'L J. ADVANCED RSCH. COMPUT. SCI. (2017)

[10] *Id.*

Commonwealth. The law aimed to expand the criminal liability for offenses related to internet and computer systems, as well as the use of illegal devices and methods concerning computer technology.

The Model Law introduced the concept of dual criminality regarding cybercrimes, which means that a person can be punished for an offense committed outside their country if their actions would constitute an offense under the laws of the country where the offense was committed. This concept may lead to prosecution or extradition. Many member countries of the Commonwealth have adopted their domestic cyber laws based on the Model Law.

4.3 The Organization for Economic Cooperation and Development (OECD)

The OECD is an organization comprising of 30 countries. In the year 1983, a committee was set up by the organization to discuss and debate reforms that needed to be made in the field of cybercrimes and criminal cyber laws. It officially approved the Guidelines for Consumer Protection in the Context of Electronic Commerce, which gave the member state's consent for consumer protection and e-commerce. The OECD also adopted guidelines for the Security of Information Systems and Networks in 2002, with its aim to promote the protection of information systems and networks among all participating members[11]

4.4 UNCITRAL Model Law on Electronics Commerce, 1996

The United Nations Commission on International Trade Law (UNCITRAL) developed the UNCITRAL Model Law on Electronic Commerce to assist countries in creating legislation that facilitates and regulates e-commerce and e-government. The Model Law serves as a guideline for countries to improve their laws regarding commercial relationships that involve the use of modern communication techniques, such as computers. This law recognizes electronic communications as having the same status as traditional paper-based communications. It includes provisions for the transmission and receipt of messages and electronic contracts but does not address issues related to jurisdiction or conflicts of law. The Model Law has established several defining characteristics, these are mentioned as follows:

[11] Widya Setiabudi sumadinata, *Cybercrime and Global Security Threats: A Challenge in International Law*, 11(3) RUSSIAN L. J. (2023)

- To establish rules that validate contracts made through electronic means and set up provisions to form e-contracts
- To define the characteristics of a valid e-contract
- To make electronic signatures legal for both commercial and legal purposes
- To include computers and other electronic devices as evidence to be used in court proceedings.

4.5 The United Nations GGE Reports

The United Nations Group of Governmental Experts (GGE) has produced several reports addressing the application of international law to cyberspace. These reports help shape state behaviour and expectations regarding responsible conduct in cyberspace. They emphasize the importance of avoiding cyberattacks on critical infrastructure and civilian targets[12].

4.6 The Tallinn Manual

While not a binding legal document, the Tallinn Manual serves as an important reference for interpreting and applying existing international law in the context of cyber conflicts. It clarifies issues related to state responsibility, sovereignty, and the use of force in cyberspace.

5. CONCLUSION

With the world becoming more interconnected, international law plays a critical role in combating cybercrimes. International law offers a framework for collaboration, setting standards, and holding cybercriminals accountable, despite its difficulties and complexities. Fighting the constantly changing threats in cyberspace will require improved international collaboration and coordination in addition to the continued development of international legislation in this area. The legislative structures and procedures that control our responses to cybercrimes must also evolve with technology in order to stay relevant and effective in the face of new threats.

[12] Sandeep Mittal & Prof. Priyanka Sharma, *supra* note 7