Page 2413 - 2423 **DOI:** *https://doij.org/10.10000/IJLMH.111609*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Cybercrimes and its Alarming Escalation During Recent Times: An International Legal Perspective

ACHYUTH B. NANDAN[1]

ABSTRACT

Cybercrime is one of the fastest growing areas of crime. These include attacks against computer data and systems, identity theft, distribution of child pornography, internet auction fraud, deployment of viruses, and various e-mail scams such as phishing. The global nature of the internet has allowed criminals to commit almost any illegal activity anywhere in the world. Traditionally, crime and its sanction are largely local, regional, or national, but today the main hurdle confronting us are associated with the transnational characteristics of cybercrimes. Therefore, it is of paramount importance to have international legal instruments ready to serve anti-crime efforts. There is always an illusory overlap or rather a fine line between internet space and international space. This paper focuses to address the sensitive issues of cybercrimes through an international legal perspective. Firstly, a brief introduction with regard to the world of cybercrimes and the underlying complications in placing legal fetters on the perpetrator. Moving on with a comprehensive analysis of Interpol's significant study and report on increase in computer crimes during the covid-19 pandemic. Methodical array of various international efforts such as United nations office on drugs and crime (UNODC) its objective and geographical scope, United nations crime and justice information network (UNCJIN,1999) and the types of cybercrimes recognised by the organisation has been actively deliberated, the organization for economic cooperation and development (OECD), commonwealth of nations, Group of 8 (G8) and other United Nations efforts to combat growing cyber threats has been elucidated. The paper is concluded with an inference made from statistical data's as well as legal statutes, various safeguard methods are also supplemented with it.

Keywords: *Cybercrime, Surge, Identity theft, Phishing, Identity Theft.*

I. CYBERCRIMES: AN OVERVIEW AND THE UNDERLYING COMPLICATIONS

Cyber-crimes otherwise known as the computer crimes involves a system and a network which is maliciously used by the perpetrator to commit the crime. It basically harms the victim's

[1] Author is a student at Cochin University of Science and Technology, India.

 [ISSN 2581-5369]

security, privacy and even financial health. "Unlawful acts wherein in the computer is either a tool or target or both". Cyber-crimes used to be an activity committed by individuals in isolation but now the scenario has been transformed, that means the class of criminals is overcrowded and cyber crimes has become an organized crime sector. People with malicious intention now knows the technical aspects to make a malware, sell it and perform strategic cyber attacks in exchange of money or to full fill personal vendettas or even to reck vengeance against individuals. Cyber crime encompasses any criminal act dealing with computer system and networks. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. It also includes non-monetary offenses, such a creating and distributing viruses on other computers or posting confidential business information on the internet.

The most prominent form of cyber-crime is identity theft, in which criminals use the internet to steal personal information from other users. It is done mainly through common cyber crime methods namely phishing and pharming.

II. CYBER-CRIMES CAN BE CLASSIFIED IN TWO WAYS

1. **Computer as a target:** using a computer to attack other computers. For example: - Hacking, Virus/worm attack etc.
2. **Computer as a weapon:** using a computer to commit real world crimes, for example, cyber terrorism, credit card frauds, printing fake currency, etc.
3. **Categories of cybercrime:** cybercrimes are broadly categorized into three, namely:
   - **a.** Individual
   - **b.** Property
   - **c.** Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

- **Crimes against individual:** This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "online grooming". Today law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.
- **Crime against property:** just like in the real world where a criminal can steal and rob, even in the cyber world criminals' resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money, misuse the credit card to make numerous purchases online run a scam to get innocent people to part with their hard-

 [ISSN 2581-5369]

earned money, use malicious software to gain access to an organisations website or disrupt the systems of the organisation. The malicious software can also damage software and hardware.

- **Crime against government:** although not as common as the other two categories, crime against a government is referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

A major challenge with respect to the enforcement of efficient municipal and international law framework in order to curb the rising cybercrime scenario is mainly the anonymity factor. That is, the world of cybercrime is highly complicated, which places a major fetter to the enforcement of law in this regard. To add more complexity to this issue, there are jurisdictional boundaries that prevents criminals from being prosecuted.

Cybercrimes and its various kind evolve each and every second as the perpetrators seek the technical know-how and advance their criminal activities so perfectly that they escape from the eyes of law and that's indeed a matter of concern.

III. INCREASE IN THE CYBERCRIME CASES AND INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL) EFFORTS

A latest report released by the INTERPOL based on the assessment of the impact of covid -19 on cybercrime [1]. It has shown a significant target shift from individual community and small businesses to major corporations, governments and critical infrastructure. As business organisations and almost all the other expertise has been rapidly deploying remote systems and networks to support staff members and other related business community to work from home so as to avoid physical contact and probable spread of the virus. But criminals are taking advantage of this network vulnerabilities to steal data, generate profits and cause disruption.

Statistical data suggests that in one fourth month period that is, January to April 807,000 spam messages, 745 incidents related to malware and 49,000 malicious URLs all of which closely related to the pandemic were detected by the study conducted by the INTERPOL's private sector partners.

As according Juren stock, INTERPOL secretary General "cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by covid 19".

 [ISSN 2581-5369]

Interpol has basically provided a technical guidance in cybercrime detection, investigation and proof collection. The Interpol information Technology Manual was compiled by the European working party on information technology crime.[2]

Along with efforts in law enforcement on cybercrime, Interpol also takes distinct actions to prevent cybercrimes, cooperating with banking companies to combat payment fraud by building a database on Interpol's website. In addition, Interpol is making efforts to establish a network to for harvesting information relating to activities on the internet.

Primarily the increased online dependency of people around the world during lockdown period but lack of cyber defences which are up to date.[3]

As per the report's findings, 86 per cent involved phishing, 65 per cent involved malware, 34 per cent involved financial fraud, 15 per cent involved extortion. 13 per cent involved in pharming, 5 per cent involved in hacking, 5 per cent involved denial of service.

The lockdown has significantly increased concerns about vulnerable persons online. Children are greatly benefiting from e-schooling, they are equally more exposed to threats coming from the internet. The elderly, who usually rely on offline shopping and have now to purchase what they need from the internet, equally find themselves more exposed to cybercrime.

Another side effect of the protracted lockdown has been a growing demand for pornography. The industry has seen an increase in the number of users, but also concerns are being raised about vulnerable categories being pushed into exploitation, including drug addicts and human trafficking.[4]

IV. INTERNATIONAL LEGAL ACTIONS AND EFFORTS AGAINST CYBER CRIMES

(A) United nations office on drugs and crime (UNODC)

In the international law perspective, the United Nations office on drugs and crime, under their initiative a global programme on cybercrime was held according to which cybercrime is highly complicated in nature. This is because it takes place in the borderless virtual cyberspace, and is compounded by the increasing involvement of organised crime groups. The perpetrators and the victims of cybercrime is geographically placed in different locations, and its effect ripple through societies around the world. This indicates the need to mount an urgent, dynamic and international response.

1. Objective and geographical scope

The global programme is designed to respond promptly to identified needs and wants in developing countries by complimenting member states to prevent and combat cybercrime in a

 [ISSN 2581-5369]

holistic manner.

During the 2017 cybercrime programme was attended by various countries such as central America, Eastern Africa, MENA and south East Asia and the Pacific with key aims of:

- Increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrimes, specifically online child abuse and exploitation. The input of a strong human rights framework is urged.
- Efficient and highly effective long term government response to cybercrime.
- National coordination, data collection and effective legal frameworks, leading to sustainable response and greater efficacy.
- Strengthened national and international communication and building up a rapport between government, law enforcement and the private sector with increased public knowledge of cybercrime risks.

(B) United nations crime and justice information network (UNCJIN, 1999)

UNCJIN recognises various types of cybercrimes which are mainly:

"When any crime is committed using computer or internet, it is referred to as a cybercrime". There are many types of cybercrimes and the most common ones recognised by the UNCJIN and has shown a sharp increase during the recent times is as follows:

1. **Hacking:** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

It involves combining the power of the internet and specialized programming skills to bypass sophisticated security systems. It comes in many forms, from the programming of malicious programs called spyware and malware to the breaking of sophisticated computer security systems.

For example, if a hacker enters your computer and steals financial information such as your credit card number, or the password to your bank account, they could use that information to make purchases.

In *K.U. V. FINLAND* the facts of this case suggests that a 12-year-old boy complained to the European Court of Human Rights that his right to respect for his private life had been violated (Article 8 of the European Convention on Human Rights (ECHR)) and the state had failed to provide him with an effective remedy (as required by Article 13 ECHR).

The court here rejected the governments argument that sufficient protection for privacy was provided by the existence of the criminal offence. "Although freedom of expression and privacy of communications are important considerations and users of this technology should have a guarantee that their own privacy and freedom of expression be respected, such "guarantee cannot be absolute, and must yield to the prevention of disorder or crime or the protection of the right and freedoms of others."

2. Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the law enforcing agencies. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

3. Cyber stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims lives more miserable.

4. Identity theft: This has become a major problem with people using the internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, social security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victims credit history.

5. Malicious software: There are internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

6. Child soliciting and abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The cyber police have been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

7. Pornography: As according to End child prostitution and trafficking (ECPA) an international NGO network solely dedicated to the fight against the sexual exploitation of children. "Describing or showing sexual acts in order to cause sexual excitement through books, films etc." it includes pornographic websites, pornographic materials produced using computers and use of internet to download and transmit pictures, pornographic videos, photos, etc. This organization tracks countries that have implemented standards as defined by

 [ISSN 2581-5369]

agreements such as the Convention on cybercrime, and Lanzarote convention through their human rights reports.

8. E-mail related Frauds

If you send an e-mail, along with it some illegal activities may happen. They are:

a) **E-mail spoofing:** It refers to e-mails that appear to have originated from one source while they are actually sent from another source.
b) **E-mail spamming:** It refers to sending e-mails to thousands and thousands of users
c) **Sending malicious code:** e-mails are used to send virus from source to another destination computer.

9. Cyber Warfare: Cyber warfare involves nations using information technology to penetrate other nations networks to cause damage or disruption. In the US and many other nations, cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space) cyber warfare attacks are primarily executed by hackers who are well trained in exploiting the loopholes of computer networks and operate with the support of a nation. A cyber warfare attack may intrude the networks of other countries for the purpose of compromising valuable data, disrupting communications, or interrupting commerce.

10. Cyber Espionage: Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holder. It is described as the stealing of secrets stored in digital formats or on computers and IT networks. Cyber espionage is most often used to gain strategic, economic, political, or military advantage. It is conducted through the use of cracking techniques and malware.

V. MULTINATIONAL LEGAL MEASURES TO CURB THE RISE IN CYBER-CRIMES GLOBALLY

Since cybercrimes are transnational and complicated in nature, it is highly advisable and is of dire need to have dedicated multinational concentrated efforts to curb the menace and dangers of cybercrimes. Three main organisations in this regard are:

1. The Commonwealth of Nations: The Commonwealth of Nations took the Initiative to put up an action plan in harmonizing laws of its member states. In October 2002, the commonwealth secretariat prepared the "Model law on computer and computer Related Crime".

Through this model law, the convention on cybercrime has become one if the legislative choices in the international legal perspective., covering the offences of illegal access, interfering with issues such as child pornography, illegal data and interception of data. When

 [ISSN 2581-5369]

you compare convention on cybercrime and the model law, the model law has clearly expanded criminal liability. The model law has covered the problem of dual criminality. That means if a person's conduct would also constitute an offence under a law of the country where the offence was actually committed. This may potentially lead to prosecution but not extradition as provided in convention on cybercrime. Some of the member countries have made concreate efforts to draft domestic laws to keep a check and curb the menace of virtual crimes.

2. The organization for economic cooperation and development (OECD) - It is an international organisation comprising 30 member countries, it has addressed computer security issues for several decades. The guidelines established mainly nine principles, including awareness, responsibility, response, risk assessment, security management etc. The practical endeavours were left to the member countries to make. OECD documented included unauthorised access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, virtual espionage.

3. G8 It is a group of 8 member nations The group of eight members has created various international organisations at the Halifax summit 1995. They initiated various dedicated efforts to keenly identify the various cybercrimes committed by perpetrators. The recommendations urged the states to increase the level of criminalization, prosecution, investigation, and international cooperation, while acknowledging in their entirety human rights protection.

And also at the Denver Summit 1997, the group of eight proposed to strengthen their efforts to realize the Lyon recommendations, by specifically concentrating on punishing cyber criminals, and promoting the governments technical and legal abilities to react to trans territorial computer crimes.

At the Okinawa summit, the Okinawa charter on global information society adopted the principle of international collaboration and harmonization of cybercrime. The charter recognized that the security of the information society necessitated coordinated action and effective policy responses.

VI. UNITED NATIONS (UN) AND APPROACH TOWARDS GLOBAL CYBERCRIME

There are umpteen global organizations but UN is one of its kind capable of being identified as the only global organization that forms a forum of its 191 member states with full and concreate functions.

In 1990, the general assembly of the UN adopted the guidelines concerning computerized personal data files. It proposed to take appropriate measures to protect the files against both natural and artificial dangers. The guidelines extended the protection of governmental

 [ISSN 2581-5369]

international organizations.

In resolution 55/63, the General Assembly noted the value of the following measures to combat computer system abuse:

- To ensure elimination of fake internet domains.
- To take into account both the protection of individual freedoms and privacy and to facilitate the preservation of the capacity of governments to fight cybercrimes.
- To ensure mutual assistance regimes for the timely investigation of cybercrimes and necessary advancements.
- To protect the security of data and computer systems from virtual crimes.
- To enhance and coordinate cooperation in the investigation and prosecution of cybercrime.
- To design IT techniques to help to prevent and combat cybercrime.
- To create awareness among general public of the requirement to prevent and combat computer crimes.
- To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations.
- Promotion of security awareness at the international level.
- Promotion of security awareness at the state level
- Harmonization of legislation.
- Coordination and cooperation in law enforcement.
- Direct anti-computer crimes actions.

VII. CONCLUSION

Cybercrimes need to be addressed in the international domain the issue must be highlighted, it is of core importance. The unprecedented rise in cybercrimes is a matter of grave concern. The transnational character of cybercrimes has clearly added up more complications to the existing crisis. Mitigation may help users and employers. The users need to be more vigilant about phishing emails and websites, practice good cyber hygiene, use only trusted wi-fi networks and consider adopting a password manager to help to avoid using the same password for multiple websites. It is advisable to look for information from trusted websites. The official online conference calls which are frequently used nowadays need to be handled with due care and caution especially while sharing screen and passing vital information. Employers working from home through virtual platforms should make sure that they secure remote access to the organization's virtual domain. They should refrain from using personal computers to do official

 [ISSN 2581-5369]

work assignments. Last but not the least, individuals and employees must be made more aware regarding the dangers of cybercrimes and gradually should equip them to enhance their cyber-security knowledge.

*****

 [ISSN 2581-5369]

VIII. END NOTES

1. Interpol's official website. Covid 19 cyber threat response. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
2. Interpol's Global guidelines digital forensics laboratory.
3. Interpol, Interpol press release, CPN02/00/COMandPR, 5 February 2001.
4. Freedom from fear magazine (cyber crime during the Covid-19 pandemic).
5. International Actions against cybercrime: Networking legal systems in the Networked Crime Scene.
6. Global programme on cybercrime, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
7. United Nations Crime and Justice information Network (1999), paragraph 245
8. *K.U V. FINLAND*, https://archive.crin.org/en/library/legal-database/ku-v-finland.html
9. End Child Prostitution, child pornography and trafficking of children for sexual purposes (ECPAT) https://www.preventionweb.net/organizations/3709
10. Convention of cybercrime (European treaty series-No 185)
11. Lanzarote convention (Council of Europe)
12. The commonwealth of Nations. https://thecommonwealth.org/media/news/commonwealth-helps-countries-make-new-cybercrime-laws-and-fight-crime-together
13. G7 24/7 cybercrime initiative https://rm.coe.int/1680303ce2
14. Human Rights treaty bodies, OHCHR.
15. Denver summit 1997, Press statement.
16. Okinawa charter on global information society, Okinawa July 2000
17. Resolution 55/63 General Assembly, https://www.cybercrimelaw.net/un.html
18. Security Awareness programme, https://www.sciencedirect.com/topics/computer-science/security-awareness-program
19. Cyber security and the need for Harmonisation of Rules., https://www.planetcompliance.com/cybersecurity-and-the-need-for-harmonisation-of-rules/.

*****

 [ISSN 2581-5369]