VOLUME 11 ISSN 2456-9704

CYBER CRIME- A GLOBAL MENACE

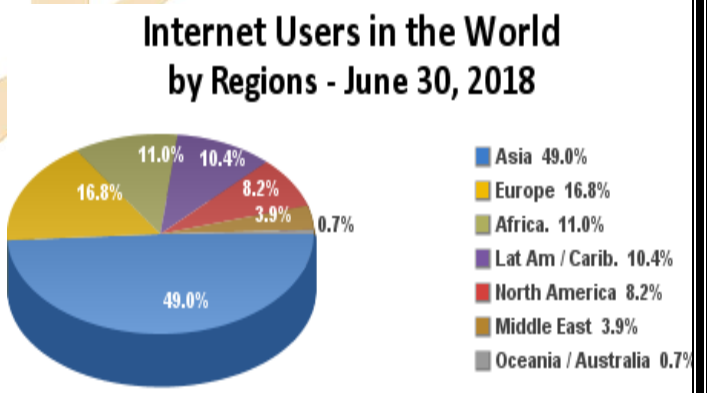
By Saksham Grover
From Delhi Metropolitan Education, Guru Gobind Singh Indraprastha University

ABSTRACT:
The evolution of information/cyber technology and the dependence on the internet has provided the population with a plethora of opportunities. However, this is laterally accompanied by the vulnerability of society to the world of cybercrime. This new medium of technology does not distinguish between good or evil, national or international and only provides a platform for the offences that take place in the cyber world. These offences include a computer as a tool or a target or both and include offences such as phishing, unauthorized access and hacking, pornography, cyber stalking, etc.

With extensive and worldwide use of the internet, the scope of cybercrime around the world is no less than terrorism today. Various countries including India have had the need of enacting legislations to curb this peril. In India, the Information Technology Act, 2000 was enacted with the prime objective of providing legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication. The last decade has witnessed a significant evolution in the international as well as regional instruments to curb cyber crime which include certain binding and non-binding instruments. Robert Mueller, American Attorney has rightly said, "We need to take lessons learned from fighting terrorism and apply them to cybercrime." Users of the internet can, however, adopt various techniques aimed at preventing cyber crimes such as firewalls, anti-virus software, etc. Plenty of national as well as international efforts have been made at intervals to prevent cross-border cybercrime. Furthermore, to prevent such crimes, special cyber-cells have been formed in various police departments across the globe which serves as a great preventive measure against cyber offences.

1. INTRODUCTION

The operation of internet is prevailing in almost every industry today. With numerous notable advancements in the information and communications industry over the last half decade, internet has now become the part and parcel of every educated person in this world. Internet is undoubtedly the easiest option to connect one person to another all around the globe.



1.

However, it also unknowingly and dangerously connects and transmits data to the cyber criminals standing by to hit the gullible users. This has raised concerns about cyber-security, IPR issues, information privacy and electronic transactions. These issues and challenges have brought about a tremendous shift in the legal system as well. Today, there exists a whole separate branch of law which governs the cyber world. Cyber law is the term which is used to refer to the legal and the regulatory framework which govern these offences.

2. WHAT IS CYBER CRIME?

Indian law, even the Information Technology Act, 2000 which deals with cyber crime nowhere specifically defines the term 'cyber crime.' In general, cyber crime means an offence which takes place on or with the means of a computer, internet or any other technology recognized under different laws globally.

Encyclopedia Britannica defines cyber crime as "*Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.*" 2

The United Nations has categorized cyber crime into two parts and thus, defined it as:

a. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
b. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).*"3

The definitions provided by various jurists and organizations time and again do not seem to be exhaustive but provide the people with an excellent starting point.

2.1 What does Cyber Crime Include?

The three major categories that cyber crime can be identified into include: individual, property and government depending on the method and the gamut of the offence.

Types of cybercrime

a. **Identity Theft:** Cybercrime where a criminal gains unauthorized access to an

[1] https://www.internetworldstats.com/stats.htm
[2] https://www.britannica.com/topic/cybercrime
[3] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

user's personal, confidential information to steal funds, to access accounts and open new accounts using a user's name, buy or rent properties and use identity of an user to commit offences.

b. **Stalking (Cyber stalking):** The development of the social media platforms have to a great extent given rise to offences of online or cyber stalking. This includes harassment of a user by another user via messages or online content. Majority of these cases are among a person's own contacts. The criminal uses content to instill fear in the victim about the consequences.
c. **Potentionally Unwanted Programs (PUPs):** The act of installing unwanted and unnecessary harmful softwares including applications falls under this category. These are a type of malware which intent to harm and damage a computer's software.
d. **Phishing:** Phishing involves a hacker making use of e-mails and other messaging platforms to lure users into accessing the message which provides the hacker with the personal information of the user.
e. **Scams:** Usually in form of online advertisements and spams claiming to provide the user which a reward or unrealistic amounts of money. These enticing offers can cause damage to software and compromise of personal information.
f. **Software Piracy:** One of the most common and known crimes which includes copying or accessing someone's invention or production. Piracy usually involves an infringement of copyright and trademark over a certain property.
g. **Web-jacking:** Deriving its name from the term 'high jacking', this type of crime includes seeking and taking control over someone's website or domain by gaining access to the website's original address.
h. **Child abuse/Child pornography:** The most heinous crimes of all, includes harassment and luring of children via means of chat rooms and other platforms into the world of pornography as well as being trafficking. There are many other activities which constitute child abuse such as downloading, selling and distribution of child pornography.

3. CYBER CRIME AGAINST WOMEN

Cyber crimes originate from the development and use of the information technology and the internet in specific. The current trends in the world of cyber crime are mostly diverted towards the individuals. In a society where the cyber laws are inadequate and perfunctory, the users of the internet are targeted by the criminals over the online platform. Various studies and statistics have shown that the most targeted and the most vulnerable victims remain to be women and children. Crimes against women have, in general increased over the years. Recently a study published that a majority of girls and women who are subjected to such harassment commit suicide after their private photos and videos are leaked online.

3.1 Common forms of cyber crimes against women

A criminal may make use of a woman's photographs, videos and other personal data without the consent of the woman and share

it online via the internet. For example: It has unfortunately become a common practice among the people to use the online services for their revengeful acts. A criminal can use a woman's profile picture from a social media platform and post it on a pornographic website or any other related platforms. Cases like these come to light every now and then today.

a. **Hate speech:** Verbal statements, comments which are directed towards women with a particular ideology and views. These statements and comments often involve negative and abusive content including body shaming, slut-shaming, sexual comments on the online social media and other platforms. Today this is used as a tool for 'trolling' and shaming the women actively using social media.
b. **Impersonation:** Another common activity which is on the rise due to inadequate regulations on the social media is impersonation and creation of fake account using a person's name and his/her picture and posting malicious information using that account.
c. **Stalking:** Cyber stalking which is one of the major cyber crimes is usually directed towards women and children. Cyber stalking not only includes keeping track of one's activities but also harassment of different kinds which victimize and compromise a woman's integrity.
d. **Defamation:** Defamation includes both libel and slander which a criminal publishes on online platforms causing the reputation of a woman to disintegrate and causes mental agony and pain.

3.2 Reasons for crimes against women

Among millions of users of the internet globally, women comprise of a sizeable number among these users. Many of these users who do not own a computer access the internet at cybercafés. It is common activity that these cybercafés often leak and share the data and information of a customer online which is then used for illegal and wrong purposes. Though India only has about 30% of female users of the internet, this number increases depending upon the region. For example in the US, this number goes up to 88% of women who use the internet at least occasionally. [4]

a. **Legal loopholes:** The Information Technology Act, 2000 was enacted for creation and enhancement of e-commerce by covering commercial and business malpractices such as hacking, fraud, confidentiality breach, etc. While the formation of the law, the legislators either being unaware or ignorant towards the safety of the users did not make the law as such to enhance not only safety of transactions but also of the population making those transactions. Though the act criminalizes acts such as publishing or sharing of obscene information electronically (Section 67), publication for fraudulent purposes (Section 74)[5]. These provisions time and again prove to be deficient in providing women and children with the safety that they need during this generation. Issues such as lack of specific enactment of laws for women and children, jurisdiction, lack of evidence, lack of cyber control associations and also lack of awareness makes it quite easy for

[4] https://www.statista.com/statistics/184415/percentage-of-us-adults-who-are-internet-users-by-gender/

[5] The Information Technology Act, 2000

the criminals to use such loopholes and get away with a lot of acts.

b. Sociological issues: Technology is one such field which is increasing at a faster pace than any other industry. Despite of being one of the most developed fields, the awareness and the education about the issues, consequences and laws are lacking. This is the reason why a majority of cyber crimes remain unreported and are handled recklessly by the authorities. The hesitation and the fear that is instilled in the victim about the defamation of herself and the family make her even more vulnerable towards such crimes. Many times the women believe herself to be responsible for the act that has taken place and even commit suicide.

3.3 Preventive measures and recommendations

a. Education and awareness beats any other solution for prevention of such digital harassment regimes. Awareness regarding the issues and the legal framework revolving around these crimes would help women in meeting these challenges in a better manner.
b. Abstaining from transmitting any personal data and information whether financial or personal to any stranger or friend whose identity is at doubt.
c. One such measure that needs to be taken in order to ensure safety is breaking the barrier of societal pressures and manipulation and making a woman hesitation free and independent enough to report such heinous acts.
d. Formation and development of regulatory organizations by the Government and stricter laws.
e. The owners of the websites and social media platforms should frame policies and rules which ensure the safety of its users. Checking the traffic and irregularities on the website can be an effective way of ensuring that no malicious act takes place.
f. A speedy redressal system for the victims of cyber crimes can also prove to be useful in gaining trust of the victims which would also encourage others to report and take actions against such offences.
g. Many social media websites now provide an option for their users with privacy options where the users can decide what a person can see on their account. The use of his option should be made effectively by the users, especially women to prevent themselves from being targeted by the cyber criminals.
h. Complete justice is provided to the victims by means of compensatory remedies and punishment of highest grade to the criminals involved.

4. CYBER CRIME AGAINST CHILDREN

In the world of cyber crime, children seem to be the newest victims that are targeted and lured by the criminals. The services of internet are being used to commit offences against the children in many ways. This technology has proved to be both a boon and bane for the young generation. The increasing magnitude of the information technology has led to this online exploitation to become an international concern. Children adapting to these technologies at a young age has exposed these children to the world of exploitation and abuse. Using the internet, access to the online content has been made easier which makes it convenient for the offenders to reach these children faster and in large

quantities. Chat rooms, social media platforms and online games are some examples of the ways by which an offender can gain access to a child.

4.1 Types of cyber crimes against children

a. **Child pornography/Sexually Malicious Content:** The most heinous of all crimes is child pornography. Child pornography is a form of child sexual exploitation. Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old). Images of child pornography are also referred to as child sexual abuse images.6 The intention is one of the requisites to be charged for an offence under this category. To be held guilty, an individual must intentionally and knowingly possess, receive or distribute such content. The legal regulations with respect to child pornography are stringent not just in India but all over the globe. Not only publishing or transmission of this content but also browsing, possession and downloading of such content is dealt with harshly under majority of civilized legal systems.

b. **Online Grooming:** The method used by a lot of sex offenders which includes building of a trust relationship with a minor/a child, befriending a minor over the internet in order to establish an emotional connection and eventually using such relationship to exploit the child sexually and indulge into intercourse with the child. These sex offenders are usually referred to as 'pedophiles'. This online manipulation of a minor becomes easier for the offender due to the lack of awareness and sense which a child inhibits. This often leads to the minor being dragged into pornography or even trafficking. Unfortunately, these cases do not always involve a stranger but sometimes includes the involvement of a known person such as a relative of the child. The overwhelming response of children and minors towards the social media platforms and their use of the internet have led to a huge increase in cases of online grooming. This not only damages a child physically but also mentally. In fact, the mental agony and stress that an activity of this sort causes to a child is unbearable and irreversible leading to a traumatized and a bleak future.

c. **Harassment and Cyber Bullying:** Unlike harassment and bullying in real life, cyber bullying can follow a person anywhere they go and can be agonizing. Cyber bullying and online harassment includes:

i. Sharing and storing personal data including images, videos.
ii. Sending offensive, threatening and abusive content online.
iii. Trolling
iv. Body shaming, slut-shaming, etc.
v. Hate speech, setting up groups to harass a child online
vi. Creation of fake accounts, hacking into a person's account.
vii. Non consensual explicit and sexual messages
viii. Manipulation and blackmail of a child into sending explicit and sexual images of him/her

5. LEGISLATIONS AND INTERNATIONAL

[6] The United States, Department of Justice

INSTRUMENTS AGAINST CYBER CRIME

According to a Global 2021 Forecast published by Cisco, there has been a rapid growth in the usage of internet. Globally, monthly IP traffic will reach 50 GB per capita by 2022, up from 16 GB per capita in 2017, and Internet traffic will reach 44 GB per capita by 2022, up from 13 GB per capita in 2017. Ten years ago, in 2007, per capita Internet traffic was well under 1 GB per month. In 2000, per capita Internet traffic was 10 Megabytes (MB) per month.7

This dramatic growth and changes in the trends of technology has lead to an evenly spread of the offences that entail such technology as well.

5.1 Indian legal structure

a. Information Technology Act, 2002

The act enacted for the regulation of the online activities majorly dealing with transaction which are commercial in nature. However, this legislation in some ways also deals with breach of privacy directed towards an individual such as penalizing the act of stalking and criminalization of child pornography. An overview of provisions under this act acting against cyber crime is:

Section 67	Punishment for publishing or transmitting obscene material in electronic form
Section 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
Section 66A	Punishment for sending offensive messages through communications service, etc.
Section 66B	Punishment for dishonestly receiving stolen computer resource or communication device
Section 66C	Punishment for identity theft
Section 66D	Punishment for cheating by impersonation by using computer resource
Section 66E	Punishment for violation of privacy
Section 66F	Cyber terrorism

b. Indian Penal Code, 1860

Section 503	Sending threatening messages by e-mail
Section 499	Sending defamatory messages by e-mail
Section 463	Forgery of electronic records, e-mail spoofing

c. **The Protection of Children from Sexual Offences Act, 2012 (POCSO)** is one of the major essential legislations that specifically deals with offences involving victimization of children. This legislation criminalizes cyber crime such as child pornography, stalking,

[7] Cisco Visual Networking Index: Forecast and Trends, 2017–2022, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

online child trafficking, harassment and other related offences committed against children in the online world.

5.2 International laws and instruments

Meeting the challenges proposed by this new category of crimes which take place via computer sources and internet is becoming a global phenomenon. Numerous legislations by different countries and instruments by the United Nations have been enacted and proposed to make and review every respective region's criminal laws that are battling against cyber crimes. During this generation, frequent crimes pop-up which involve a crime using the internet as a source. Laws acting against various acts such as unlawful access to data and information, spying and stalking, frauds, etc. have been formed in respective states. Though, not exhaustive and sometimes inadequate in fighting against cyber crimes, these laws do provide a great start to the population to act and end cyber crime in the world.

a. **International organizations:** Regional international organizations such as Council of Europe (COE), Asia-Pacific Economic Cooperation (APEC), and The European Union (EU) have been setup to intercept cyber crimes. This organization comprises of 21 member economies working towards minimization of cyber crime. Some of the members include The United States of America, Russia and China. Interpol is one such other major organization which is committed to the fight against cyber crime.
b. **Multi-national cooperation:** The organization for economic cooperation and development (OECD) is one example of multi-national organizations which has been addressing cyber security as one of the most important regime. Comprising of 30 member countries, this organization is a major instrument tackling cyber crime.
c. Several conventions and resolutions enacted by the United Nations Organization to take strict actions in order to eliminate crimes via communication sources, internet, etc. Various publications by the United Nations Commission on Crime prevention and Criminal Justice (CCPCJ) have addressed the growing cyber crimes against children and the need to eliminate them. These laws extend over jurisdictions governed by the United Nations Office on Drugs and Crime which undertakes international actions to combat national as well as transnational crimes.

6. CONCLUSION

The anonymity, secrecy and ease of association that internet provides has been taken advantage of by the cyber criminals time and again. Though every individual in the world is a potential victim of crimes taking place via the internet, women and children still remain to be one of the most vulnerable groups in the population. Furthermore, in cases involving children, age and gender remain a major factor. It is often witnessed that children belonging to lower strata of society and from a particular socio-economic background are targeted more than children belonging to upper class of the society. Here, education and awareness plays a major role in the safety of a child. For a very long time, the legislatures of almost all countries have been ignorant of

crimes taking place online but with such rapid growth in the information and communication technology the legal authorities are now coming up with finer and more developed laws to deal with the issue of cyber crime.

Because of the nature and the methodology of such crimes, they differ in a major way from crimes committed in the real world. Cyber crimes are unfortunately a harsh truth that exists in the modern technological world. The economic and personal damage that cyber crimes can cause is massive. Such criminals not only target individuals but also government and other governmental organizations which could also be a huge blow to the privacy of the citizens as well as the organization. The need of the hour is to tackle cyber crimes to the maximum for minimizing and even elimination of these offences. The future trends in this field only seem to be increasing. An increase in technology would lead to a simultaneous increase in the number of cyber crimes. Cyber crimes need more than just a motive and an intention. Most of the online criminals are committed by educated and qualified people since there is a need of a particular skill set needed to commit such an offense. The laws against cyber crimes need to become more stringent and have to be developed at a faster pace than the crimes. However, there is a thin line of difference between protection of a citizen and infringement of privacy and rights of a citizen, this difference needs to be taken care of by the authorities while any law progresses. There is so much that we can do personally, in individual capacities to fight against the cyber crime and to ensure a safe and a secure environment for present as well as future generations.

*****