Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 4, July-2021, ISSN 2230-7540

# Concept of Cyberspace and Types of Cyber Crimes in India

**Harsh Gopalia[1]* Dr. Arvind Rathore[2]**

[1] Research Scholar, Maharishi Arvind University, Jaipur-302041

[2] Supervisor, Faculty of Law, Maharishi Arvind University, Jaipur-302041

***Abstract – Social networking sites have been very popular right from the beginning of the new millennium. These sites provided space for many to relax, connect with old friends and also get new also. But the cyber-criminal organizations have sadly misused these sites to serve their criminal acts. In the past couple of years, people started spending more time on these networks as the populations are gradually dependent on them. In the digital era, information technology growth influences the lives of people all over the world. Day after day, modern inventions and discoveries have broadened the science spectrum and created new problems for the legal community.***

***Key Words – Cyber Crime, Social Networking, Cyber Space, Netizens, Cyber security, Hacking, Phishing***

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - X - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

## INTRODUCTION

With the rapid development of this technology leads to the commission on cyber space with emerging different types of new cybercrime today, which has also been a topic of global interest in the future. In the cyber world era as computer use became more widespread, the rise of technology also grew, and people became more familiar with the word 'cyber.' The evolution of IT gives rise to the "cyber space" in which internet provides all people with equal opportunities to access information , analysis, data storage, etc. by using high technology.[12] Such offences are like the assault on people, companies, or governments' guarded records. Such types of attacks don't exist on the physical body but on virtual body, either personal or corporate. Technology has the communities, businesses and individual’s life over the last two decades altering the way people study, work and interacts with each other. People in different parts of the world can connect on a range of devices, such as computers, cell phones or tablets in real time.[13] A text message, photo, video, or email exchanged by a single person can be seen by hundreds users in a couple of seconds, and can go viral. The IT has now become a modern tool for harassing, doing misconduct or bullying, manipulating and harming others. Through a socio-cultural viewpoint, there is a negative distinction between the limitations of machine criminal activity of environmental (computer availability) and societal (norms, legislation) which is a direct consequence of technology globalization. Despite having a major impact on daily life through computers and the internet, the truth remains that only a small percentage of people understand what the computer and the internet are all about?[14]Systematic analysis is required which discusses in detail the basic concepts of cybercrime, cyber space and types of cybercrime.

## CONCEPT OF CYBER SPACE

William Gibson first used the phrase 'cyber space,' which he later defined as "an evocative and essentially meaningless" buzzword that could act as a code for all of his thoughts of cybernetic (transforming a text to hide its meaning). Now it's used to explain anything related to computers, IT, the internet and the complex culture of the internet. Also referred to as 'Cyber Space' is the cyber environment in which all information technology Driven contact and actions take place. Cyberspace cannot be placed spatially. It's made of intangible objects like the website, forum, social networks, personal information, reputation and email addresses. Cyber space can be called an online global community with quick connectivity and no territorial barriers.[15]Cyber space is the interactive system of computer networks where online communication takes place between the people and where people can communicate, exchange ideas, transfer knowledge, provide social support, perform

[12] Farooq Ahmad, “Cyber Law in India- Law on Internet”, p. 367, (2nd ed. 2008)
[13] Saraswathi Murali, “ Information Technology Handbook”, p.234, (2003)

[14] S.C. Sharma, “Study of Techno- Legal Aspects of Cyber Crime and Cyber Law Legislations”, p. 86, (2nd ed. 2008)
[15] Anirudh Rastogi, Cyber Law- Law of Information Technology and Internet, p. 2 (2nd ed. 2014).

business, create artistic media, direct actions, participate in political dialogue, etc.[16] Cyberspace, the modern frontier, is mankind's shared heritage, but sadly certain people exploit the common heritage and thus cyberspace is indeed a new frontier with various forms of crime. Now it's used to explain anything related to computers, IT, the internet and the complex culture of the internet.[17]The people participating in cyberspace are recognized as Netizens by the fusion of two terms 'Net' and 'citizen.' Whereas Netizens implies any person affiliated with the use of Internet, computers, IT Webster's Dictionary explain the Cyberspace, it is the electronic structure of computer, bulletin board, interlinked networks that is considered to be a boundless world providing access to information, digital networking, and a type of virtual reality in science fiction. Cyberspace means that “the notional environment in which electronic communication occurs or virtual reality” F. Randall Farmer and Chip Morningstar defined cyberspace, by the involving social interactions than by its implementation of technology.

## MEANING AND CONCEPT OF THE CYBER CRIME

The word 'Cyber,' whose usage became common in the 1980s, emerged many decades earlier since Norbert Wiener coined the word 'cybernetics' in 1948 and defined same as 'studying message as a method of controlling society and society.'[18] In reality, the phrase 'cybercrime' is mostly used in knowledge society of the 21st Century, and is created by combining two terms cyber and crime. The term cyber signifies the cyber space, and it means the computer-modeled information space in which there are different objects or information of symbols image exist. It is, therefore, the place where computer programs operate and data processing takes place.[19] Cybercrimes are nothing but real-life crimes perpetuated in digital medium and thus there is little distinction between the concept of a crime in the cyber world and the real world. The only difference is medium of crime. Cybercrime is ' 'transnational or international' – there is no border in cyber world. Computer crime, cybercrime, electronic crime, e-crime or hi-tech crime typically refers to illegal activity in which computer or network is source, device, target or crime location as well as conventional crime through use of technology such as, Internet fraud, child pornography. Broadly cybercrime means an act or omission, which committed on through internet connectivity, may me directly or indirectly, this is forbidden by any statute, and for which corporal and/or monetary punishment is given.

## DEFINITION OF CYBER CRIME

The term 'cybercrime' as a generic term that refers to all type criminal activities perpetrated through the use of computers, the Internet on the cyber space and the www. In India, in no law has any definition of the term 'cybercrime' been given yet. In addition, the IPC 1860 does not at any time use the word 'cybercrime. Even after 2008 amendment cybercrime is not define under Act. "In absence of a specific definition of notion of 'cybercrime' in European Union's legal system, a range of steps proposed in the Strategy to tackle 'cybercrime' (such as initiatives to improve cooperation between law enforcement agencies) are not explicitly related to concrete and well-defined offences."[20] Cybercrime can be defined as any unlawful act promoted or facilitated by the computer, whether computer is object of a crime, a repository of evidence relating to a crime, or an instrument that used commit a crime. In plain language cybercrime means crime engaged in computer network or computer. But in such simplistic and limited terms complex nature of the cybercrimes can't be sufficiently expressed. Cybercrime, according to Pavan Duggal, refers to all activities that are carried out with criminal intention in cyberspace or using internet medium. These can be either traditional or newly developed criminal activities with growth of new medium. Any conduct that basically offends human awareness may be included in the cybercrime context. Commit a crime with the using of computer technology is better definition of cybercrime; engaging in activities that threaten the ability of a society to maintain internal order. So this definition covers both traditional cybercrimes and the emerging ones. This also includes the use of computer technology, and not just the use of the networked computer technology.

## RELATION BETWEEN CYBER CRIME AND CYBER SECURITY

Cyber-crime Cyber criminality is a crime involving use of the computer devices and Internet. This can be committed against private organizations, governmental, individual, group of individuals. It is usually with the intention of harm someone's reputation of someone, causing mental or physical harm, and benefit from it such as spreading hate, monetary benefits, and terror.[21] As happened in 1998, more than 800 e-mails were sent to Sri Lankan embassies by Tamil guerrillas, (Tamil Tigers.) According to mail sent by Tamil Tigers "We are Internet Black Tigers and we are doing this to interrupt your communications." Intelligence authorities have described it as the first recorded

[16] Jyoti Ratan, Cyber Laws & Information Technology, p. 48. (3rd ed. 2017)

[17] Ibid

[18] Dhawesh Pahuja, “Cyber Crime & the law”, Legal India, July (2011) last access on 20 may 2020.

[19] Jyoti Ratan, Cyber Laws & Information Technology, p. 62. (3rd ed. 2017)

[20] Prabhash Dalei & Tannya Brahme,”Cyber law in India: An analysis”, 2 IJHAS, p.1, (2013).

[21] Cyber Crime Vs Cyber Security: What Will You Choose?; Europol; https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/cybercrime-vs-cyber-security-what-will-you-choose Last accessed on 15 may 20

terrorist attack on computer systems in a country.[22] The basic principle of cybercrime law is to punish, who is with criminal intentions access without authority or unlawful use of the computer systems and internet, in order to prevent damage and alteration of systems and data on it. The greatest threat of cybercrime, however, is to an individual's financial security as well as government. Cyber security Cyber security is strategy against unauthorized access or threats to computers, programs, networks, personal data, etc. This is an activity which protects and defends information and communication systems against who is to be authorized to use or alteration or device exploitation. Cyber protection is often referred to as security in information technology.[23] It involves the techniques to protect networks computers, data and programs from access, which does not have authorization or attacks that can harm or manipulate them in some way. Cyber security is basically a technical approach to safeguarding systems from such attacks. All threats to computer system or network and all vulnerability by good cyber security recognize. It identifies the cause and fixes, as well as ensuring system security. Strong cyber security systems are focused on a blend of human and technical elements.[24]

## TYPES OF CYBER CRIME

We can see every day cases of cybercrime increasing and figuring out what is traditional crime and cybercrime,, is quite difficult. However cybercrime can be categorized and discussed under following heading to tackle this challenge: Cybercrime against

1) Person

2) Property

3) Government

4) Society

## CYBERCRIME AGAINST THE PERSON

Cybercrime against persons committed. This form of offences directly influenced the individual's personality. Following are the cybercrimes of some kinds that threat the user.[25]

**Harassment via E-Mails-** This form of harassment is very popular by file attachments, sending letters, & links, i.e. through e-mails. Harassment is growing nowadays as the use of social media sites like Twitter, Facebook, Orkut, Instagram, etc. day by day increasing.

**Cyber-Stalking-** The phrase derives from the term 'stalking,' which means following a person to embarrass or harass that person. If computer or email is used for commit stalking. It is often achieved by using certain criminal activities such as abuse of identity, extortion, defamation, spoofing etc. Cyber stalkers may create fake websites, create fake forums, send threatening spam, make fake profile or send harassing mails for stalk another person.

**Cyber Defamation**- for causing defamation Injury can be done through oral or written words, or through signs or visible representations. The person making that defamatory comment must be intent to lowering the image of person about whom the accusation was made in general public's eyes.[26] If anybody publishing any defamatory statement by using cyber technology by like website, email or any social site may amount to cyber defamation

**Hacking-** In simple language hacking means accessing in computer for which you are not authorized. Hacking isn't necessarily a crime because when a hacker is permitted to access computer networks lawfully called "ethical hacking". However, hacking crosses criminal line after computer network of someone is accessed by a hacker without their permission or authority.

**Cracking-** it is an act of without my consent or knowledge breaking into the computer system and he tampered with the confidential information or data.

**E-Mail Spoofing-** Here an attacker steals another person's identity in form of a cell phone number and receives the SMS from the victim's cell phone number via internet and receiver. It is a very dangerous cybercrime against any human.

**Carding**- It means fake credit and Debit cards used by offenders with Draw money from the bank account of victim for their monetary gains. This type of cybercrimes often includes illegal use of ATM cards.

**Child Pornography-** Defaulters in this cybercrime create access materials or distribute that exploit the sexual exploitation of minors. This is classified among India's most heinous type of cybercrime.

**Phishing-** Phishing is financial crime in which criminal acts as a legitimate individual and sends an email demanding that person update his records or may be confirm details of his credit card and acquires confidential personal information.

## CYBER CRIME AGAINST THE PROPERTY

The second category of the cybercrimes is cybercrimes against property, including computer

[22] Pravin Karna "Cyber law & Cyber Crime The Concept of Cyber Crime: Nature, Scope" SSRN 2011

[23] Robert Roohparvar, Elements of cyber security by; InfoGuard Cyber Security; Dated: 02.03.2019; < http://www.infoguardsecurity.com/elements-of-cybersecurity/> last accessed on 1 May, 2020

[24] Ibid.

[25] Prabhash Dalei & Tannya Brahme, Cyber law in India: An analysis, 2013. IJHAS, volume 2, issue 1

[26] Prabhash Dalei & Tannya Brahme, Cyber law in India: An analysis, 2013. IJHAS, volume 2, issue 1

vandalism, harmful program transmission, and unlawful computer trespassing through cyberspace and without possession of computerized information without authority.[27]

**Intellectual Property Crimes-** depriving owner wholly or partially of his rights is a crime if it is done unlawfully. Most common type of breach of IPR may be s copyright infringement, software piracy, patents, trademark infringement, service mark infringement and designs, computer source code theft, etc.

**Cyber Squatting-** It involves two people claiming the similar domain name either through claiming to have first registered the name by right to use it before other or by using something which is similar to the previous one.

**Cyber Vandalism-** Vandalism means intentionally damaging another's property and includes the destruction or disruption of information or data stored on a computer when network service is disrupted and stopped. These actions may take form of a computer theft, any computer component.

**Hacking Computer System-** Hackers target those like Popular Facebook, Twitter, Instagram, blogging site via unauthorized computer access / control. These attacks were not intended primarily for financial gain as well as to diminish public image of a particular company or person. In April, 2013, hackers targeted MMM India.

**Transmitting Virus-** Virus is a type of programs which is written by the programmers which attach to a pc or file and then transmit to other computers and files on a network in order to alter or delete it. Cyber Trespass: it means accessing in to computer or network of someone without any right or authority of owner and alters, misuse, disturb and damage data by using internet.

## CRIME AGAINST GOVERNMENT

Third category of the cybercrime is crime against crime government. Under this category cybercrime is deferent kind of crime. The development of internet has shown[28] that individuals and groups use the medium of cyberspace for international governments as well as to threaten nationals of a country. Such crimes manifest themselves in terrorism when a person "cracks" into a website run by a government or the military.

**Cyber Terrorism-** Issue of Cyber terrorism concern both domestically and globally. Attacks on the Internet by Terrorist are by the distributed denial of the service attacks, hate emails and hate websites, attacks on the sensitive computer networks etc. Cyber terrorism practices threaten the nation's security and dignity.

**Cyber Warfare -** It refers to hacking which is politically motivated for espionage and sabotage. It is often seen as an analogous type of information warfare to conventional warfare however this analogy is controversial both for its political motivation and for its accuracy.

**Distribution of Printed Software-** This includes distributed "Printed Software" from one device to different with the purpose of destroying government data and official records. Possession of unauthorized information- Using the Internet, it is quite easy to obtain any information by terrorist and to hold that information for religious, financial, political, ideological purposes.

## CYBER CRIME AGAINST THE SOCIETY

This is fourth category of crime. If a crime is done with intention of causing harm via using cyber means to the society at large or number of the people.[29]

**Child Pornography-** It involves using computer network to develop access or distribute materials that exploit the sexual abuse of minors.

**Financial Crimes-** Phone networking and network sites where the offender will attempt to attack by sending false mails or messages via the internet, like using credit cards by illegally obtaining password.

**Forgery-** This means deceiving large numbers of people by sending threatening mails, since online business payments are the normal lifestyle requirement of today.

## CYBER CRIME DURING COVID -19

Most of the countries are affected by the Covid-19 till now more than 50,000 people are infected. Due spreading risk government of India announced lockdown for the whole country which started from 25th March, 2020 in starting phase of lockdown all private or public companies are closed. Employees suggested to do work from home. Companies' security is at risk as all the data like financial details, customer information, trade secrets, and all other business confidential information can be accessed by click of a button to employees from their homes. To avoid misuse of the data or loss of confidential information, it is important for the employees to take special care of the data of the company and protect it from family members and friends. In addition to company information, an individual's personal confidential and financial information is also at risk given the increase in the cyber-attacks.[30]

[27]

[28] Shital Kharat, "Cyber Crime – A Threat to Persons, Property, Government and Societies", SSRN (2017)

[29] Harpreet Singh Dalla & Ms. Geeta, "Cyber Crime – A Threat to Persons, Property,Government and Societies", ARCSSE 2013.

[30] Kiratraj Sadana & Priya Adlakha, "Cyber Crime During Coronavirus Pandemic", Mondaq (2020)

## COVID-19 AND MALWARE, SPYWARE, RANSOM WARE [31]

Virus Attacks ,During this lockdown period , people access websites on social media such as twitter, Facebook , Instagram, more frequently than watching series and movies by subscribing to the web channels such as Amazon, Netflix , Zee 5, HotStar etc. and even indulging in the online games by downloading various applications. Both of these practices are internet-based. People have to provide and/or offer permissions to readily access their personal details on their mobile, tablets, computers, and social media pages in order to use services offered by applications. Many times, users share financial information too in order to purchase applications or access online services. Citizens are becoming more dependent on different payment gates to pay their electricity bills, recharge their cell phones, purchase online essential goods and medicines, and participate in the various online activities of this nature. All those activities opened the door to attacks on ransom ware and spyware. A spyware steals the user's confidential personal data thus; ransom ware monitors a person's username and other important credentials. Such attacks could lead to losses not only economically but also otherwise for people. Different agencies recommend other counter-measures and safe activities that can be followed to prevent these attacks. Secured apps and Operating systems are sending its users regular updates to address security vulnerabilities and to provide additional security.

## PHISHING ATTACKS AND OTHER BANKING RELATED FRAUD

Banks currently operate with limited sources & people are recommended to use online banking or telephone banking to take advantage of banking services. Cyber criminals make phishing calls or SMS massage or send phishing emails to customers of the bank claiming to be officials of bank and demanding confidential details, such as their a/c number, debit or credit card number, OTP, CVV etc. Recently, in compliance with the RBI's COVID 19 regulatory plan, banks have allowed a moratorium by postponing payment of Term Loan/EMI Installments & Interest for 3 months. Cyber attackers are now contacting loan holders on pretext of negotiating the postponement of payment of EMI and requesting them for sharing CVV, OTP, PIN or password relevant to their accounts in order to make use of moratorium facility.[32]

## FAKE NEWS OR RUMOURS

Fake news or rumors that are circulating quickly throughout the country are another key concern that has arisen. Below are some instances of rumors & their side effects in the month of March, the on social media there is one misleading information where "chicken is a carrier of Corona virus" was declared cost poultry industry an lump sum loss of 1.6 billion rupees in a day. In another incident, an audio clip gone viral, claiming that vegetable vendors licked vegetables to spread Corona virus. The Government subsequently responded and released a statement saying the audio clip was false. There were other rumors that during lockdown period, government was going to cut pension by 30 per cent.[33] Taking into account the rising number of the fake news, Karnataka and Maharashtra Cyber Police have agreed to take serious actions against anyone found to be spreading false and unverified information about COVID-19 on social media. It was also determined that in these situations a person found posting misinformation on the What's App group, admin of the group should be held personally responsible in his group for these material and will be liable under the applicable law. Together GOI, police and social media channels are taking steps to prevent the spread of rumors.

## CONCLUSION

The world is facing a great malady called Cybercrime since the last two decades. Use of the malevolent programs in computers and over internet by malicious people to attack data or sell contraband and someone else’s identity is known as Cybercrime. This type of crime is committed with the use of computers and internet. A Cybercrime criminal is capable of hacking and planting viruses to destroy website and other portals across the world. Fraudulent transactions and online banking frauds are carried out by them by gaining access to highly confidential information as well as cyber pornography and various other crimes are committed. In simple words, no one is secure in the cyber world. Like the conventional concept of crime, cybercrime is also an act or omission which results in breach of law and backed by sanction of the state. Two essential ingredients of cybercrimes are *actus reus* and *mens rea*. The main reason behind the growing menace of cybercrime is our heavy dependence on computers and internet. Cyber spaces have advantages as well as disadvantages. Conventional crime can be prevented to an extent by patrolling of policemen, but in the Cyber space, information is open to Trojan Horses and other viruses as well as to cyber stalking and cyber terrorism. This type of crime poses a bigger challenge to the police, prosecutors and legislators. The only solution at present can be suggested that we must update ourselves with the Technology and keep watch over our children as well as other family members who are not too good in technology. We must pledge not to overlook any suspicious message or mail as well as control ourselves to reply without probe any mail or opening any link as we all know that it is still difficult to prove the commission of offence and identify the actual person because of

[31] Dr Mohan Dewan “COVID 19 Lockdown: Increasing Cyber Crimes in India”, Lexology 2020.

[32] Kiratraj Sadana & Priya Adlakha, “Cyber Crime During Coronavirus Pandemic”, Mondaq (2020)

[33] Dr Mohan Dewan “COVID 19 Lockdown: Increasing Cyber Crimes in India”, Lexology 2020.

lack advancement in our system of investigation and other processes.

## REFERENCES

1. Moore, R. (2005) "Cyber-crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

2. "cybercrime | Definition, Statistics, & Examples". Encyclopedia Britannica. Retrieved 25 May 2021.

3. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.

4. Bossler, Adam M.; Berenblum, Tamar (20 October 2019). "Introduction: new directions in cybercrime research". Journal of Crime and Justice. 42 (5): 495–499. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.

5. "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2021.

6. "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. Retrieved 17 May 2021.

7. "Cyber-crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.

8. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025". Cybercrime Magazine. 4 March 2018. Retrieved 17 May 2021.

9. "Cybercrime— what are the costs to victims - North Denver News". North Denver News. 17 January 2015. Retrieved 16 May 2015.

10. Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (PDF).

11. "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.

12. Netherlands, Statistics. "Less traditional crime, more cybercrime". Statistics Netherlands. Retrieved 17 May 2021.

13. Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.

14. "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.

15. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53. ISBN 9781438110196.

16. "Cybercriminals Need Shopping Money in 2017, too! - SentinelOne". sentinelone.com. 28 December 2016. Retrieved 24 March 2017.

17. Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on 6 July 2011.

18. Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Archived from the original on 25 September 2015. Retrieved 20 September 2015.

19. "Kaspersky Security Bulletin 2016. The ransomware revolution". securelist.com. Retrieved 17 May 2021.

20. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021". Cybercrime Magazine. 19 October 2018. Retrieved 17 May 2021.

21. Carback, Joshua T. (2018). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin. 54 (1): 64–183. p. 64.

22. "IJM Seeks to End Cybersex Trafficking of Children and #RestartFreedom this Cyber Monday and Giving Tuesday". PR Newswire. 28 November 2016.

23. "Cybersex Trafficking". IJM. 2020.

24. "Cyber-sex trafficking: A 21st century scourge". CNN. 18 July 2013.

25. "Senator warns of possible surge in child cybersex traffic". The Philippine Star. 13 April 2020.

**Corresponding Author**

**Harsh Gopalia***

Research Scholar, Maharishi Arvind University, Jaipur-302041