CYBER CRIMES IN INDIA : AN ANALYSIS

Christopher Lalchhandama [iD]* **& T. Sadashivam**

Department of Public Administration, Mizoram University, Aizawl, India

*✉ chrisdamdama1409@gmail.com

[iD] Christopher Lalchhandama: https://orcid.org/0009-0004-2666-9922

ABSTRACT

Due to globalization, India has opened its windows to the outside world which has led to the development of technology. Internet has been rapidly developed in the last two decades and especially, in the latter part of the last decade, its growth has been exponentially high. This paper will focus on the evolution of the internet, and how it has led to cyber crimes and its various aspects. Also, it discusses the cyber crimes in India which have been increasing with the help of data from the National Crime Records Bureau (NCRB).

Keywords: *Cyber Crimes, Cyber criminals, Data, Technology, National Crime Records Bureau.*

Introduction

Cyber crime is the use of computer, mobile phones, tablets, and any electronic gadget which can access the internet as an instrument to commit crimes. It can be committing fraud, stealing money, stealing intellectual property, human trafficking, child pornography, and identity theft. Cyber crimes have been on the rise in the past decade and is a concerning issue which has targeted individuals, private companies, and the government as a whole. The increased use of the internet without proper knowledge has caused an increase in the rate of cyber crimes. The rise of a covid-19 pandemic in the early part of the year 2020, has increased the usage of electronic gadgets and the internet to a whole new level. Schools were attended in online mode, and people worked from home using applications like Zoom or Google Meet, etc. This has hugely increased the rate of cyber crimes and cyber criminals have been on the loose without being caught. Cyber criminals haven't left anyone out, be it men, women, or children, all have become targets. India being the largest populated country in the world has a huge number of cyber crimes happening all over the country.

Studies and data shows that India has a huge way to go in terms of cyber security to reduce cyber crimes happening in the country. Cyber crimes are not attacks on a physical body but on a virtual body through an electronic gadget which can mentally affect the individual, target corporations and even governments. The internet offers criminals several places to hide in the real world as well as on the internet. Cyber crimes have been neglected to an extent that the cyber criminals have no fear of themselves being suspected or being caught. But with the increase in the need for cyber security, the government has taken steps to reduce cyber crimes happening all over the country (Sunday Times, August 2023).

Evolution of Cyber Crimes

Technology has been a rapidly growing sector for the past thirty to forty years. The internet was developed around the early 1960's has had a slow growth rate by the end of the 20th century. Hacking was first recorded in the early 1970s when computerized phones were the main targets. The "Phreakers" who were technology-savvy people were the first hackers who were known to modify the software and hardware inside a computer (Panda Media Center 2023). In 1990 a project called 'Operation Sundevil' where a total of 42 computers and over 20,000 floppy disks were confiscated as they were used by criminals for several illegal purposes. When Tim Berners-Lee invented the Worldwide Web (www) in 1994 which was mainly aimed and developed for automated information-sharing, it has paved the way for the rapid growth of the internet in the

United States and also in the global picture (CERN). With the advent of globalization in the late 1990's, India has opened up to the global economy which has led to a rise in technological advancement. The mobile phones were introduced in the year 2004 which is an important stepping stone in the technological industry. People can easily buy mobile phones as they are affordable in price and the cheap availability of data plans is also a huge factor. As time passed, the usage of mobile phones has increased to an uncountable rate that in 2023 almost every member of a family has one for him/herself. The covid-19 pandemic from the year 2020 has led to a high increase in the use of mobile phones and other gadgets as students need to attend classes from their phones.

The growth of technology has had several advantages and disadvantages. It has led to getting things done easier through the internet and technology more importantly the online financial transactions. It has led to easier processing and storing of data in computers. Also, it has helped to communicate with people living in other countries easily through applications like WhatsApp, Facebook, Instagram, and so on. On the other hand, there are several disadvantages that the internet has brought about where a computer or a mobile phone has been used as a tool for committing crimes to a large extent. Cyber criminals can easily practice criminal activities without them being caught. With the gradual rise of the internet, this was bound to happen. Gateways were opened and there were more rooms for committing cyber crimes. Hackers became more and more skilled which became deep threats to the system. Few

companies have even hired hackers so that they can win against their competing companies.

In India, the first case of cyber crime occurred in 1999 when Akash Arora was accused of using a domain named 'yahooindia.com' which was known as Yahoo Akash Arora case (IPleaders, 2021). Since then, it has spread its wings all across the country. Several researches have been carried out to study the number of cyber crimes happening in the country. A treaty on cyber crime after years of discussion by the United Nations was finally on the way. The United Nations General Assembly in December 2019 voted for the negotiation of a treaty on cyber crime which has the potential to develop numerous policies on a global front by giving significance to human rights (United Nations, 2022).

Concept of Cyber Crimes

Generally, there is no international definition of cyber crime or cyber attacks. According to the United Nations Office on Drugs and Crime, 'the offences typically revolve around the following categories: offences that are computer-related and content-related and offences related to infringements of copyright' (United Nations, 2022). Cyber Crimes can be defined as the use of a computer as a weapon for illegal ends crimes such as committing frauds, identity theft or breaching privacy. It refers to the unlawful acts wherein the computer is either a tool or target or both. Mirriam-Webster dictionary has defined cyber crime as 'crime such as fraud, theft or intellectual property violations or distribution of child pornography committed electronically' (Mirriam-Webster Dictionary, 2023).

Types of Cyber Crimes:

Several types of cyber crimes have been practiced by cyber criminals. Some of them are:

- **Phishing**: It is a type of crime that involves stealing information from individuals through e-mails who claim they have won a lottery or huge sums of money.

- **Identity theft**: Individuals are tricked into giving away their personal information which is then further used for criminal acts by cyber criminals.

- **Cyber Bullying**: This is a form of bullying, that is carried out using computers and mobile phones where the individual is bullied and harassed. This can cause mental issues in the individual.

- **Child Pornography**: This refers to the creation or distribution of sexually explicit photos and videos of underage children.

- **Cyber Stalking**: It involves online harassment where the cyber stalkers use social media as a main source of to carry out cyber stalking. Lots of online messages and emails are spammed to the user which is done to instill fear in the individual.

- **Cyber Vandalism:** It means destroying or damaging the data or information in a computer when a

network service is stopped or disrupted.

- **Ransomware:** It is a computer malware that encodes the files stored desktops, laptops, mobile phones, etc. and gaining access to their data or information and holding them hostage. The victim is blackmailed into paying the demanded ransom (money) to give his data or information back.

- **Online Scams:** They are usually in the form of ads or emails which seem to include good rewards of high amounts of money or gadgets. When clicked on the link, it can inject malware and virus or even steal the user's money.

- **Espionage:** It is the act of obtaining data and information without the permission and knowledge of the owner.

- **Online Sextortion:** It is used as a method for threatening individuals by planning to send private and sensitive material through an electronic medium if he/she does not provide money or sexually explicit images.

Cyber Crimes in India

There are several cases of cyber crimes happening in the country. The National Crime Records Bureau (NCRB) under the Ministry of Home Affairs, Government of India is responsible for providing data on cyber crimes in India. The Table 1 shows the number of cyber crimes in the last three years from the year 2019-2021 (as per the latest available data).

In the year 2019, the state of Karnataka had the highest number of cyber crime cases followed by Uttar Pradesh. Both Sikkim and Nagaland have the least amount of cyber crimes in the Northeast region of India. Among the Union Territories, Delhi has the highest number of cyber crime cases recorded, with Ladakh being the only Union Territory to have zero cyber crime cases in 2019. In 2020, Uttar Pradesh leapfrogged Karnataka to become the state with the highest number of cyber crime cases recorded but the number of cases in Uttar Pradesh was lower by 319 in comparison with the year 2019. The state of Karnataka also had a slight decrease in the cyber crime cases in 2020 with 1279 fewer cases. The state of Sikkim was the only one amongst all the states/UTs in India that had zero cyber crime in 2020. Among the Union Territories, Delhi again was the highest with 53 more cyber crimes than the previous year and, Ladakh had one cyber crime case. The increase of the total cyber crimes among the states in India in 2020 from the previous year i.e. 2019 was 5197 cases, and the UTs also had an increase of 103 cases in 2020 from the previous year. In 2021, Telangana topped the list with 10303 cases followed by Uttar Pradesh (8819) and Karnataka (8136) both had a significant decrease in comparison with the previous two years i.e. 2019 and 2020. Sikkim was again the only state with no cyber crime case. The total number of cyber crimes among the states in the past three years (2019-2021) was a whopping 1,46,649 cases. Among the Union Territories, Delhi for the third straight year holds the highest number with 356 cyber crime cases and, Puducherry had no cyber -

Table 1: Cyber Crimes in India (States/Union Territories wise) from 2019 to 2021

SL	States/Union Territories	2019	2020	2021
1	2	3	4	5
States				
1	Andhra Pradesh	1886	1899	1875
2	Arunachal Pradesh	8	30	47
3	Assam	2231	3530	4846
4	Bihar	1050	1512	1413
5	Chhattisgarh	175	297	352
6	Goa	15	40	36
7	Gujarat	784	1283	1536
8	Haryana	564	656	622
9	Himachal Pradesh	76	98	70
10	Jharkhand	1095	1204	953
11	Karnataka	12,020	10,741	8136
12	Kerala	307	426	626
13	Madhya Pradesh	602	699	589
14	Maharashtra	4967	5496	5562
15	Manipur	4	79	67
16	Meghalaya	89	142	107
17	Mizoram	8	13	30
18	Nagaland	2	8	8
19	Odisha	1485	1931	2037
20	Punjab	243	378	551
21	Rajasthan	1762	1954	1504
22	Sikkim	2	0	0
23	Tamil Nadu	385	782	1076
24	Telangana	2691	5024	10,303
25	Tripura	20	34	24
26	Uttar Pradesh	11,416	11,097	8829
27	Uttarakhand	100	243	718
28	West Bengal	524	712	513
	Total States	44,511	49,708	52,430
Union Territories (UTs)				
29	Andaman & Nicobar Islands	2	5	8
30	Chandigarh	23	17	15
31	D&N Haveli and Daman & Diu	3	3	5
32	Delhi	115	168	356

33	Jammu and Kashmir	73	120	154
34	Ladakh#	NIL	1	5
35	Lakshadweep	4	3	1
36	Puducherry	4	10	0
	Total UTs	224	327	544
	Total All India	44,735	50,035	52,974

Note: #Ladakh was a newly created Union Territory in 2019

Source: Crime in India Report 2021, Vol-II, National Crime Records Bureau, Ministry of Home Affairs, Government of India, p. 785

crime case in the year 2021. The total number of cyber crime cases in the Union Territories from (2019-2021) was 1095. The total number of cyber crime cases covering both the State and the Union Territories between the year 2019-2021 was 1,47,744 cases.

Conclusion

The evolution of the internet has made cyber crimes inevitable. People all over the world are accustomed to the use of internet and we have even made it a necessity in our daily life. The United Nations has also taken steps to develop policies on the cyber crime front. Cyber crimes will not be erased completely as long as the internet is present. The pandemic had changed our lives completely and has increased the cyber cases in India. Even though the Information Technology Act has been passed, cyber crimes have not been tackled completely in India. The government should take steps to educate the people in regards to the security against these cyber crimes which can go a long way in tackling cyber crimes in the future. A digital literacy scheme implemented by the Central Government named Pradhan Mantri Gramin Digital Saksharta Abhiyaan (PMGDISHA) was approved in February 2017 for the sole purpose of making six crore rural persons digitally literate (Sadashivam, 2020). Cyber crime has been a serious issue and should be given more and more importance as our world is becoming more and more digitalized.

References

CERN. A short history of the Web. Retrieved from: home.cern/science/computing/birth-web/short-history-web on 29th August 2023.

ClearIAS (2021). Cybercrime- Definition, Types and Reporting. Retrieved from: www.clearias.com/cybercrime/ on 24th August 2023.

IPleaders (October 29 2021). Critical analysis of cyber crime in India. Retrieved from: blog.ipleaders.in/critical-analysis-cybercrime-india/#:~:text=The%20first%20cyberc

rime%20occurred%20in%201992%20 when%20the,a%20permanent%20inju nction%20was%20sought%20in%20th is%20case. On 29th August.

Mirriam Webster (22 August 2023). Definition of cyber crime. Retrieved from: www.merriam-webster.com/dictionary/cybercrime on 31st August 2023.

National Crime Records Bureau (2021) Crimes in India Vol II. Annual Report. Ministry of Home Affairs. Pg-785. Retrieved from ncrb.gov.in/sites/default/files/CII-2021/CII_2021Volume%202.pdf on 25th August 2023.

Panda Media Center. Panda Security (2023) Types of Cybercrime. Retrieved from: www.pandasecurity.com/en/mediacent er/panda-security/types-of-cybercrime/ on 23rd August 2023.

Sadashivam, T. (2020). Cyber Crime in India: An Introspection. *Studies in Indian Place Names, 40*(60).

Sunday Times (6th August 2023). There is no doubt, fake news causes real harm. Sunday Times English Newspaper, Pg-5, Volume 10, No 31.

United Nations (2022). A UN treaty on cybercrime en route. Retrieved from: unric.org/en/a-un-treaty-on-cybercrime-en-route/ on 27th August 2023.