ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

CYBER LAW AWARENESS AMONG YOUTH TO ERADICATE CYBERCRIME WITH SPECIAL REFERENCE TO DELHI-NCR

Dr. Aradhana Chadha
Assistant Professor, Swami Shraddanand College.
University of Delhi, Delhi

ABSTRACT

Due to the fact that cybercrime is becoming a worldwide phenomenon, it is impossible to generalise crimes committed across the country given the current state of affairs. Alongside the widespread lack of awareness regarding internet use, a disturbing new trend that has emerged on the scene is cyber crime. The development of computers has made a number of human activities and requirements significantly easier. Criminals were given access to new methods of operation, which are collectively referred to as cybercrime, when they discovered that it was possible to share data and information on such a massive scale. This was a novel method of exhibiting criminal tendencies on a broad scale without even making use of a firearm or other physical weapon. At any given time, millions of people are impacted by criminal activity committed online. Its rapid mode of operation, in conjunction with the fact that it can inflict harm on a massive number of people all at once, contributes to the fact that it poses a significant threat. This can be done by outlining a behavioural profile from the key personality characteristics. In the present paper, an attempt is made to do the same thing. The researcher conducted in-depth interviews with a sample of sixty students who had prior academic experience and used a questionnaire with a set of predetermined questions. The main objective of the research is to create awareness of cyber law among youth to eradicate cybercrime with special reference to Delhi-NCR. In addition, the purpose was to identify the common themes that emerged from their responses with regard to the personality traits of cyber-criminals & questioned by the researcher in order to gain insight into their beliefs concerning the identifiable characteristics that are associated with a cyber-criminal. A behavioural profile of a cybercriminal was created by compiling data from a variety of sources into a small number of recurring themes. These themes were then used to construct the profile. The analysis was carried out with the assistance of SPSS by means of a one sample t-test.

Keywords : Cyber-Crime, Cyber Law, Delhi, NCR, Security, Awareness

INTRODUCTION

The world is relatively new to the concept of cyber-crime as a kind of criminal based activity. The most widespread form of criminal activity that plays a devasting role in Indian modernisation is cyber-crime. Not only are criminals responsible for enormous financial losses incurred by society as a whole and the government, but they are also highly skilled at keeping their identities hidden. On the internet, technically savvy criminals carry out a variety of illegal activities. These criminals are involved in a number of illegal activities. When viewed from a more expansive perspective, the term "cybercrime" can be understood to refer to any illegal kind of activity in which a computer based or the internet is used in some capacity, whether as a tool, a target, or both.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

In some of the judgements that have been handed down by courts in India, the term "cybercrime" may be interpreted in a legal sense; however, the term has not been defined in any act or statute that has been passed by the Indian Legislature. The misuse of people's ever-increasing reliance on computers in today's modern life is the root cause of the uncontrollable evil that is cybercrime. The demand for the use of computers and other related technologies in day-to-day life is rapidly increasing, and this has turned the convenience they provide into an addiction for users. It is a medium that cannot be measured and possesses infinite scope. No matter how many positive things the internet does for us, it also has a number of negative aspects. 1 The terms "cyberstalking," "cyberterrorism," "e-mail spoofing," "e-mail bombing," "cyberpornography," and "cyberdefamation," among others, are examples of some of the more recent types of crimes that have emerged online. If they are carried out using a computer or the Internet, traditional crimes may be included in the scope of the term "cybercrime," along with other types of illegal activity.

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)

Nature and Scope of Cyber Crime

There is a strong link between society and criminal activity. No matter how hard we try, we will never live in a society that is free from the effects of cybercrime. In a practical sense, given that we are not yet capable of bringing the rate of crime in the real world down to the desirable minimum rate in the virtual world, given that it is comparatively more unreal, everlasting, and legally less controllable than the real world. Nevertheless, the nature of crime, its scope, and definition all shift over the course of time in any given society. There is no such thing as a crime-free society, and crime cannot exist in isolation from a society. Therefore, the nature of a society determines the nature of the crime that occurs in that society. The complexity of a society is directly correlated to the complexity of the criminal activity that evolves around that society.

The socioeconomic and political structure of the society needs to have a better understanding of crime and the means by which it can be prevented, so that appropriate action can be taken. When investigating the origins and repercussions of a criminal act, it is important to take into account the preventative and corrective steps taken by the institutions that are responsible for maintaining social order and policing criminal behaviour in the community. The development of technology has resulted in new socio-economic and political problems in society. However, rather than assisting the state in its efforts to control the problems, the advancement of technology has resulted in the creation of a new complex situation that is difficult to comprehend and even more challenging to apply existing law to in order to deal with the situation. It has not only made life more convenient, but it has also significantly assisted in bringing different parts of the world closer together on social, economic, and cultural levels.

Because of advancements in computer technology, it is now possible to travel to any part of the world while remaining seated in a single location. The advancement of technology has eliminated the limitations imposed by both time and space. On the other hand, despite the remarkable benefits of having computers available today, the legal system has experienced the creation of a jurisdictional issue as a result of this. When conducting international business over the internet, determining which country's laws apply can be one of the more challenging aspects.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

This is due to the fact that our machinery is not compatible with dealing with transnational crimes. Since the nature of cybercrime is very different from that of traditional crime, the law that applies to the region is not sophisticated enough to be able to regulate it effectively. As a result, the fact that cybercrime is committed on a global scale makes it difficult to handle and prosecute. The development of internet technology has provided us with many benefits, including the ability to solve future problems and increase our rate of growth, but it has also made it easier for criminals to commit their acts while minimising the likelihood that they will be discovered. The internet has been a blessing in disguise for people who engage in questionable behaviour in society. The idea of committing crimes online has been picking up steam, and there is a significant risk that its effects will have an adverse effect on global society. Because of increasing reliance on digital tools, human society is increasingly at risk of being victimised by criminals operating online.

Characteristics of Cyber Crime

The idea of committing crimes online is quite distinct from the more conventional criminal activity. As a result, it is essential to investigate the peculiar characteristics of cyber crime.

1. Individuals with specialised knowledge of Cybercrimes, an individual must have a high level of expertise in internet and computer use in addition to internet use. Because those who have committed cybercrime have a high level of education and an in-depth knowledge of the functionality of the internet, the work of the police machinery to combat those who have committed cybercrime has become extremely difficult as a result.

2. Obstacles posed by geography – In cyberspace, the boundaries of physical space are effectively eliminated, in a matter of minutes while sitting in any part of the world. Take, for instance, the case of a hacker in India who breaks into a system located in the United States.

3. The Virtual World – The act of committing a cyber-crime takes place in the cyber spaces, while the offender who is physically committing the act is located outside of the cyber space. Every step that the criminal takes during the commission of the crime is carried out within the context of the virtual world.

4. The magnitude of the crime is incomprehensible. The potential for harm and loss of life that can be caused by cybercrime is of a magnitude that cannot be conceived of. Crimes committed online, such as cyber terrorism and cyber pornography, for example, have a wide reach and the potential to destroy websites and steal data from businesses in a short amount of time.

5. The Different Types of Online Criminality In this chapter, the researcher investigates the ways in which computers and other forms of technology can be used to commit illegal acts. Typically, these kinds of activities involve the adaptation of traditional criminal behaviour through the utilisation of various forms of information technology.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

Source[*1]

Fundamental elements of Cyber Crime

Actus Reus and Mens Rea are the two most essential elements of a crime that need to be demonstrated in order to establish a person's guilt in relation to a criminal offence. The actus reus of cybercrime is extremely fluid and diverse in its presentation. Actus Reus is notoriously difficult to establish in the context of cybercrime. It is impossible to prove without first demonstrating that consent or permission was not granted. Mens rea consists of two main elements in the case of cybercrime: first, there must be an intend to get the data from a certain device; second, the knowledge of actus reus should be there when committing the crime. whereas, in the case of traditional crimes, mens rea consists of a single element.

Review Literature

In Samresh Bose v. Amal Mitra, the Supreme Court has held that "A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novels, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences". "the Judge should ... place himself in the position of a reader of every age group in whose

[11] https://nhrc.nic.in/sites/default/files/Group%201_FEB%202022.pdf

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers"

According to a recent ruling from the Supreme Court, "a vulgar writing is not necessarily obscene. Although vulgarity can cause feelings of disgust and revulsion, as well as boredom, it does not have the effect of depraving, debasing, or corrupting the morals of any reader of the novels. On the other hand, obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences. In this particular case, the court distinguished between vulgarity and obscenity and went on to hold that in order to properly judge the question of obscenity, "the Judge should... place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers" (Source)

Section 67 of the Information Technology Act of 2000 is analogous to Section 292 of the Indian Penal Code, 1860. State of Maharashtra, it was decided that unlike other provisions, which have words like "knowingly" or "negligently" and thus make mens rea a condition precedent to establish guilt, the provision at issue in Ranjit D. Udeshi v. State of Maharashtra established that mens rea is necessary to prove guilt. The knowledge of an obscenity is not a requirement for the commission of the offence under Section 292. The prosecution does not provide evidence to support a requirement that is not imposed on it by the law. Because it is difficult to obtain legally sufficient evidence of the offender's knowledge of the obscenity of the book, etc., the liability has been made extremely stringent. The lack of such knowledge may be taken into consideration as a mitigating factor, but it does not remove the case from the provisions of the provision.

If we apply the judgement from the Ranjit D. Udeshi case (supra) to Section 67 of the Information Technology Act of 2000, we can reach the conclusion that the simple publication and transmission of obscene material constitutes an offence, regardless of the mental state of the offender. On the other hand, this can't be a universal law that applies to everyone and anyone (Source).

The court noted that the literature of India, both religious and secular, is replete with sexual allusions, sexual symbolisms, and passages of such overt eroticism, the likes of which are not to be found anywhere else in the literature of the world. This was said to be the case despite the fact that India is a predominantly religious country. It went on to say that "While an artist should have creative freedom, he is not free to do anything he wants" (while an artist should have creative freedom, he is not free to do whatever he wants). The need for a line to be drawn is between art as an expression of beauty and art as an expression of a sick mind intoxicated with a vulgar manifestation of counterculture, the latter of which needs to be kept away from a civilian society. Art as an expression of beauty should be allowed in civilian society, but art as an expression of an ill mind intoxicated with a vulgar manifestation of counterculture should not Another statement made by the court was along the lines of "there should be freedom for the thought we hate." If there isn't freedom after speech, then "freedom of speech" doesn't mean anything at all. The degree to which freedom and tolerance are extended is one way to evaluate the degree to which democracy is actually practised (Source).

Research Methodology

Twenty people from Delhi and the National Capital Region (NCR) were selected to take part in the study. They were students whose primary academic backgrounds were in the fields of social science, commerce, and management. The participants' ages ranged anywhere from 18 to 24 years old and even higher in some cases. There was an effort made to ensure that there was an equal number of male and female participants. The participants who agreed to take part in the study were those who

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

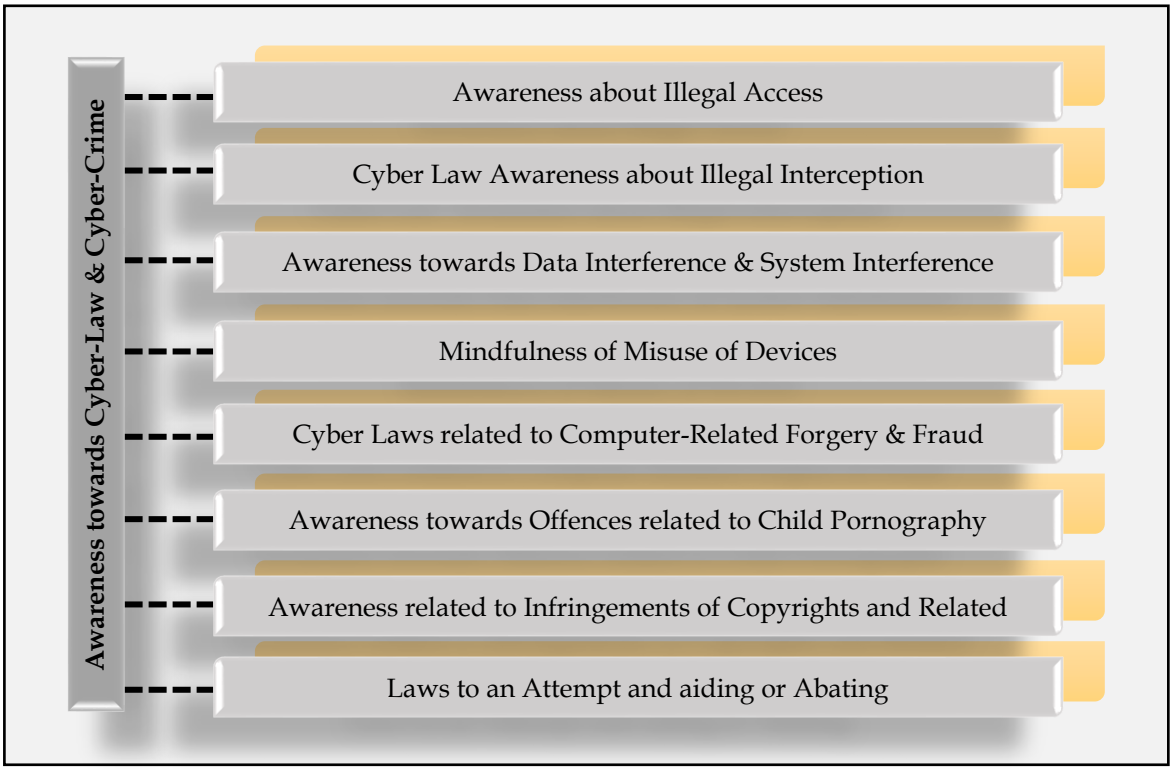
demonstrated an awareness and familiarity with the concept of cybercrime on some level. They participated in online activities on a regular basis, making them qualified participants in light of the objectives of this study. The current study aimed to collect the perspectives of students in order to create a profile of cybercriminals, and it was successful in doing so. In order to accomplish this goal, the participants were subjected to a lengthy questionnaire full of specific questions. They were specifically asked to identify the characteristics that, in their opinion, were inherently present in cyber criminals and that could be understood as precursors to criminal behaviour. The interviews were, for the most part, unstructured to make it easier for people to freely share information with one another and to leave room for the researcher to conduct more in-depth questioning as and when it was necessary. In order to come up with characteristics of cyber criminals, they were tasked with drawing on both the academic knowledge they possessed and the personal experience they had gained.

Objectives of the study

1. To explain major kinds of cyber-crimes and related laws in India.
2. To analyse major variables towards awareness of cyber laws & cyber-crimes.
4. To recommend measures and reforms necessary for cyber laws among youth.

Hypothesis of the Study

- There is significant relation among awareness of cyber laws & cyber-crimes among youth in Delhi NCR”
- There is no significant relation relation among awareness of cyber laws & cyber-crimes among youth in Delhi NCR



ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

Figure 1 : Proposed Framework of the Study

Result and Discussion

Demographic Analysis

Table 1: Demographic Analysis

Demographic Analysis

Gender		**Frequency**	**Percent**
	Male	47	78.33
	Female	13	21.66
Age	18-20	16	26.66
	20-22	24	40.00
	22 -24	15	25.00
	24 & above	05	8.33
Stream/Domain	Social Science	25	41.66
	Commerce/Management	35	58.33
Education Level	Graduation	20	33.33
	Post-Graduation	35	58.33
	Others	05	8.33

Table 2: Descriptive Statistics

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Awareness about Illegal Access	60	1	5	3.78	.721
Cyber Law Awareness about Illegal Interception	60	1	5	2.46	.687
Awareness towards Data Interference & System Interference	60	1	5	3.59	.810
Mindfulness of Misuse of Devices	60	1	5	3.24	.779
Cyber Laws related to Computer-Related Forgery & Fraud	60	1	5	3.96	.718
Awareness towards Offences related to Child Pornography	60	1	5	4.18	.832
Awareness related to Infringements of Copyrights and Related Rights	60	1	5	2.31	.723
Laws to an Attempt and aiding or Abating	60	1	5	2.67	.754
Valid N (listwise)	60				

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

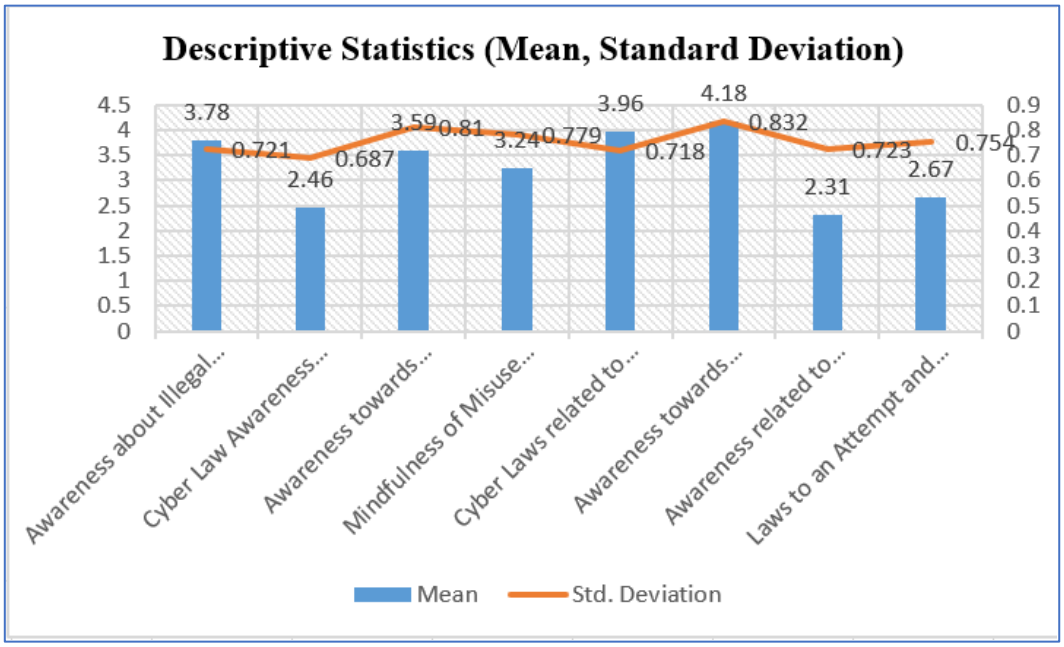


Figure 1 : Descriptive Statistics (Mean, Standard Deviation)

Table 2 depicted the descriptive analysis and identify that majority of respondents focusing on Awareness towards Offences related to Child Pornography (Mean=4.18 and standard deviation=.832) followed by Cyber Laws related to Computer-related Forgery & Fraud (Mean=3.96 and standard deviation=.718). Where, Awareness about Illegal Access (Mean=3.78 and standard deviation=.721), Awareness towards Data Interference & System Interference (Mean=3.59 and standard deviation=.810) & Mindfulness of Misuse of Devices (Mean=3.24 and standard deviation=.779) & Laws to an Attempt and aiding or Abating (Mean=2.67 and standard deviation=.754). The least values of mean falls in Cyber Law Awareness about Illegal Interception (Mean=2.46 and standard deviation=.687) & Awareness related to Infringements of Copyrights and Related Rights (Mean=2.31 and standard deviation=.723). Therefore, findings of the study stated that for youth of Delhi NCR (Belonging to sampled study of social science, commerce & management field) are very much aware of such cyber crimes & cyber laws.

Table 4: One-Sample Test

One-Sample Test	
	Test Value = 0

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

	T	Df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Awareness about Illegal Access	91.301	60	.000	3.114	3.13	4.19
Cyber Law Awareness about Illegal Interception	63.613	60	.000	3.217	3.56	4.25
Awareness towards Data Interference & System Interference	88.127	60	.000	2.614	3.17	4.23
Mindfulness of Misuse of Devices	74.362	60	.000	4.019	3.10	4.47
Cyber Laws related to Computer-Related Forgery & Fraud	98.013	60	.000	3.921	3.18	4.54
Awareness towards Offences related to Child Pornography	103.602	60	.000	3.702	3.10	4.26
Awareness related to Infringements of Copyrights and Related Rights	59.128	60	.000	3.117	3.23	4.39
Laws to an Attempt and aiding or Abating	71.225	60	.000	2.986	3.27	4.17

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

Above table 3 depicted the t-test and identify that majority of respondents Aware towards Offences related to Child Pornography (t=103.602) followed by awareness towards Cyber Laws related to Computer-Related Forgery & Fraud (t=98.013). Respondents then more focused about Awareness about Illegal Access (t=91.301). Therefore, findings of the study stated that for youth of Delhi NCR (Belonging to sampled study of social science, commerce & management field) are very much aware of such cyber-crimes & cyber laws.

Hypothesis Testing:

The findings of t test analysis stated that majority of respondents are having significant relation to be aware of child pornography, cyber laws for forgery & fraud & illegal access of the things. So the alternate hypothesis that "there is significant relation among awareness of cyber laws & cyber-crimes among youth in Delhi NCR" is accepted & null hypothesis that "there is no significant relation relation among awareness of cyber laws & cyber-crimes among youth in Delhi NCR is rejected at the same time".

Findings of the study

- Utilization of encryption software by Information Security Officers, who are tasked with being responsible for the overall protection of the organisation
- Treaties and agreements reached on a global scale can be leveraged to present a united front. makes certain that all applicable local legislation is in harmony with international laws and conventions
- Establish progressive programmers for capacity building for national law enforcement agencies.
- Relationships that are mutually beneficial between corporations, governments, and civil societies in order to fortify legal frameworks for cyber-security.

Recommendations

1. Raising people's awareness of information security issues and improving their skills in this area

2. Establish an official framework for the coordination and prioritisation of research and development in the field of cyber security

3. Establish a testing and certification programme for information technology security systems.

4. Create, encourage, and uphold a culture of cyber security at the national level

5. Efforts to standardise and coordinate efforts regarding the cybersecurity education and awareness programme

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

Conclusion

Since cybercrime is becoming a worldwide phenomenon, a nationwide generalisation of criminal activity is no longer applicable in the context of the current situation. Understanding and regulating cybercrime cannot be done on a national level; rather, they require an international approach. Only by passing brand-new legislation and developing both preventative and reactive measures on a global scale will we be able to shield our culture from the threat posed by the phenomenon known as "Cyber Crime." As a result, the world and its agencies face a significant obstacle in the form of the threat posed by cyber terrorism. The use of technology by terrorist organisations to incite hatred among the general population, as well as to recruit potential militants and provide educational resources for said recruits, They are also setting up websites that teach people how to use weapons, make bombs, and other such things.

The incidence of cybercrime is rising at an exponential rate across the world, including in India. Infringement of intellectual property rights, cyber terrorism, cyber extortion, and sexual harassment are some of the types of crimes that can occur in cyberspace. These crimes have been thoroughly examined in this paper within the context of Indian jurisprudence. In addition to this, the paper offered a comparative analysis with the New challenges that are encountered in cyber security in electronic networks. It is time for the legal system in India to pick up the pace with the increasing number of cyber crimes and the growing international jurisprudence surrounding it. In this age of information, there are opportunities for growth for those who are best able to utilise both technology and information. Because of the pandemic caused by COVID-19, the need for this change has become more pressing and essential. Statutory laws, government policies, and specialised investigative agencies will all go a long way toward securing cyberspace in India. Programs designed to raise people's awareness of their legal rights should provide them with the information necessary to enable them to defend themselves against the dangers posed by online criminals. There have been no confirmed cases of pure cyber terrorism to date; however, given the fact that critical infrastructures across the states suffer from significant security flaws, its occurrence may only be a matter of time before it takes place.

References

1. Alexander P.J. (2002) “Policing India in the New Millennium”, Allied Publication, New Delhi
2. A.K. Shrivastav & Dr. E. (2013), ICT Penetration and Cybercrime in India: A Review, International Journal of Advanced Research in Computer Science and Software Engineering A. Sen (2013), Linking Cyber Crime to the Social Media: A Case Study of Victims in Kolkata, Scientific Committee of Reviewers, 378.
3. Bidgoli Hussein (2004) “The Internet Encyclopedia, Vol.1”, John Wiley & Sons Publication, New Jersey
4. Clough J. (2010) “Principles of Cybercrime”, Cambridge University Press, New York
5. D. Halder, & K. Jaishankar (2011), Cyber crime and the victimization of women: laws, rights and regulations, Information Science Reference.
6. Grabosky Peter & Roderic Broadhurst. (2005) “Cybercrime: The Challenge in Asia”,Hong Kong University Press, Hong Kong
7. Kamath Nandan. (2009) “Law relating to Computers, Internet and E-commerce”, Universal Law Publication, Delhi.
8. Prof. R.K.Chaubey, “An Introduction to Cyber Crime and Cyber law”, Kamal Law House, 2012, p. 440 .
9. Samresh Bose v. Amal Mitra , AIR 1986 SC 967
10. Sood Vivek (2001) “Cyber Law Simplified”, Tata McGraw-Hill Publication, New Delhi

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,S Iss 1, Nov 2022

11. Waelde, Lilian Edwards and Charlotte (2009), "Law and the Internet", Hard Publication, Portland
12. Wall David (2001) "Crime and the Internet-Cyber crimes and Cyber fears" Routledge Publications, London.
13. *http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf*
14. 27 AIR 1965 SC 881