STUDY OF CHHATTISGARH'S CYBERCRIME RATE

Dr. Sneh Kumar Meshram Assistant ProfessorDepartment of Sociology, Bharti Vishwavidyalaya, Durg, Chhattisgarh, India

Abstract

Analyzing the harm that cybercrimes pose to society is the goal of the investigation. As examples of some of the effects caused by cybercrime activities, the concepts of cybercrimes are provided, and various types of cybercrimes are studied. The findings of this inquiry demonstrate that there are numerous negative repercussions of cybercrimes that are felt by the general population, which is why computer or systems administration are targets for violations. The discoveries are used to generate the conversations.

The majority of information is now processed online, making it vulnerable to cyber dangers. Cyber dangers abound, and because it is impossible to predict their behavior in the early stages of an attack, it is also challenging to stop them. Cyberattacks could be motivated in some way since they might be carried out unintentionally. The processing of attacks with knowledge is what is known as cybercrime, and it has major repercussions on society in the form of economic disruption, psychological disorder, threat to national security, etc. The ability to limit cybercrimes depends on an accurate understanding of their behavior and the effects they have at different societal levels. In this manuscript we are focusing on the enhancing rates of Cybercrimes in Chhattisgarh.

Keywords: *Cybercrime, Cyber Attacks, Types of Cybercrime, Effects of Cybercrime.*

1.INTRODUCTION

A separate independent state was requested by the local populace, and Chhattisgarh was established on November 1, 2000 a part from Madhya Pradesh. With a population of almost 25.5 million, the state of Chhattisgarh ranks as the 16th most populated in all of India.The land area of Chhattisgarh is 135,190 sq. km, making it the tenth largest state.

Although the word "cyber-crime" has no universally agreed-upon definition, it is used in this paper to refer to "any crime that is assisted or performed utilising a computer, network, or hardware device."

Networked computers and other information and communication technologies provide quick, anonymous, secure, and inexpensive multi-media communication. They may be utilised as a means of organisation and communication to further develop already-existing criminal activities, offer fresh methods for carrying them out, broaden their geographic scope, or invent new categories of criminal activity.

Online Crime Since the beginning of the digital age, criminals have used computers to facilitate their illicit acts. Criminals use computers in much the same way that they would use a lockpicking instrument or a counterfeiting machine. Criminals have discovered that using computers allows them to maintain an anonymity that was before impossible in society.

Technology is already prevalent, and the Internet in particular is becoming more commonplace, with almost 3.2 billion people (nearly 40%) of the world's population now using it (International Telecommunications Union, 2015). Being an information superhighway, the Internet presents a wealth of opportunities for learning, networking, and communication. Nevertheless, it can also provide risks, particularly in relation to criminal behaviour, which has ramifications for both the real world and the virtual world. This article's goal is to explain how forensic phenomena have affected society in this new field.

Financial crimes, the sale of illegal goods, pornography, online gambling, crimes involving intellectual property, email spoofing, forgery, cyberdefamation, and cyberstalking are only a few examples of the activities that the computer may be utilised in. Unauthorized access to computers,

computer systems, or computer networks, theft of data contained inside are only a few instances in which the computer may be the object of illegal activity.

Cybercrime Subtypes :-

- **Hacking-**In plain English, "hacking" refers to unauthorised access to a computer system without the owner's or user's consent.
- **Denial-of-service assault**- This is a criminal conduct that deprives the victim of the services he is legally entitled to receive or offer by overburdening the victim's network with traffic or by flooding his email account with spam.
- **Virus Transmission**- malevolent programme that affixes itself to other software (malicious software includes viruses, worms, Trojan horses, Time bombs, Logic Bombs, Rabbits, and Bacterium).
- **Software theft**- Software theft is a felony that occurs when the unauthorised duplication of legitimate software or the production and sale of counterfeit goods that pass for the real thing. Global retail revenue losses are on the rise, and this crime can be committed in a number of methods, including end-user copying, hard disc loading, counterfeiting, illegal internet downloads, etc.
- **Pornography**- The first continuously profitable e-commerce product is pornography. Pornography entices clients to access their websites via deceptive marketing strategies and mouse trapping technologies. Anyone, even children, can use a computer to connect to the internet and click a mouse to view websites with pornographic material. According to Section 67 of the IT Act of 2000, it is unlawful to publish or send any anything in electronic form that is lewd or appeals to the desires of others.
- **IRC**- People from all around the world can congregate in chat rooms on Internet Relay Chat (IRC) servers to converse with one another. Criminals use it to connect with potential accomplices. It is used by hackers to share strategies and discuss their exploits.Chat rooms are used by paedophiles to seduce young children. In cyber stalking, a woman's phone number is provided to others on the pretence that she wishes to befriend a man in order to harass her.
- **Credit card theft**- For online transactions, all you need to do is type your credit card information into the merchant's web page. If electronic transactions are not secure, hackers may use this card fraudulently by pretending to be the cardholder.
- **Online extortion**- stealing the company's trade secrets in order to demand a large sum of money.
- **Phishing**- It is a method for tricking bank or financial institution account holders into divulging private information.
- **Spoofing**- Obtaining access to other computers on the network by convincing one computer on a network to assume the identity of another computer, typically one with specific access privileges.
- **Internet stalking**- In order to steal credit card details, the criminal routinely enters chat groups and sends emails to the victim.
- **Online slander-**The offender puts the defamatory material on a website or sends emails containing it to anyone who knows anything about the victim.
- **Threatening**- The offender contacts the victim in chat rooms or sends threatening emails. (Anybody who is dissatisfied with their boss, a friend, or an official may do this.)
- **Salami assault**- In these crimes, the perpetrator makes little adjustments in a way that prevents detection. The criminal creates a programme that withdraws a little sum, say once per month, from the accounts of all bank customers and puts it into his own account. In this

instance, no account holder would go to the bank for such a small sum, but the thief makes off with a sizable sum of money.

- **Sale of illegal drugs**- Online drug sales and purchases are both possible. There are websites that offer the sale and delivery of illegal drugs. They might conceal the messages using stenographic techniques.

2. LITERATURE REVIEW

- In 2022 Shobha Bhave in her PhD research work **Cyber Crime in Banking Sector the Study of Customers perception and Responses**focused on what are the perspectives of customers related to banking sector's cyber crime. She found that customer's opinion related to these crimes blaming on lack of updation of government for monitoring and securing the banking sector.
- In 2021 Durgesh Keswani in his PhD research work **A Critical Study of Cyber Crimes with Special Reference to Social Media in Central India**focused on social media related cyber crimes such as Profile Hacking, Photo Morphing, Offer and Shopping Scams, Romance and Dating Scams etc. Researcher stated that basically in central India region social media users are not so aware about safety and criminal factors about using of that means.
- In 2021 Akash Thakkar in his PhD research work **New approach for post exploitation analysis of cyber crime** focused his study on blackmailing and exploitation physical/ mental-emotional/ economical after the incident of cyber crime by making it base of exploitation. Our Indian Traditional social structure's respectability oriented mindset is one of the reason for such kind of post exploitation according to the researcher.
- In 2020 Indrajeet Singh in his PhD research work**A Critical Study of Cyber Crimes in India with Special Reference to Offence Against Women**focused onvarious aspectsthat are hidden behind cyber crimes which are related to women. In this study his research & analysis reveled the factors behind cyber blackmail, threats, cyberpornography, posting and publishing of obscene sexual content, stalking, bullying, defamation, morphing, and the establishment of fake profiles.
- In 2020 Narinder Singh in PhD research work **Cyber crime a study of Chandigarh**highlightedthe causeswhich are responsible for cyber related various crimes in Chandigarh such as Stolen credit card information, committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Researcher had minutely study the causes behind above mentioned cyber crimes which are lack of awareness about digitalization, cyber laws and monitoring loopholes.
- In 2019 Shiv Raman in his PhD research work **Cyber crimes in India issues challenges and strategies** focused on year wise data of cyber crime in India and it's various nature, orientation, new fields etc. Researcher had found that hackers from abroad are more active in India then as comparison to Indian hackers. He also stated how to resist cyber attacks by his research work.
- In 2014 V.S. Chowbe in his PhD research work **Legal Control of Cyber Crime in India** focused his study on which are the agencies in India for cyber crime control & how they manage and control the cyber crime. Researcher Stated that monitoring agencies such as National Cybercrime Threat Analytics Unit (TAU), National Cybercrime Reporting, Platform for Joint Cybercrime Investigation, National Cybercrime Forensic Laboratory (NCFL) Ecosystem, National Cybercrime Training Centre (NCTC), Cybercrime Ecosystem Management Unit, National Cyber Crime

ISSN: 2278-4632
Vol-13, Issue-05, No.02,May : 2023

Research and Innovation Centre etc. They are working efficiently to create awareness about cyber crimes and also for the quick action against such kind of incidence.

3. OBJECTIVE

Cyber crimes are various in their nature and it is now a well establish factor that it is also not easy to deal with them or to resist them. The objectives are here:-

- Study the rate of cyber crime in Chhattisgarh.
- Causes and effects of cyber crime in Chhattisgarh.

4. HYPOTHESIS

These are the hypothesis to study Chhattisgarh's Cyber crime rate:-

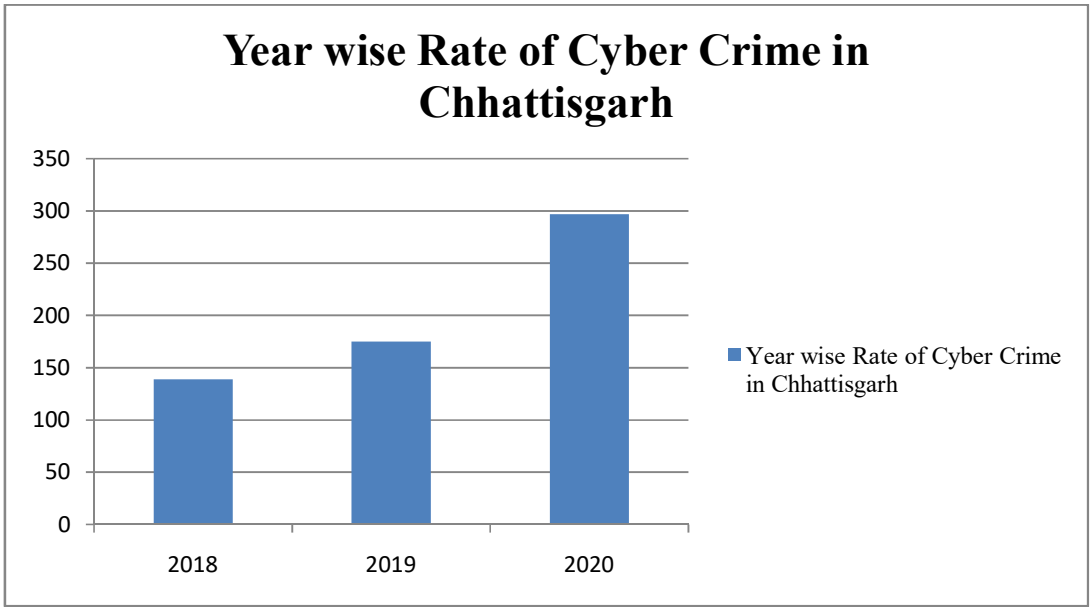
- Cyber crime rate are increasing in Chhattisgarh's society.
- Impact of cyber crimes in Chhattisgarh is harmful for social harmony.

5. METHEDOLOGY

Analytical research method has been adopted to study the cyber crime rate in Chhattisgarh.
This research work is based on secondary data. Descriptive approach is also used to explain the facts related to cyber crime and social harmony.

5. RATE OF CYBER CRIME IN CHHATTISGARH

SN.	YEAR	CASES OF CYBER CRIME
1.	2018	139
2.	2019	175
3.	2020	297



*Table& Chart's data is from official website of CG Police

In above mentioned table we can easily observe that rate of cyber crimes are increasing rapidly year by year, CG Polices study also say that it is effecting badly the Social Harmony in Chhattisgarh's society.According to the conventional view, social harmony entails the absence of conflict and mutual cooperation among all members of society. The "democracy and run of the law" and "fairness and justice" are two components of social amicability. It reflects a fundamental concern shared by the broader populace.

In the contemporary situation, where the state is primarily responsible for ensuring the welfare of its inhabitants, social harmony is fundamentally a social idea, embedded in social relationships, and it may support a more adjusted theory and routine with regard to capable citizenship.

Additionally, there is a natural way to measure the idea of societal harmony. It offers more significant potential for addressing the unquestionably important issue of peaceful coexistence between man and nature.

Social harmony has roots in ancient China, at the reign of Confucius.

As a result, the ideology has also been described as a form of New Confucianism (Guo and Guo, 15 August 2008). The Scientific Development Concept, which General Secretary Hu Jinato devised in the middle of the 2000s, is now re-presented by the HuWen Administration during the 2005 National People's Congress, and it has developed into a significant component of that philosophy. (Ruiping Fan, March 11, 2010)

The ideology is seen as a response to the growing social unrest and imbalance that are emerging in Chinese society as a result of unfettered economic growth, which has led to social conflict. Accordingly, the underlying philosophy shifted from monetary growth to overall society harmony and balance (The Washington Post, October 12, 2006). The decision vanguard Communist party set it as one of the national goals, along with a moderately prosperous society.

Hu Jintao's political worldview differed from that of his forebears, as seen by the promotion of the "Harmonious Society" (Zhong, Wu, October 11, 2006). The administration of Hu's successor, Xi Jinping, has used the philosophy less frequently, probably to emphasise his vision of the Chinese Dream, whereas near the end of his tenure in 2011, Hu appeared to extend the ideology to an international dimension, with an emphasis on the worldwide peace and cooperation, which is said to lead to a "harmonious world".

'Social harmony' refers to the emergence of a peaceful society within the confines of a federal or communist republic. Social Harmony is characterized as a procedure of esteeming, communicating, and advancing affection, trust, adoration, peace, congruity, regard, liberality and value upon other individuals in a specific culture paying little heed to their national origin, weight, conjugal status, ethnicity, colour, gender, race, age and occupation and so on among different angles. Hence Social harmony is highly vital for really being social as being social furthermore involves living harmoniously with each other. For this reason, it is important for us to understand the many public institutions and the social ties that connect them.

The fundamental value and the most desired value in any civilization is social peace. In a global, information society where children are prioritised, social congruity is an integrative motivation that unites in itself love, peace, justice, freedom, equality, brotherhood, collaboration, nonviolence, tolerance, and other universal ideals. Therefore, harmony can prevent the collision of civilizations and is a virtue shared by both western and eastern cultures. Beyond wars, terrorism, and poverty, social harmony brings forth a peaceful, lasting solution to conflict.

Therefore, it suggests that people in general who live nearby and in close proximity work together to make things better for everyone. Unfortunately, since people are better at causing conflict than fostering goodwill, this idea is still just that—a concept. In order for this to occur, most pointless disputes and trivial issues would have to end, and people would have to consider everyone else's happiness and peace as if it were their own. However, it doesn't look that this will happen anytime soon.

6.CONCLUSION

- The rate of cybercrime is rising in Chhattisgarh.
- Cybercrime has a negative impact on social cohesion in Chhattisgarh.

Generally speaking, social harmony refers to a flourishing, balanced, congruent, and supportive society. It is a state free from disputes, tensions, and unrest. Social harmony allows for variances in degrees rather than being an all or nothing situation. The amount of harmony attributes present in a society's major dimensions determines its level of harmony.

Depending on the relative frequency of its harmony components at various points in time, a civilization might display varying levels of harmony over time. A community may therefore be extremely harmonic at time A while becoming less harmonious at time B. Furthermore, one aspect of a community may be in perfect harmony at any particular time, while another may be experiencing discord. A society is in the best possible harmony when its key components are in line with social harmony. A society is disharmonious when its key elements are out of harmony. Societies differ from one another in their levels of harmony. Because they contain more harmonious components than others, certain cultures are more harmonious than others.

Despite the fact that there is no such thing as a crime-free society and that crime is an omnipresent phenomena that cannot be separated from social existence, the question "Why is there so much fuss about crime?" can irritate certain people.Nobody can deny that crime is a social phenomena; it is pervasive, and there is nothing new about crime as it is one of the defining characteristics of all civilizations that have ever been, whether they were civilised or not, and it is one of the fundamental drives behind all human behaviour. However, it should be remembered that the reason for society's concern over a high crime rate isn't the crime itself, but rather the potential disruption it could produce. Additionally, some people become victims of crime in a more extreme way.

7. REFERNECE

- Bhave, Shobha (2022): Cyber Crime in Banking Sector the Study of Customers perception and Responses, pp.110-139
- Keswani , Durgesh (2021): A Critical Study of Cyber Crimes with Special Reference to Social Media in Central India, pp.14-79
- Thakkar, Akash (2021): New approach for post exploitation analysis of cyber crime, pp.47-86
- Singh,Indrajeet (2020):A Critical Study of Cyber Crimes in India with Special Reference to Offence Against Women, pp.88-124
- Singh,Narinder (2020):Cyber crime a study of Chandigarh, pp.60-94
- Raman,Shiv (2019):Cyber crimes in India issues challenges and strategies, pp.114-178
- Chowbe, V.S., 2014Legal Control of Cyber Crime in India, pp.110-139
- Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.
- Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.
- CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117. html, Visited: 28/01/2012.
- Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.
- Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.
- DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r261824 68-NetworkSabotage-or-incompetentmanagers-trying-to-, Visited: 28/01/2012

ISSN: 2278-4632
Vol-13, Issue-05, No.02,May : 2023

- IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012
- Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/htm l/cyber_crime_glossary.shtml, Visited: 28/01/2012
- Leagal Info (2009), Crime Overview aiding and Abetting or Accessory, Available at: http://www.legalinfo.com/content/criminallaw/crime-overview-aiding-and-abetting-oraccessory. html, Visited: 28/01/2012
- Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/ forensic/ cybercrime.htm, Visited: 28/01/2012
- By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/arti cles-news/one-infive-victims-ofcybercrime3907.html, Visited: 28/01/2012.
- Prasun Sonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/I ndia-emerging-as-centre-for-c.html, Visited: 10/31/09
- India emerging as major cyber-crime centre (2009), Available at: http://wegathernews.com/ 203/indiaemerging-as-major-cyber-crimecentre/, Visited: 10/31/09
- PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/ slideshow/2009/aug/20/slide-show-1-indiamajor-hub-for-cybercrime.htm, Visited: 28/01/2012.
- Crime Desk (2009), Million Online Crimes in the Year: Cyber Crime Squad Established, Available at:http://www.thelondondailynews.com/millio n-online-crimes-year-cyber-crime-squadestablished-p-3117.html, Visited: 28/01/2012.
- Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/5536 55/, Visited: 28/01/2012.
- Cyber law times (2009), Available at: http://www.cyberlawtimes.com/forums/index. php?board =52.0, Visited: 10/31/09
- Kevin G. Coleman (2011), Cyber Intelligence: The Huge Economic Impact of Cyber Crime, Available at: http://gov.aol.com/2011/09/19/cyberintelligence-the-huge-economic-impact-ofcyber-crime/, Visited: 28/01/2012
- Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
- D. Ariz. (April 19, 2000), American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99- 185 TUC ACM, 2000 U.S. Dist. Lexis 7299.
- Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.
- Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502 _enron.html, Visited: 28/01/2012
- Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.
- Hoffer, J. A., and D. W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43
- Sprecher, R., and M. Pertl, 1988, IntraIndustry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.
- Baskerville, R., 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121- 130.
- Lyman, J., 2002, In Search of the World_s Costliest Computer Virus, http://www. newsfactor.com/perl/story/16407.html. 2002.
- D_Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute

ISSN: 2278-4632
Vol-13, Issue-05, No.02,May : 2023

- Hancock, B., 2002, Security Crisis Management—The Basics, Computers & Security, 21(5): 397-401
- Cyber Trust and Crime Prevention, MidTerm Review, November 2005 – January 2009, Available at: http://www.bis.gov.uk/assets/bispartners/fore sight/docs/cyber/ctcp_midterm_ review.pdf, Visited: 28/01/2012
- Nigel Jones, Director or the Cyber Security Knowledge Transfer Network, was featured in the daily telegraph (May 6, 2008), Cyber Security KTN,
- NilkundAseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), CyberCriminal Activity and Analysis, White Paper, Group 2.
- Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at: http://www.sans.edu/research/securitylaboratory/article/security-predict2011