RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Curve Fitting Model Analysis of Cyber Crimes, Cyber Bullying and Online Sexual Exploitation in India

By

Dr.TRR.Gopalakrishnan
Associate Professor, Department of Journalism and Communication University of Madras, Chennai
Email: trggopi@unom.co.in

Dr.K.Ravichandran
Associate Professor, Department of Visual Communication and Animation DR M G R Educational and Research Institute, Chennai
Email: ravi.news10@yahoo.com

SenthilKumar Ilango
Principal Software Engineer/Computer Science Graduate, Florida Institute of Technology, Melbourne, FL, USA
Email: silango2009@my.fit.edu

Abstract

Mobile phones and the Internet are not only powerful tools but they can also become great weapons and have the same impact as physical abuse on the Internet against women. In this era, when technology is entering all the cornerstones of the world, the repercussions of which are much greater. Devices that are connected to the internet have become an in-evitable tool for all sections of the society including women and young girls. Thus, there are already millions of women around the world who are being targeted for sexual violence while online. With the development of internet technologies, and the advent of social media, there have been new ways of predating victims. Over, 95 percent of the abusive behaviors online are directed at women. The Internet has been subverted by all the positive promises it has made for promoting the freedom of women's thoughts. In many cases, it promotes anonymous cruelty and aggressive behavior towards women and girls. Cyber bullying is a global menace, and coping with it is not very easy. In this research, we use a curve fitting model to analyze the data from the National Crime Archives on cyber fraud, cyber bullying and online sexual exploitation in India.

Key words: Cybersecurity, Cyber Forensics, Data Security, Cyber Attacks, Cyber Bullying, Online Sexual violence, Cyber Fraud, Curve Fitting Model, Piracy

Introduction

A recent survey by the Indian Internet and Mobile Association (IAMAI) shows that India has 451 million monthly active Internet users next to China. The report titled Indian Internet 2109, reports that 72 percent (139 million) of urban users, and 57 percent of rural users (109 million) use the Internet daily[1-2]. Majority of these internet users are in the ages between 16 and 29. The internet has been growing exponentially with new devices being connected every single day. In all inventions, good and evil are blended; wherein the Internet is no expectation, the evil reaches everyone very quickly[3-4]. One of the popular scams online wherein the victim is sexually intimidated is known as Sextortion. Generally, females are more targeted for cybercrimes. But, in the case of Sextortion, the victims are males[5]. There are

thousands of men who fall prey to these scams daily. In a majority of these cases, the victims are lured into these scams via the social media and other online platforms and are sexually intimated. Internet scams like these are spreading in the Philippines and have grown into a major business in the recent past[6-7].

According to a leading official of the Philippine Police, "These fraudsters are making hundreds of US dollars a day from victims. We have recently discovered a section of fraudulent gangs that act like this. They hire many young workers, make random fake calls pretending to be a beautiful woman on the other end, and then target innocent men [8-9]. They then record private video conversations with them and often have video clips saved on their computer[10].

The National Security Council Secretariat has requested comments on the creation of the National Cyber Security Strategy 2020 (NCSS 2020), which was published in the first quarter of 2020 [11]. Table:1 and Figure:1 shows the different kinds of cyber crimes and their motives that were registered between 2016 and 2018, that totalled 61316 [12]. There were 12,317 cybercrimes reported in 2016, up from 21,796 in 2017 - an increase of 77% year over year [13]. In 2018, the number of such incidents increased to 27,248 - meaning that the number of cybercrimes reported in 2018 was 121% higher than in 2016 [14].

Table:1 *Total All India Cyber Crime Motives During 2016 to 2018*

	Year		
	2016	**2017**	**2018**
Personal Revenge	5987	628	794
Anger	1056	714	461
Fraud	686	12213	15051
Extortion	571	906	1050
Causing Disrepute	569	1002	1212
Prank	448	321	296
Sexual Exploitation	149	1460	2030
Political Motives	141	139	218
Terrorist Activities (Total)	121	110	44
Terrorist Activities - Terrorist Recruitment	40	1	2
Terrorist Activities - Terrorist Funding	33	0	0
Terrorist Activities - Others	23	109	42
Inciting Hate against Country	18	206	218
Disrupt Public Service	14	55	21
Sale purchase Illegal drugs	9	8	6
Developing own business	3	156	198
Spreading Piracy	2449	90	671
Psycho or Pervert	5987	17	4
Steal Information	1056	10	16
Abetment to Suicide	686	5	2
Others	571	3756	4956

a. Limited to the first 100 cases.

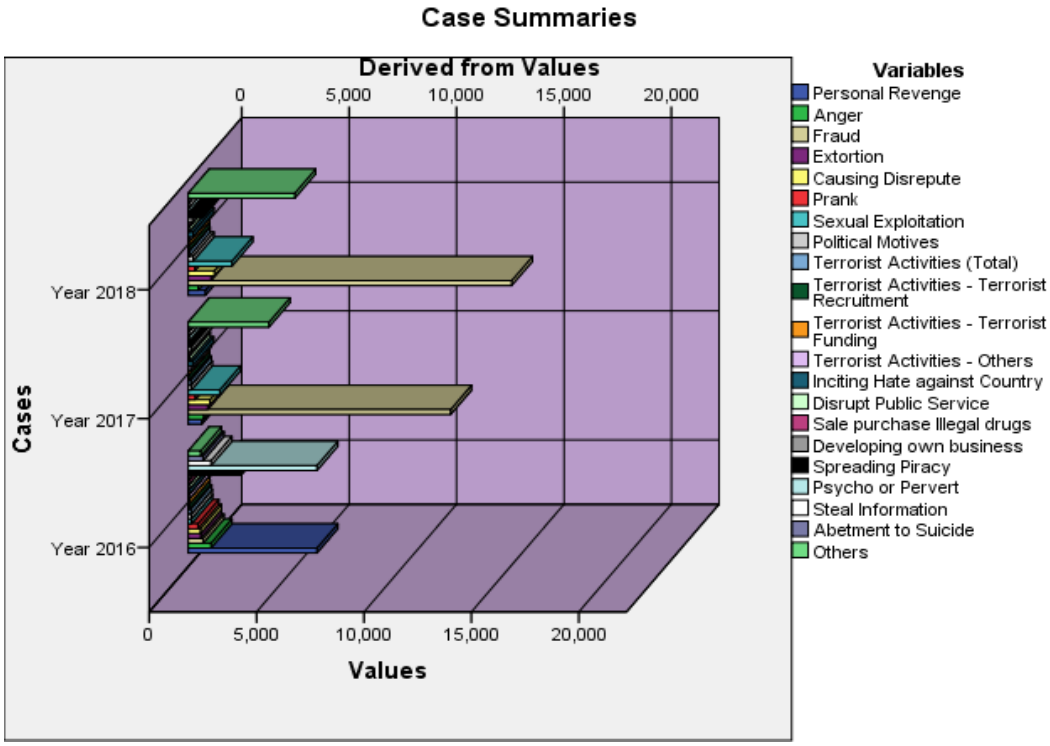

Figure:1 *Total All India Cyber Crime Motives During 2016 to 2018*

Cybersecurity threats such as software vulnerabilities, malicious software, viruses, trojan horses, spyware, ransomware, phishing attacks etc originate in the web and are multiplied by technological advancements like 5G, artificial intelligence, augmented reality, robotics, quantum computing, and the Internet of Things[15]. Unethical hackers can steal bank or credit card account details, login details and passwords, threaten internet users, stalk them online, and fund terrorist activities or promote child pornography. Ransomware and other cyber attacks threaten operations of critical infrastructures, such as Power Grid or Ports, and the load on the grids can substantially increase through the spread of fake news[16-17]. During the Covid pandemic, more than 4,000 fraudulent websites were exposed, and on a given typical day in April 2020, Google blocked more than 240 million spam messages and 18 million phishing scams. There were many similarly sounding fake UPI's (Unified Payments Interface) that emerged soon after Prime Minister PM CARES fund was announced to raise funds and combat the Covid-19 pandemic[18].

"As awareness and reporting of cybercrimes improve, so does the increase in the number of cybercrimes". In addition, the federal government has announced that states and union territories are primarily responsible for preventing, detecting, investigating, and prosecuting crimes by their law enforcement agencies to check cyber crimes in the country. The Ministry of Home Affairs is developing "state-of-the-art initiatives to provide alerts/advice through various consultations and programs, build the capacity of law enforcement personnel, and improve cyber forensic facilities[19-20]."

The Government of India launched a National Cyber Crime Reporting Portal to report civilian cybercrime incidents. Furthermore, there have been reports that at least 3,000 e-mail IDs from government agencies such as the Indian Space Research Organization (ISRO) and the Bhabha Atomic Research Center (BARC) were exposed in a cyber attack. The Ministry of Corporate Affairs, Ministry of External Affairs, the Nuclear Regulatory Board, and the Indian

Securities and Exchange Board (SEBI) systems have been compromised, and some of the user(s) passwords that were available in plain text in various databases were leaked in the dark web. This comes just months after Nuclear Power Corporation of India Limited (NPCIL) confirmed that the internet-connected computer at Kudankulam Nuclear Power Plant was infected[21].

Research Problem

With the advent and popularity of social media, there have been various cyber crimes and cyber attacks against users and systems connected to the internet, and they pose a very big problem.

Objectives and Approach

The objective of this study is to analyze the nature of cyber crimes in India and statistically study its effects.

Methodology

In this study, a total Number of 27248 cyber crime cases were registered in India in the year of 2018, was obtained as secondary data from The National Crime Records Bureau (NCRB).

Result and Discussion:

Table:2 *Descriptive Statistics-Total All India Cyber Crime Motives During 2018*

	Sum	Mean	Std. Deviation
Personal Revenge	794	22.06	44.941
Anger	461	12.81	25.485
Fraud	15051	418.08	1007.892
Extortion	1050	29.17	54.345
Causing Disrepute	1212	33.67	72.200
Prank	296	8.22	31.826
Sexual Exploitation	2030	56.39	129.881
Political Motives	218	6.06	12.095
Terrorist Activities (Total)	44	1.22	3.330
Terrorist Activities - Terrorist Recruitment	2	0.06	.232
Terrorist Activities - Terrorist Funding	0	0.00	.000
Terrorist Activities - Others	42	1.17	3.317
Inciting Hate against Country	218	6.06	13.260
Disrupt Public Service	21	0.58	1.645
Sale purchase Illegal drugs	6	0.17	.561
Developing own business	198	5.50	14.484
Spreading Piracy	671	18.64	102.147
Psycho or Pervert	4.00	0.1111	.39841
Steal Information	16.00	0.4444	1.22927
Abetment to Suicide	2.00	0.0556	.23231
Others	4956.00	137.6667	349.02345

The curve estimation process generates curve estimation regression statistics and related plots for 11 different curve estimation regression models. It is made as a separate model for each dependent variable. It can also save predicted values, residues and prediction intervals as new variables. For each model, the regression coefficients are multiple R, R2, adjusted R2, standard error of estimation, analysis-variance table, and predicted values, residuals and prediction intervals. Specifically, models are linear, logarithmic, inverse, quadratic, cube, power, compound, S-curve, logistic, growth and exponential.

Table:3 *Model Summary and Parameter Estimates*

Dependent Variable: Sexual Exploitation								
Equation	Model Summary					Parameter Estimates		
	R Square	F	df1	df2	Sig.	Constant	b1	b2
Linear	.219	9.552	1	34	.004	31.158	.060	
Quadratic	.641	29.458	2	33	.000	-8.791	.296	-5.040

The independent variable is Fraud

The linear model shows that the expected number of online sexual exploitations as 31.158+ 0.060*. A P1 value greater than 1 suggests that a cyber attacker makes as much money on fraud as he/she does in repeated online sexual exploitation. In practice, this does not mean much as a person's lust has an enrichment point. Expected Sexual Exploitation is -8.791+ 0.296*, Online Fraud is -5.040* via Quadratic model which equals squared fraud. The model suggests that if the negative value for P2 exceeds a certain point, the increased fraud will actually reduce sexual exploitation. More precisely, fraud decreases past 0.296 / (2 * -5.040) = -0.0293 expected sexual exploitation.

F, TF1, TF2, and sig. columns summarize the results of the F test of the model fit. The significance value of the F statistic is less than 0.05 for both models, meaning that the variance explained by each model is not due to chance. The R Square statistic is the best measure of the strength of the relationship.

The R squared statistic is a measure of the strength of the correlation between the observed and model-predicted values of the dependent variable. Large R square values indicate a strong correlation for both models. The R square for the quadratic model is large, although it is not clear whether this is due to the quadratic model with the possibility of an additional parameter.

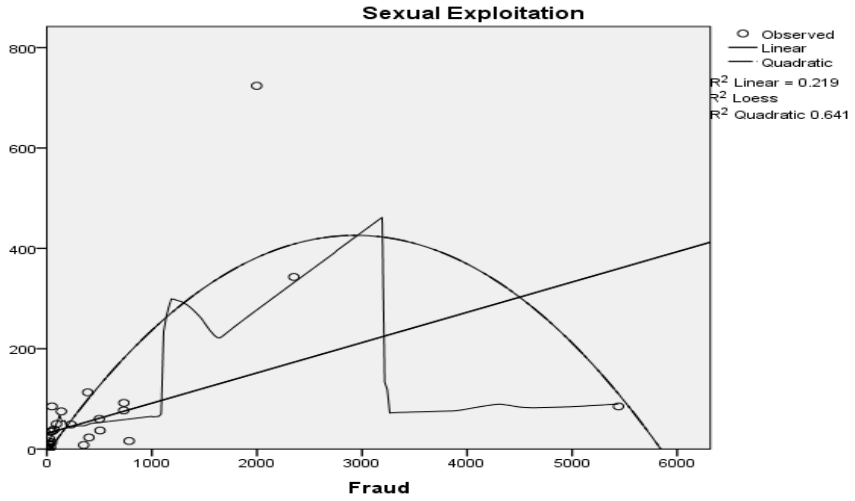

Figure:2 *sexual exploitation Fraud*

The curve fit chart gives us a fast visual assessment of the fit of every model to the observed values. From Figure:2, in this plot it appears that the Quadratic model better follows the form of the information. Especially, the linear model seems to overestimate sexual exploitation for cases with small or large values of Fraud and underestimate Personal Revenge for cases with medium values of Fraud. As an extra visual check, it should check out plots of the residuals versus predicted values for every model.

Table:4 Model Summary and Parameter Estimates

Dependent Variable: Spreading Piracy								
Equation	Model Summary					Parameter Estimates		
	R Square	F	df1	df2	Sig.	Constant	b1	b2
Linear	.114	4.389	1	34	.044	4.312	.034	
Quadratic	.350	8.875	2	33	.001	-19.164	.173	-2.962

The independent variable is Fraud.

In Table:4 from the Linear model, it is seen that the expected spreading piracy is equal to 4.312+0.034 * fraud spending. The b1 value greater than 1 suggests that a fraudster spends as much on fraud as he/she can because they will make that investment back and more in spreading piracy. Practically, this doesn't make much sense because the market has a saturation point for fraud.

The Quadratic model states that the expected spreading piracy is equal to -19.164+0.173*fraud spending -2.962*squared fraud spending. The negative value for b2 means that this model suggests that past a certain point, increased fraud would actually decrease spreading piracy. More exactly, increased fraud past 0.173/(2 * -2.962) = -0.0292 will decrease expected spreading piracy.

The F, df1, df2, and Sig. columns summarize the results of the F test of model fit. The significance value of the F statistic is less than 0.05 for both models, which means that the variation explained by each model is not due to chance. The R Square statistic is a better measure of the strength of the relationship.

The R Squared statistic is a measure of the strength of association between the observed and model-predicted values of the dependent variable. The large R Square values indicate strong relationships for both models. The R Square for the Quadratic model is larger, though it is not clear whether this is due to the Quadratic model capitalizing on a chance with an extra parameter.

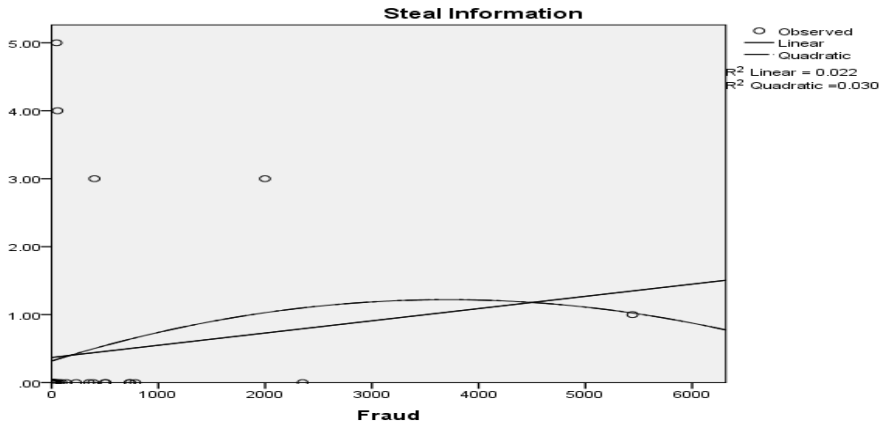

Figure:3 *Curve fit chart of steal Information for cases with small or large values of Fraud*

The curve fit chart gives us a fast visual assessment of the fit of every model to the observed values. In Figure:3, from this plot, it appears that the Quadratic model better follows the form of the information. The linear model seems to overestimate stealing information for cases with small or large values of fraud and underestimate personal revenge for cases with medium values of fraud. As an extra visual check, it should check out plots of the residuals versus predicted values for every model.

Table:5 *Model Summary and Parameter Estimates*

Dependent Variable: Causing Disrepute								
Equation	Model Summary					Parameter Estimates		
	R Square	F	df1	df2	Sig.	Constant	b1	b2
Linear	.135	5.289	1	34	.028	22.678	.026	
Quadratic	.376	9.950	2	33	.000	5.870	.125	-2.121
The independent variable is Fraud.								

In Table:5, from the Linear model, the expected causing disrepute is equal to 22.678+0.026*fraud spending. The b1 value greater than 1 suggests that a cyber attacker would spend as much on fraud as he/she can because that person will make that investment back and more in causing disrepute.

From the Quadratic model it is seen that the expected causing disrepute is equal to 5.870+0.125*fraud spending -2.121*squared fraud spending. The negative value for b2 means that this model suggests that past a certain point, increased fraud would actually decrease causing disrepute. More exactly, increased fraud past 0.125/(2 * -2.121) = -0.0294 will decrease expected causing disrepute.

The F, df1, df2, and Sig. columns summarize the results of the F test of model fit. The significance value of the F statistic is less than 0.05 for both models, which means that the variation explained by each model is not due to chance. The R Square statistic is a better measure of the strength of the relationship.

The R Squared statistic is a measure of the strength of association between the observed and model-predicted values of the dependent variable. The large R Square values indicate strong relationships for both models. The R Square for the Quadratic model is larger, though it is not clear whether this is due to the Quadratic model capitalizing on the chance with an extra parameter.

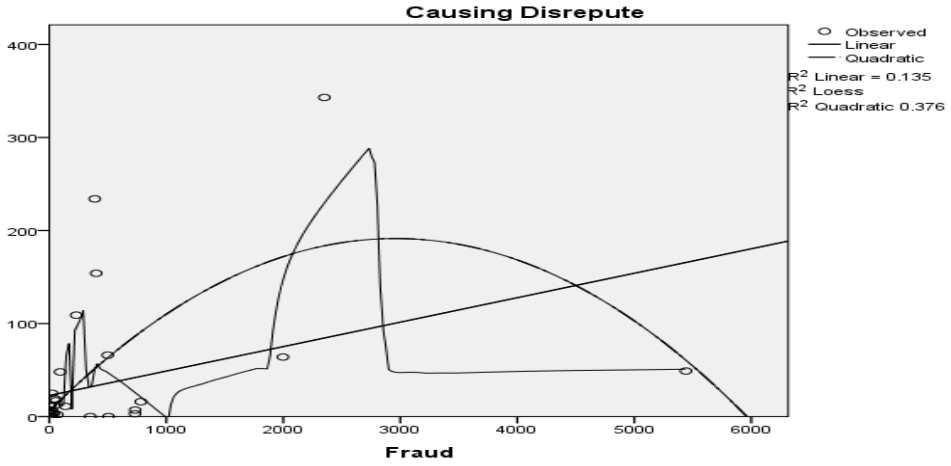

Figure:4 *Curve fit chart of Causing Disrepute for cases with small or large values of Fraud*

In Figure:4, from this plot, it appears that the Quadratic model better follows the form of the information. The linear model seems to overestimate causing disrepute for cases with small or large values of fraud and underestimate personal revenge for cases with medium values of fraud. As an extra visual check, it should check out plots of the residuals versus predicted values for every model.

Table:6 *Model Summary and Parameter Estimates*

Dependent Variable: Political Motives								
Equation	Model Summary					Parameter Estimates		
	R Square	F	df1	df2	Sig.	Constant	b1	b2
Linear	.230	10.132	1	34	.003	3.652	.006	
Quadratic	.320	7.747	2	33	.002	1.934	.016	-2.168

The independent variable is Fraud.

In Table:6, the Linear model states that the expected Political Motives is equal to 3.652+0.006*fraud spending. The b1 value greater than 1 suggests that an attacker spends as much on fraud as he/she can because they will make that investment back and more in Spreading Piracy.

From the Quadratic model it is seen that the expected political motives is equal to 1.934+0.016*fraud spending - -2.168*squared fraud spending. The negative value for b2 means that this model suggests that past a certain point, increased fraud would actually decrease political motives. More exactly, increased fraud past 0.016/(2 * -2.168) = -0.0036 will decrease expected political motives.

The F, df1, df2, and Sig. columns summarize the results of the F test of model fit. The significance value of the F statistic is less than 0.05 for both models, which means that the variation explained by each model is not due to chance. The R Square statistic is a better measure of the strength of the relationship.

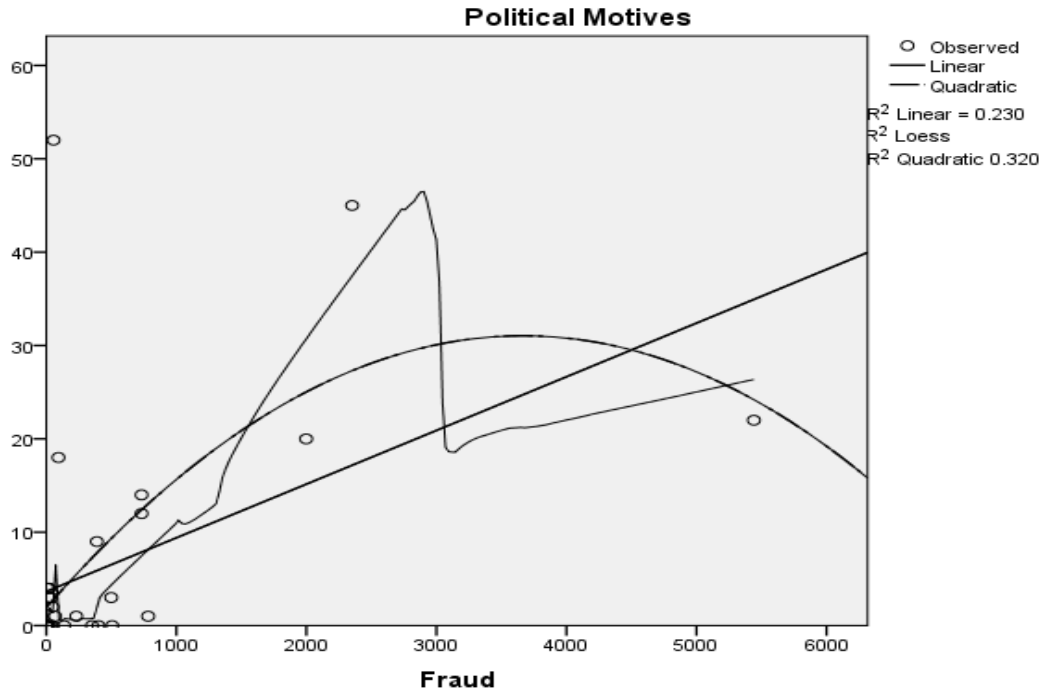

Figure:5 *Curve fit chart of Political Motives for cases with small or large values of Fraud*

In Figure:5, the Quadratic model better follows the form of the information. The linear model seems to overestimate political motives for cases with small or large values of fraud and underestimate personal revenge for cases with medium values of fraud.

Discussion

From Table:1, Personal Revenge had a sum value of 794 with a mean of 22.06, Anger had a sum value of 461 with a mean of 12.81, Fraud had a sum value of 15051 with a mean of 418.08, Extortion had a sum value of 1050 with a mean of 29.17, Causing Disrepute had a sum value of 1212 with a mean of 33.67, Prank had a sum value of 296 with a mean of 8.22, Sexual Exploitation had a sum value of 2030 with a mean of 56.39, Political Motives had a sum value of 218 with a mean of 6.06. India is ranked 3rd for malicious activities and cyber crimes in the world. This has a severe impact on the expansion of the economy and adds more costs to it. With the increase in cyber crimes, there is a direct and significant impact on jobs, innovation, economic progress, and investments. Additionally, IP theft makes up a minimum of 25% of cyber crimes and is a much bigger threat to military technologies and in turn the sovereignty of the country.

In general, cyber crimes promote all sorts of online violence to harass the victim with scandalous messages, cheating, extortion, slander and revenge pornography. Cyber crimes like online fraud, financial fraud, stalking, bullying, hacking, email spoofing, information piracy and forgery and property crime can wreak havoc in victims' lives. At worst, cybercrime can cause bankruptcy and potentially threaten a victim's reputation and privacy. During cyber extortion, hackers hold the victim's data, website, computer systems, or other sensitive information hostage until their demands for payment are met. Any organization that does business online should protect their systems against cyber attacks.

In general, there have been over two thousand cases of cyber crimes that have led to harassment or exploitation across India in 2018. This was a stark jump within the number of such cyber crimes within the country compared to the previous two years. Although the rate had indeed gone up within the country in 2018, the Indian government's efforts to determine new mechanisms to tackle cyber crimes, alongside more awareness among people were a number of the factors causing such an enormous spike in reported cases of cyber crimes. Hackers on other hand use the knowledge to cause disruption to the network for private and political motives. Section 66 (b) of the Information Technology Act of 2000, punishes the cyber attacker with an imprisonment for a term of three years and a fine of up to two lakhs rupees, or both. There should be a transparent understanding of what cybercrimes are and how they need to be reported.

Conclusion

Case studies analyzed previously have concluded that the use of online technologies affects communities, especially through the emergence of pseudonymous cyber crimes that have a negative impact on the population. Cyber crimes that have occurred in India include online bank fraud, cyber bullying, online sexual abuse, hacking, and many other scams such as online credit and debit card frauds. Cyber crimes on the Internet have become a social problem and there have been many such instances in the endless Internet community. The curve fit model summarizes the parameters and dependent variables such as sexual exploitation, piracy, causality and political motivation, etc on which cyber crimes are evaluated. Each column summarizes the results of the F-model fit test. The F value of both models is less than 0.05,

indicating that the variation attributed to each model is not random. The R-square statistic can measure the strength of the relationship between the observed and predicted values of model variables. The significant squared R value indicates a strong relationship between the two models. The square model is larger; although it is not clear whether this is due to the additional parameter capabilities of the quadratic model. Therefore, advanced telematics technologies are used to spread such crimes. Because it is often difficult to define and can originate anywhere, it is difficult to avoid the forces that drive social issues. Every participant in social life must abide by the social discipline system called society. But failure to comply with this rule will only cause social problems. The main social problems in India are classified as violations of any of the values and rules, cyber crime cases, or cyberspace crimes that plague society. Changes are unlikely to attract other important things, such as communications and data development. All elements of politics, society, and economy will adapt to the communications revolution, but if we are a community and deal with it wisely, then there is no danger for comparison.

References

Smith, M. D., &Krannich, R. S. (2000). "Culture Clash"Revisited: Newcomer and Longer-Term Residents' Attitudes toward Land Use, Development, and Environmental Issues in Rural Communities in the Rocky Mountain West. Rural sociology, 65(3), 396-421.

McFarland, J., Hussar, B., Wang, X., Zhang, J., Wang, K., Rathbun, A.,.& Mann, F. B. (2018). The Condition of Education 2018. NCES 2018-144. National Center for Education Statistics.

Tadeusiewicz, R. (2008). Selected problems resulting from the use of the internet for teaching purposes. Bulletin of the Polish Academy of Sciences: Technical Sciences, 403-409.

Funk, T. (2011). Social Media Playbook for Business: Reaching Your Online Community with Twitter, Facebook, LinkedIn, and More: Reaching Your Online Community with Twitter, Facebook, LinkedIn, and More. ABC-CLIO.

Powell, A., & Henry, N. (2017). Sexual violence and harassment in the digital era. In The Palgrave handbook of Australian and New Zealand criminology, crime and justice (pp. 205-220). Palgrave Macmillan, Cham.

Kumar, H. (2015). Mass Marketing Frauds in the garb of Mobile Towers in India: Evolving a Framework to handle it. Post-Graduate Programme in Public Policy Management. Gurgaon: Management Development Institute Gurgaon.

Wittes, B., Poplin, C., Jurecic, Q., &Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. Center for Technology at Brookings.

Barendregt, B., & Van Zanten, W. (2002). Popular music in Indonesia since 1998, in particular fusion, Indie and Islamic music on video compact discs and the internet. Yearbook for traditional music, 34, 67-114.

Guzik, K., Sesay, A., Oh, O., Ramirez, R., & Tong, T. (2021). Making the material routine: a sociomaterial study of the relationship between police body worn cameras (BWCs) and organizational routines. Policing and society, 31(1), 100-115.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact on secondary school pupils. Journal of child psychology and psychiatry, 49(4), 376-385.

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

SoumyarendraBarik(2020), More Than 60,000 Cyber Crime Cases Registered Between 2016-18: Home Ministry, https://www.medianama.com/2020/02/223-cyber-crimes-india-2016-2018/

Panwar, K., Sihag, V. K. (2020). Changing forms of Cyber Violence against Women and Girls. The Indian Police Journal, 111.

Vijaita Singh(2020) Crime against Scheduled Castes, Scheduled Tribes saw a rise of 7% and 26% in 2019: NCRB, NewDelhi, September 30, 2020 15:43 Ist.

Bidgoli, H. (2006). Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management (Vol. 3). John Wiley & Sons.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55.

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.

https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

Chatterjee, S., Kar, A. K., Dwivedi, Y. K., &Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People.

Press Information Bureau (2019), Government of India Ministry of Corporate Affairs 07 JUN 2019 6:00 PM by PIB Delhi Ministry of Corporate Affairs & SEBI.

AditiAgrawal(2019),https://www.medianama.com/2019/12/223-national-cyber-security-strategy-comments-invite/

Mohammad Anisur Rahaman, Cyber crime affects society in different ways, July 04, 2016, https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways