VOL.6 ISSUE 4
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

INCHOATE CYBER-CRIMES AND SUBJECTIVE FEELINGS OF SAFETY IN THE CYBERSPACE: A PILOT STUDY ON INDIAN NETIZENS

KIRTI MINHAS[1]

ABSTRACT

The anonymity assured by the cyberspace greatly influences criminal tendencies and fear of victimization online. The term "inchoate crimes" refers to a group of offences that do not require the completion of the intended criminal act for the target person to feel victimized. A criminological understanding of cyber-crimes, other than financial crimes in cyberspace, strongly indicates this incomplete nature of online victimization as well, especially in cases of cyber-stalking, cyber-bullying, and the likes. This nature of the outlawed behaviour poses a challenge for the concerned authorities to provide appropriate and timely assistance to victims of such cyber-harassment, let alone bring the perpetrators to justice.

The researchers have designed an online survey to evaluate the awareness of what constitutes such cyber offences, and the fear of these inchoate cyber-crimes amongst the Indian population. Based on an analysis of the data collected, the researchers have suggested prospective victim assistance mechanisms by law enforcement officials for victims of inchoate cyber-crimes. In conclusion, the paper suggests legislative changes required in the existing cyber laws in India, wherein the dearth of a comprehensive definition of cyber-crimes even in the Information Technology Act, of 2000 despite an amendment being made in the rules of the IT Act, in 2021, is a primary challenge.

[1] *Assistant Professor (Law), Rashtriya Raksha University ,Ph.D (MNLU, Mumbai) (Pursuing) LL.M (RGSOIPL, IIT Kharagpur), B.A LL.B (Hons) (ILNU, Nirma University)*

Keywords: *inchoate crimes, cyber-crimes, law enforcement, victim assistance*

INTRODUCTION

A. Cyber-crimes vis-à-vis Inchoate Cyber-crimes:

Sussman and Heuston previously proposed the expression "cyber-crime" in the year 1995.[2] Cyber-crime can't be presented as a stand-alone definition; it is best thought to be an variety of acts or leads. Cyber-crime is otherwise called electronic violations, computer-related wrong doings, e-wrong doing, high-innovation wrongdoing, data age wrongdoing and so forth. *In basic terms, we can portray "Cyber-crimes" as the offenses or violations that happens over electronic correspondences or data frameworks*[3]. These sorts of violations are essentially the criminal operations in which a PC and an organization are involved. Due of the improvement of the web, the volumes of the cyber-crime exercises are likewise expanding on the grounds that while perpetrating a wrong there could be as of now not a requirement for the actual presence of the crook.

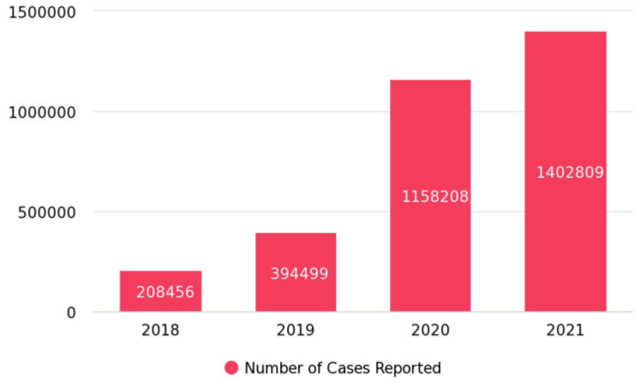


Figure 2: Reported Cyber Crimes in India (2018-2021)
Source: Indian Computer Emergency Response Team (CERT-In)

The surprising attribute of cyber-crime is that the person in question and the wrongdoer might in all likelihood never come into direct contact. *Cyber-criminals frequently select to work from*

[2] George Tsakalidis and Kostas Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents," 49 *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 710–29 (2019).
[3] *Ibid.*

nations with non-existent or feeble cyber-crime regulations to lessen the possibilities of recognition and prosecution.[4] And as the victim and perpetrator rarely come in direct contact and many times are anonymous, it is important to question the safety of citizens in cyber spaces. Since, 1995 the evolution of cyber-crime can be seen against individuals, society, or organisations and against property (physical and intellectual). Safety in cyberspace is talked about a lot nowadays. Hence, this paper also evaluates the subjective feelings of safety in cyberspace through a survey. The anonymity assured by cyber-space greatly influences criminal tendencies and fear of victimization online. *The term "inchoate crimes" refers to a group of offences that do not require the completion of the intended criminal act for the target person to feel victimized*[5]. A criminological understanding of cyber-crimes, other than financial crimes in cyber-space, strongly indicates this incomplete nature of online victimization as well, especially in cases of cyber-stalking, cyber-bullying, and the likes. This nature of the outlawed behaviour poses a challenge for the concerned authorities to provide appropriate and timely assistance to victims of such cyber-harassment, let alone bring the perpetrator to justice.

B. Challenges to Investigation and Prosecution of Inchoate Cyber-crimes:

A December 2000 study noted four major disputes in the prosecution and prevention of cyber-crimes as opposed to terrestrial crimes: "(i) they are easier to learn and try out; (ii) they require fewer resources in contrast to the potential damage caused; (iii) they can be committed in a jurisdiction without being physically present in it; (iv) they are often not clearly illegal under the

[4] Rashmi Saroha, "Profiling a Cyber Criminal," 4 *International Journal of Information and Computation Technology* 253–8 (2014).

[5] Jelle Brands and Janne Van Doorn, "The Measurement, Intensity and Determinants of Fear of Cybercrime: A Systematic Review," 127 *Computers in Human Behavior* 747–5632 (2022).

laws of either the jurisdiction in which the person is present nor in the physical space in which the offence is detected."[6]

Several INTERPOL reports on cyber-crimes have also reiterated that not only does such ambiguity give the police less time to react to any potential criminal threat online that might even transcend to the physical space, but it raises issues of privacy, and anonymity, besides jurisdictional challenges of investigation and prosecution.

The June 10, 2022 episode of The Indian Express Podcast "3 Things", exclusively talks about why cyber criminals thrive in India and one of the important yet oven trivialised reason stated was the challenge of logistic hassles on the part of law enforcement when due to the transcending all state and national borders nature of cyber-crimes, the cost of investigation and prosecution is vastly higher than the cost of the crime committed.

REVIEW OF LITERATURE

1. The paper discussed about the cyber-crime and its categories, professions giving birth to cyber-crimes and its impact on businesses and the preventive measures to be taken to control the cyber-crime.[7]
2. The authors identified and presented the features of cyber-crime incidents, a classification system for related offences and a schema that binds together the various

[6] "Cyber Crime and Punishment" <http://zybook.weebly.com/uploads/2/6/4/6/26468840/mcconnell-cybercrime.pdf> accessed July 1, 2022

[7] K Sambi Reddy, "Cyber Crimes in India and the Mechanism to Prevent them," 3 *International Journal of Innovative Research in Information Security (IJIRIS)* 2014–7 (2016).

elements and examines their interrelations to better suggest corresponding actions, measures and policies.[8]

3. Cyber safety depends on the knowledge of the technology and the care taken while using internet and that of the preventive measures adopted by user and server systems. It is well said that the problems created cannot be solved with the same level of awareness that created them. Hence there is need to enhance awareness about the cyber-crime. The growing danger by cyber-crimes in India needs technological, behavioural and legal awareness; along with proper education and training. This study analyses netizens' awareness of cyberlaws and the role of police.[9]
4. This handbook is intended as a reference work to help individuals quickly realize the current state of the field with respect to technology use and abuse. The book is global in scope, drawing young and established scholars alike to share their knowledge. This work also provides a robust examination of cyber-crime from multiple perspectives, including criminology, sociology, and political science. The legal, theoretical, and policy frameworks that guide researchers and practitioners in the field are also explored in depth.[10]
5. Inchoate crimes extend across the spectrum of conspiracy, incitement, solicitation and attempts. Of all these concepts, the most difficult challenge exists in the cases involving attempts of criminal acts. Occasional suggestions by the Commonwealth courts calling for rectification or legislative intervention to address the complexity and

[8] G. Charles Babu et al., "A systematic approach toward description and classification of cyber crime incidents," 7 *International Journal of Recent Technology and Engineering* 1886–9 (2019).
[9] Saroj Mehta and Vikram Singh, "a Study of Awareness About Cyberlaws in the Indian Society," 4 *International Journal of Computing and Business Research* (2013).
[10] Thomas J Holt and Adam M Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*.

incoherence of the common law provisions governing attempts of criminal acts has so far been acted upon in England and New Zealand in part. *When the Justice System responds appropriately with the attempt of a crime itself, it not only helps minimise criminality in the budding stage itself, but it also assures citizens of a safer society which builds their trust in the national governance.*[11]

6. The importance of having equivalency in international laws since cyber-crimes permeate all national borders. Nations came up with extradition treaties for offenders who commit crime in one country and flee to another but this does not quite work as effectively for cyber-crimes because of legislative challenges. *Thus, the Indian legislation against cyber-crimes needs an upgradation to incorporate such relevant equivalency in terms of cyber-crimes as addressed in legislations of other countries.*[12]
7. This study explains the use of regression and corelation to study crime patterns in offences-prone states based on data retrieved from the National Crime Records Bureau (NCRB) database. *However, it is to be noted that the NCRB reports clearly indicate financial cyber-crimes being recorded more frequently as compared to cyber-crimes against persons and/or inchoate cyber-crimes as discussed in this paper.* [13]
8. Inchoate liability can be observed in international law as well in an incremental and cautious mention in the anti-terrorism treaties of the 1970s to 1990s. And, the UN

[11] Peiris, G. L. (1984). Liability for Inchoate Crime in Commonwealth Law. *Legal Studies, 4*(1), 30-66. DOI:10.1111/j.1748-121X.1984.tb00432.x

[12] Marc D Goodman, Susan W Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, *International Journal of Law and Information Technology*, Volume 10, Issue 2, SUMMER, Pages 139–223, https://doi.org/10.1093/ijlit/10.2.139

[13] P. Kapoor, P. K. Singh and A. K. Cherukuri, "IT Act Crime Pattern Analysis using Regression and Correlation Matrix," *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 1102-1106, DOI: 10.1109/ICRITO48877.2020.9197835.

Security Council's response to the terrorist attacks of 11 September 2001 further extended this scope. In resolution 1373 (2001), the Council required all states to criminalize new pre-inchoate terrorism offences of financing, planning and preparation, and support for terrorism, while resolution 2178 (2014) also required states to criminalize a range of conduct related to travel. *Although this resolution has received criticism for the lack of clarity in the definitions of the inchoate nature of various acts included in its ambit, the idea stands tall that fixing criminal responsibility of inchoate offences is believed to be a crucial step in ensuring justice for crimes of all magnitudes, up to and including terrorism.*[14]

9. This paper substantively explores the hypothesis that the concept of criminal responsibility has shifted over time from a liability fixed in ideas of character to a capacity-based construct. This implies that the criminal responsibility ascertained to inchoate crimes have seen an increase over time, thereby rendering a socio-theoretic framework to the structure and content of criminal justice.[15]

10. Developed from the philosophical analysis of foreseeability of harm, this book is said to provide the fullest account available of the philosophical foundations of the law of causation, clarifying its role in attributing responsibility. It elaborates on the fact that ascribing legal responsibility in criminal justice stems from a thorough

[14] Saul, B. (2022). "Chapter 14: Precursor Crimes of International Terrorism". In *Precursor Crimes of Terrorism*. Cheltenham, UK: Edward Elgar Publishing. Retrieved May 16, 2022, from https://www.elgaronline.com/view/edcoll/9781788976312/97817889763.

[15] Brenner, S. W. (2001). Is There Such a Thing as "Virtual Crime"? *Cal. Crim. Law Rev*, *1*, 11.

understanding of the concept of causation causation in criminal and tort law presupposed by the legal doctrine.[16]

11. This research explores the crucial dispute law enforcement officers and prosecutors often encounter when they implement the existing laws to criminal activities in the cyberspace. Difference in laws across nations and then the consequent problem with extradition of criminals even when they are found guilty, in addition to pertinent questions like, "Do countries need to outlaw offences like cyber stalking if they have already criminalised stalking?" The other consideration here is how one country's cyber-crime laws, or lack of such laws, impact other countries as well.[17]

RESEARCH METHODS

A. Research Objectives:

The overarching research question answered in this study is: *"Based on a criminological understanding of criminal tendencies in the cyber space and subjective feelings of safety among netizens, how can law enforcement provide better assistance to victims of inchoate cyber-crimes, and what legislative changes would better empower law enforcement to achieve this purpose?"*

The research objectives can thus be enumerated as follows:

1. Categorizing the mentioned set of cyber-crimes as inchoate cyber-crimes and including them accordingly in the legislation.

[16] Moore, M. S. (2009). *Causation and Responsibility: An Essay in Law, Morals, and Metaphysics*. United Kingdom: Oxford University Press.

[17] Goodman MD, "The Emerging Consensus on Criminal Conduct in Cyberspace" (2002) 10 International Journal of Law and Information Technology 139

2. Analysing the gap between fear, awareness and reporting of the mentioned inchoate cyber-crimes.
3. Role of law enforcement in addressing this gap to enhance subjective feelings of safety in the cyber space.

B. Research Design

The research uses data from an empirical survey conducted online via Google Forms to analyse subjective feelings of safety in the cyber space with respect to the reported fear of inchoate cyber-crimes. These conclusions have then been studied in relation to the cyber laws of India and the role and responsibility of law enforcement officials. Essentially, data was gathered from reports, judicial decisions, and statutes, studied together with the 57 responses received to the survey conducted by the authors. The Google Form automated charts generated for each question separately were examined, and further analyses of the responses was done using Graphs and Pivot Charts in MS Excel.

INCHOATE CRIMES IN CYBER SPACE

Inchoate means something which has "*just begun and not so fully formed*"[18]. Inchoate crimes would be those crimes that have initiation but the completion is dicey, as in the crimes that have been initiated but were never completed. What does the law say about crimes which have not been committed completely? A few examples of inchoate crimes are an attempt to murder, conspiracy, abetment, instigation, etc. The laws in India strictly the Indian Penal Code still punish these laws even if no actual act of crime has been committed yet. A similar set of crimes exists in cyberspace

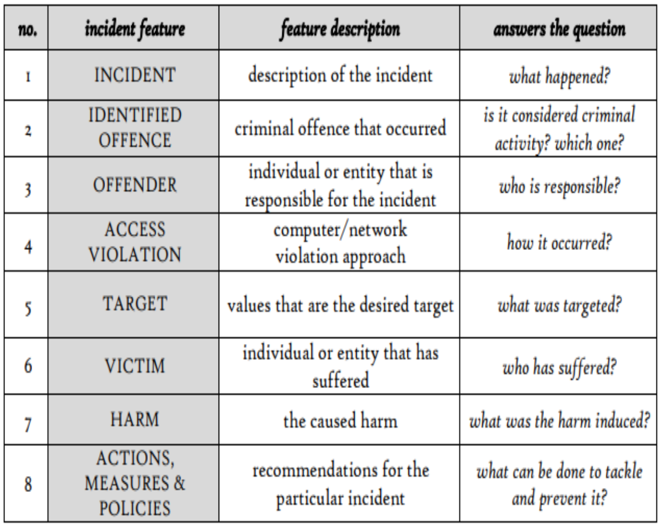
[18] Prof. R.K.Chaubey and 2012, "'An Introduction to Cyber Crime and Cyber law'" *Kamal Law House, 2012available at*: https://www.bbau.ac.in/dept/Law/TM/1.pdf (last visited July 19, 2022).

as well, where the harm to the victim cannot be actually or physically committed but an intervention can protect against greater harm. We can also call it the underdeveloped crime of cyberspace. This paper through rationale and doctrinal research has explained the types of inchoate cyber-crimes.

A. A few types of Cyber-crimes:

The feature of identifying a cyber-crime

'target', victim', and 'harm' describe the aim of the cyber-crime incident along with those that suffered and the consequences like individual, systemic and inchoate harm sustained. Based on harm crime can be divided into Individual, systemic and inchoate harm.



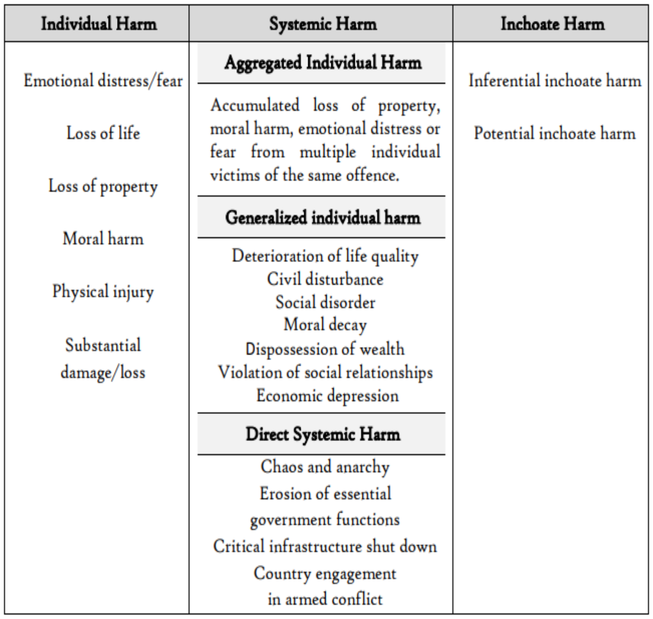
no.	*incident feature*	*feature description*	*answers the question*
1	INCIDENT	description of the incident	*what happened?*
2	IDENTIFIED OFFENCE	criminal offence that occurred	*is it considered criminal activity? which one?*
3	OFFENDER	individual or entity that is responsible for the incident	*who is responsible?*
4	ACCESS VIOLATION	computer/network violation approach	*how it occurred?*
5	TARGET	values that are the desired target	*what was targeted?*
6	VICTIM	individual or entity that has suffered	*who has suffered?*
7	HARM	the caused harm	*what was the harm induced?*
8	ACTIONS, MEASURES & POLICIES	recommendations for the particular incident	*what can be done to tackle and prevent it?*

Table 1: Categorizing Inchoate Crimes

Source of Table 1 & 2: Table 1 & 5 from A systematic approach toward description and classification of cyber-crime incidents. (George Tsakalidis and Kostas Vergidis).

Traditional crimes and cyber-crimes share essential commonalities and therefore crime metrics can be understood to cyber-crimes as they both inflict harm either individual, systemic or inchoate. The possible harm that can result from cyber-crime incidents is presented in Table 2.[19]

[19] George Tsakalidis and Kostas Vergidis, "A Systematic Approach Toward Description and Classification of Cybercrime Incidents," 49 *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 710–29 (2019).



Individual Harm	Systemic Harm	Inchoate Harm
Emotional distress/fear Loss of life Loss of property Moral harm Physical injury Substantial damage/loss	**Aggregated Individual Harm** Accumulated loss of property, moral harm, emotional distress or fear from multiple individual victims of the same offence. **Generalized individual harm** Deterioration of life quality Civil disturbance Social disorder Moral decay Dispossession of wealth Violation of social relationships Economic depression **Direct Systemic Harm** Chaos and anarchy Erosion of essential government functions Critical infrastructure shut down Country engagement in armed conflict	Inferential inchoate harm Potential inchoate harm

Table 2: Identifying Inchoate Cyber-crimes

Inchoate harm is the harm inflicted by inchoate cyber-crimes. It is obvious that there is no actual harm resulting from these crimes as they have not been completed, but they embody a potential for harm that is illegal according to criminal law. The two types of inchoate harm are: inferential and potential. When a fraudster sends out phishing e-mails, apart from individual harm to the ones successfully victimized, the offender sought to inflict, but failed to do so to those that did not respond, which is characterized as inferential inchoate harm.

For example, online posting of personal information can lead to their injury which to the residual category of potential inchoate harm. The illegal downloading of a movie is a copyright-related offense, against the intellectual property of a company resulting in loss of property and potential inchoate loss of property.

B. The Cyber-crimes Mentioned and their Inchoate Nature:

1. Cyber Harassment

    a) Cyber Hate – The natural human tendency to let go off "casual remarks" even in the physical space increases the difficulty in designating criminal intent to hateful comments and posts online. And then of course, the blurred line between the internet bestowing the ultimate freedom of speech and everyone's right to dignity and respect make this an inchoate cyber-crime.

b) Cyber Bullying – What in the physical space is shrugged off as friendly banter can take on the ugly face of cyber bullying when it crosses the legal threshold of cyber criminality, and that is what makes cyber bullying an inchoate cyber-crime.

c) Defamation – What counts as defamation when shared in a public space, does not amount to the same offence when shared over emails or private messages despite the similar underlying behavioural tendencies, thereby giving the offence of defamation an inchoate nature.

d) Impersonation – The varying intentions of impersonating another makes it an inchoate cyber-crime until the person impersonated actually suffers harm due to the act of impersonation.

2. Cyber Stalking – The widely accepted harmlessness or even alleged good intent of cyber stalking is what give it an inchoate characteristic wherein, till the time the victim is physically harmed or even visibly harmed in the cyber space, despite the constant dread and threat to safety, it is difficult to prove criminal intent beyond reasonable doubt in a court of law.
3. Obscene Content Sharing – Since a one-time incident can be bailed out as an "unintentional mistake", and because it is not until persistent sharing unwanted obscene messages that the criminal intent would even be detected, obscene content sharing too has an inchoate nature to it.

4. Cyber Grooming – The nature of such criminal behaviour which often starts off as seemingly harmless friendly behaviour towards a child give it an inchoate nature where, till the time the “friendliness” turns exploitative, it is difficult to consider it an offence and yet, the child is under constant threat of potential abuse without and visible red flags in the situation.
5. Child Pornography – While child pornography in itself is a defined criminal offence, the fact that privately viewing child pornography is protected by right to privacy and not included in the ambit of the definition of the crime, makes this particular behaviour, i.e., viewing child pornography in private an inchoate cyber-crime.

The survey conducted by the researchers had eliminated questions on fear and experience of child grooming and child pornography for ethical reasons. The other crime typologies as mentioned above has been studied with respect to awareness, fear and experience of the same by Indian netizens.

C. Related Laws in India

The following table illustrates in details the legislation related to cyber-crimes in India:

Names of the Acts	Sections	Types of Cyber-crimes Covered
	292: Sale, etc., of obscene books, etc. 345 C: Voyeurism	Obscene Content Sharing Child Pornography (Hicklin’s test)

Indian Penal Code, 1860		*Ranjit D. Udeshi vs. State of Maharashtra*
	354D: Stalking	Cyber Stalking *Kalandi Charan Lenka vs. State of Odisha, 2017*
	499: Defamation	Cyber Defamation
	503: Criminal intimidation 509: Word, gesture or act intended to insult the modesty of a woman	Cyber Hate and Cyberbullying
Information Technology Act, 2000	66A: Punishment for sending offensive messages through communication service, etc. [struck down by *Shreya Singhal vs. Union of India,* AIR 2015 SC. 1523.] 66E: Punishment for violation of privacy 67: Punishment for publishing or transmitting obscene material in electronic form.	Obscene Content Sharing Child Pornography *Sam Infant Jones vs. State, 2021 SCC OnLine Mad 2241*

	67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form 67B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	
	66C: Punishment for identity theft	Impersonation

Table 1: The table is made by the authors

With the invention of the internet, the world around us changed forever and there is no denying that. During the difficult years of the pandemic, we have observed more dependency on the internet all over the world. When earlier people use to have televisions, computers, and phones for different purposes now in each device an internet connection is a must, everything and anything you want to do can be done online. The fast-growing and evolving convenience of people has also resulted in an increase in the crime rate in cyberspace. While in the pandemic we saw a decrease in the rate of physical/traditional crimes[20] like an offense against women, offenses against the human body,

[20] Crime in India – 2020, https://ncrb.gov.in/sites/default/files/CII%202020%20SNAPSHOTS%20STATES.pdf
Crime Cases See 28% Rise Since 2019, COVID-19 Violations Among Leading Causes: NCRB, https://thewire.in/government/crime-cases-see-28-rise-since-2019-covid-19-violations-among-leading-causes-ncrb

kidnapping and abduction, etc. there was an overall increase in the crimes in cyberspace[21] that can be seen in the following graphs of figure I (2010-2018) which depicts the registered cases according to the report of NCRB and figure II (2018-2021) which depicts reported cases according to the CERT-In a nodal agency responding to the computer security incidents in India established in 2004 and designated as an agency on cyber security under the Information and Technology 2008 Act. The statistics on cyber-crimes are collected under the following heads by NCRB:

i) Offences registered under the Information Technology Act, 2000.

ii) Offences under the IPC related to cyber-crimes

iii) Offences under the Special and Local Laws (SLL) related to cyber-crimes

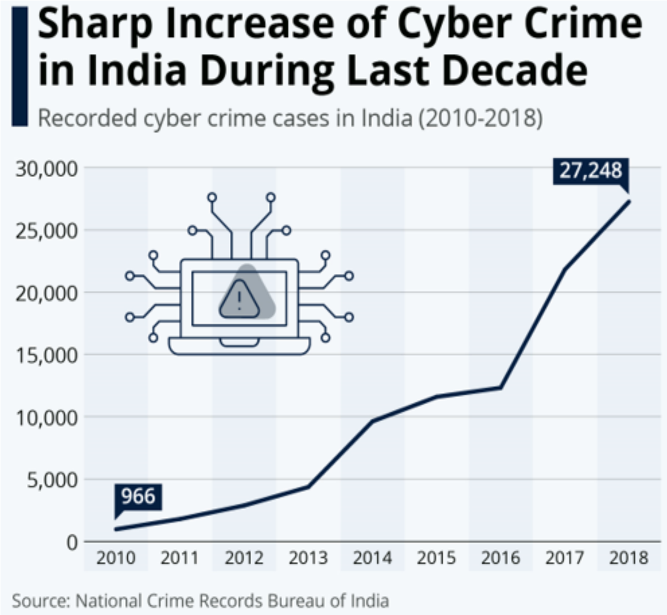


Figure 3: Cyber-crime Data in India from NCRB

Cyber laws as we all understand don't have a fixed definition, Indian legislation doesn't define or provide a definition for cyber-crimes in any statute even the Information Technology Act, 2000 (IT Act) which essentially deals with cyber-spaces and crimes doesn't define the term. In general, through scholars' cyber-crime is understood as any illegal activity which takes place over the internet or computers.

[21] Crimes against women dip by 24%, cybercrimes see 55% rise: NCRB data, https://www.thehindu.com/news/cities/Delhi/crimes-against-women-dip-by-24-cybercrimes-see-55-rise-ncrb-data/article36486113.ece

Reporting of Cyber-crimes in India

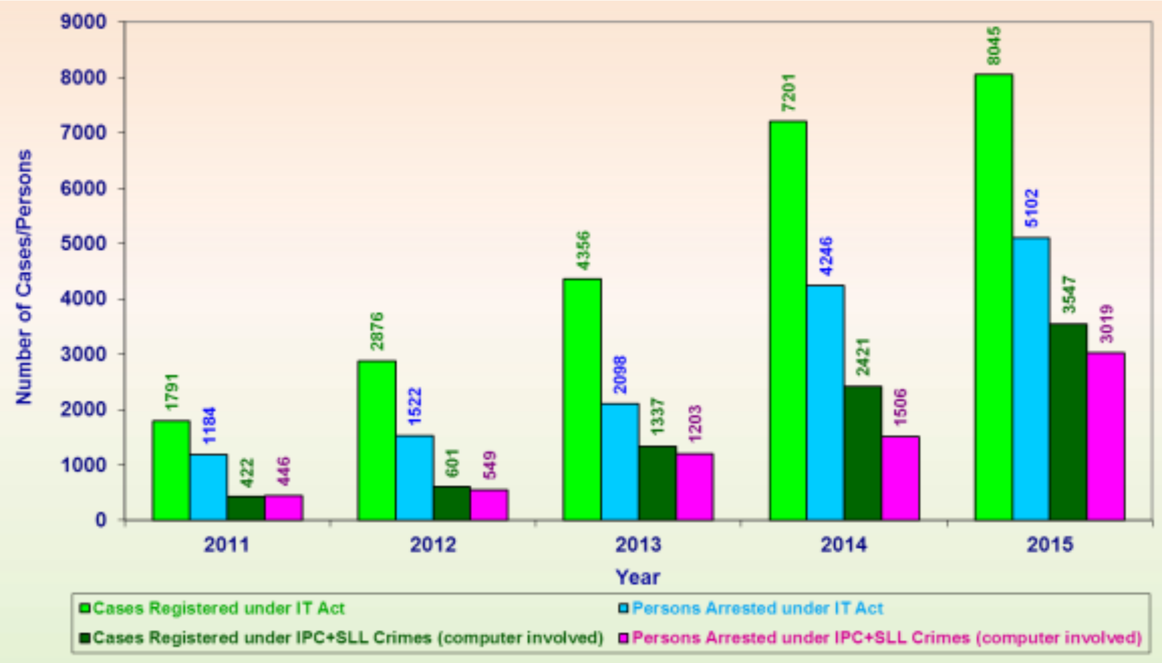


Figure 4: Cases Registered and Persons arrested under IT Act and IPC
Source: NCRB

It is also interesting to note that while financial cyber-crimes are largely reported to the authorities, inchoate cyber-crimes as described in this paper rarely, if ever, get reported to the police. It is to address this disparity in the category of cyber-crimes reported and consequently investigated in India that this research project had been designed as a pilot study into the matter.

RESEARCH FINDINGS

A. Research Participants:

Since parental consent could not be ensured via an online circulated Google Form, all research participants were above 18 years of age, with the large majority of participants being in their 20s.

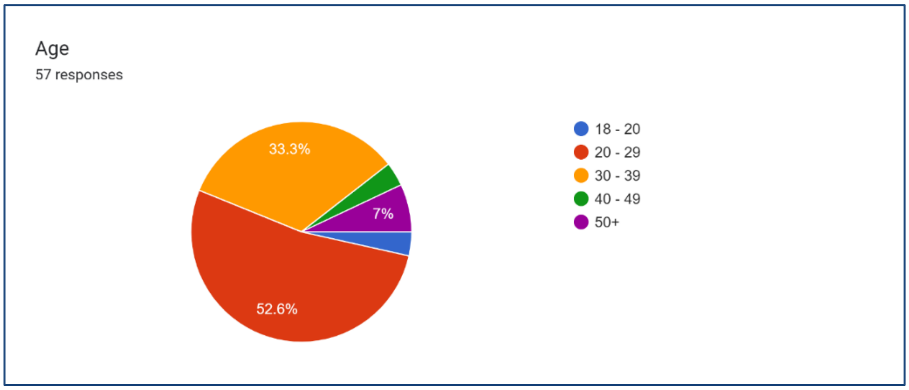


Figure 5: Age Distribution of Research Participants (Graph Downloaded from Google Form Response Sheet)

The questionnaire was so designed to group the research participants into the following 7 categories:

i) Criminal Justice professionals with Cyber/IT knowledge/affiliation

ii) Security/defence professionals with Cyber/IT knowledge/affiliation

iii) Civilians with Cyber/IT knowledge/affiliation

iv) Criminal Justice professionals with Non-IT background

v) Security/Defense professionals with Non-IT background

vi) Civilians with Non-IT background

vii) Civilians from Non-IT unorganized sector of work

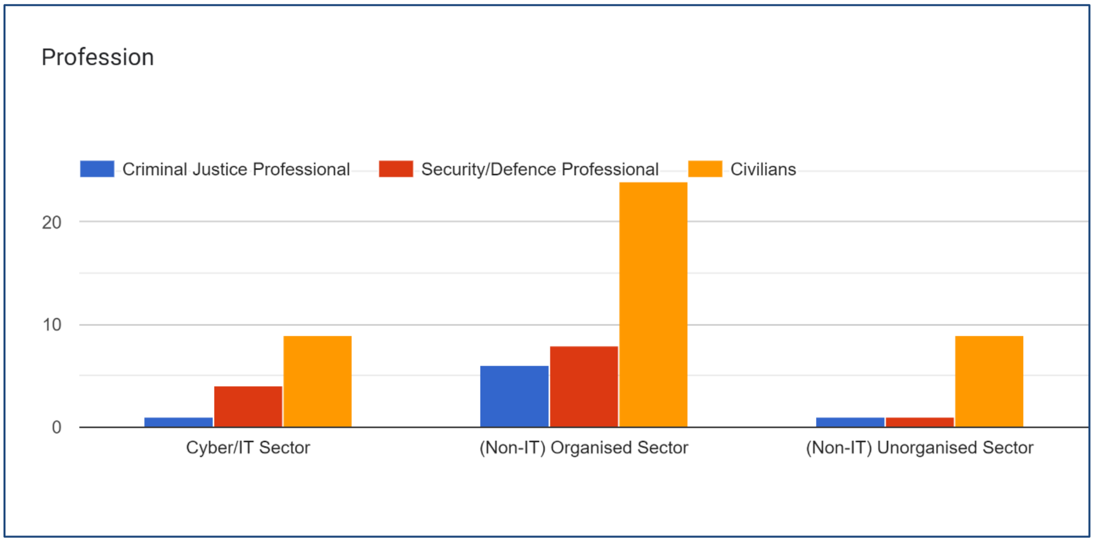


Figure 6: Professional Typologies of the Research Participants (Graph Downloaded from Google Form Response Sheet)

However, as the chart above represents, due to lack of comparable number of participants form each group, a comparative analysis based on professional affiliations was not statistically possible.

B. Demographic Details and Subjective Feelings of Safety:

- Given the limited number of respondents, and also due to random sampling, we did not get comparable number of respondents from different religious groups and ethnic communities. Hence, we couldn't analyse the data in terms of:
  i) Any possible co-relation between religion and subjective feeling of safety online.
  ii) Any possible co-relation between ethnicity and subjective feeling of safety online.

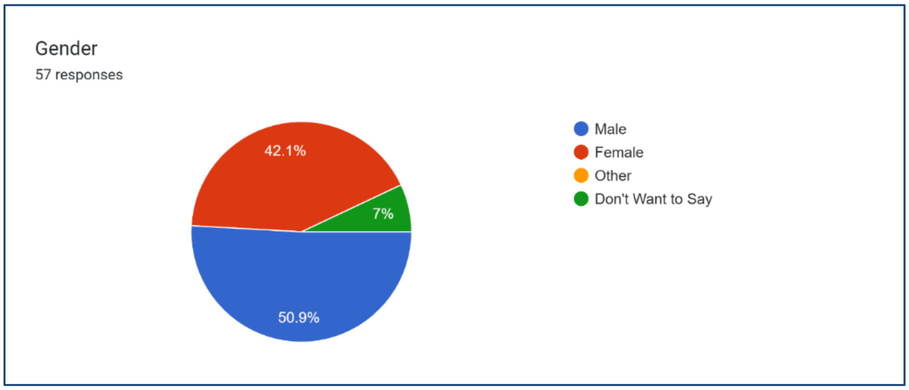


Figure 7: Gender Groups of the Research Participants (Graph Downloaded from Google Form Response Sheet)

- However, the data has been analysed in terms of gender and overall reported fear of inchoate cyber-crimes to conclude that *only a 2% difference in the Overall Fear of Inchoate Cyber-crimes and the different Gender Groups of the Respondents was recorded, with female participants showing an overall higher average of over fear scores than the male respondents*.

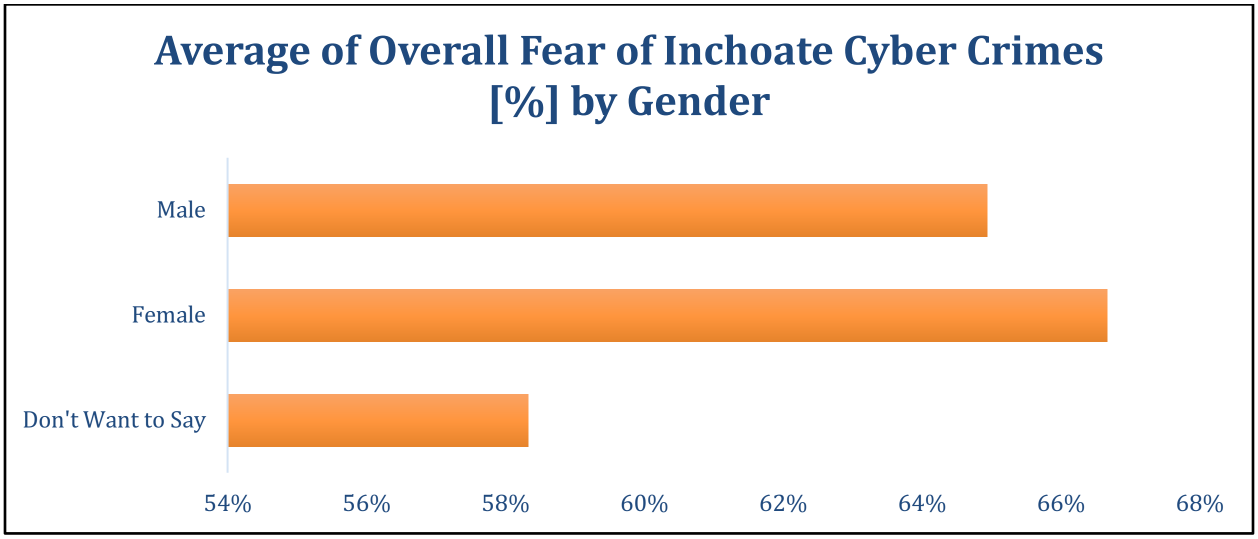


Figure 8: Gender vs Fear of Inchoate Crimes (Graph created on MS Excel)

C. Awareness and Fear of Inchoate Cyber-crimes/Subjective Feelings of Safety in the Cyberspace:

This was assessed in the following two ways:

i) Fear of inchoate cyber-crimes in comparison to awareness of the online acts that actually count as criminal.

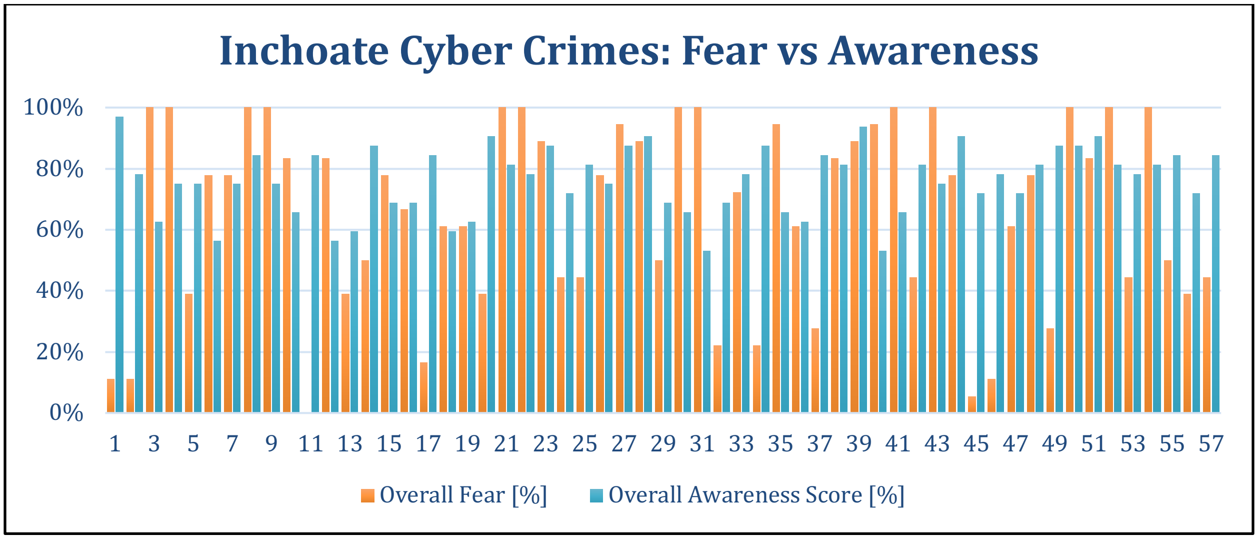


Figure 9: Fear of Inchoate Cyber-crimes vs Awareness of Inchoate Cyber-crimes
(Graph created on MS Excel)

ii) Self-reported scores of awareness recorded at the very beginning of the survey in comparison to the actual reported awareness of online acts criminalised by the law.

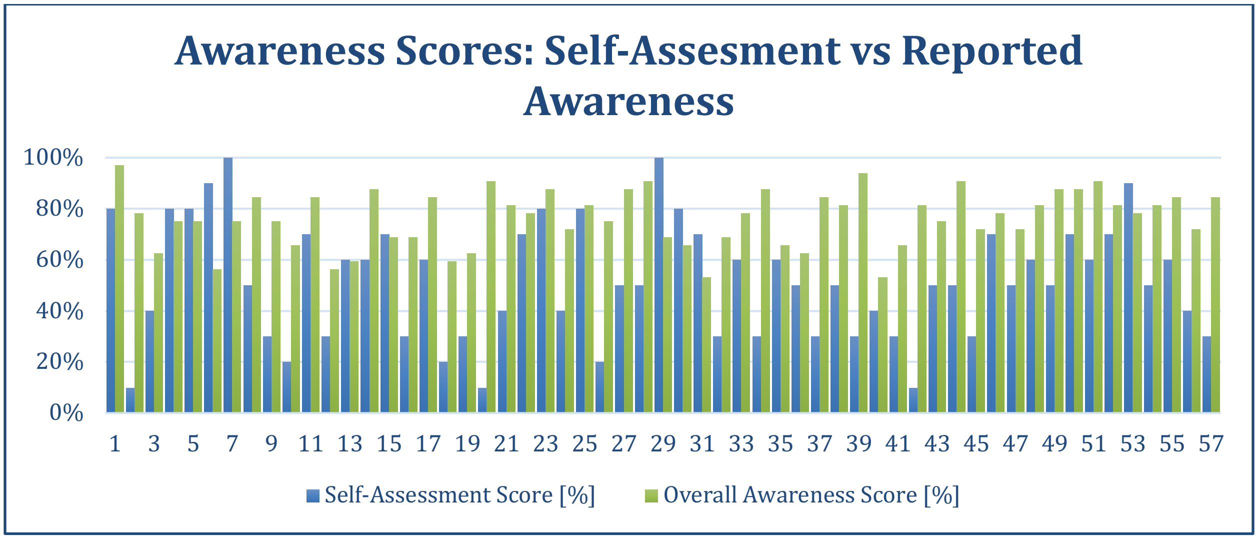


Figure 10: Self-Assessed Awareness vs Actual Awareness of Inchoate Cyber-crimes (Graph created on MS Excel)

- In congruence with the hackneyed suggestion of the dire need for awareness, most of the research participants are observably unaware of the list of legally unacceptable online behaviour. As appalling as it is to note the indifference of research participant to questions on subjective feelings of safety, as expressed in the "there's nothing we can do about it anyway" option, it is equally alarming to go through the specific ingredients of inchoate cyber-crimes that have not been cognizantly selected as criminal in the survey. *While the apathy to any possible redressal mechanism on the part of the potential victim pool poses great challenge for law enforcement initiatives to be effective, the lack of knowledge about potentially criminal behaviour massively hinders any efforts in apprehending a potential criminal and managing his/her criminogenic risk factors and re-routing the person into civil society.*

D. Fear of Inchoate Cyber-crimes and Actual Experiences of the Same in the Cyberspace:

- Another observable fact from this data set is that most of the participants report being fearful of specific cyber-crimes even without an actual experience of the same. Of course, there is no limitation observed in the total number of hours they spent in the cyberspace or even any significant difference in the types of online platforms accessed. *However, this general sense of fear, in other words this lack of subjective feelings of safety is important to take notice of and implement cyber surveillance strategies since increasing complacence to fear of a certain group of crimes only increases victim proneness among the population.* The following set of 7 charts (Figures 11 to 17) illustrate this observation, wherein the first set of legends on the vertical axis refers to reported fear of the crime while the consequent set of legends show an actual experience of the same:

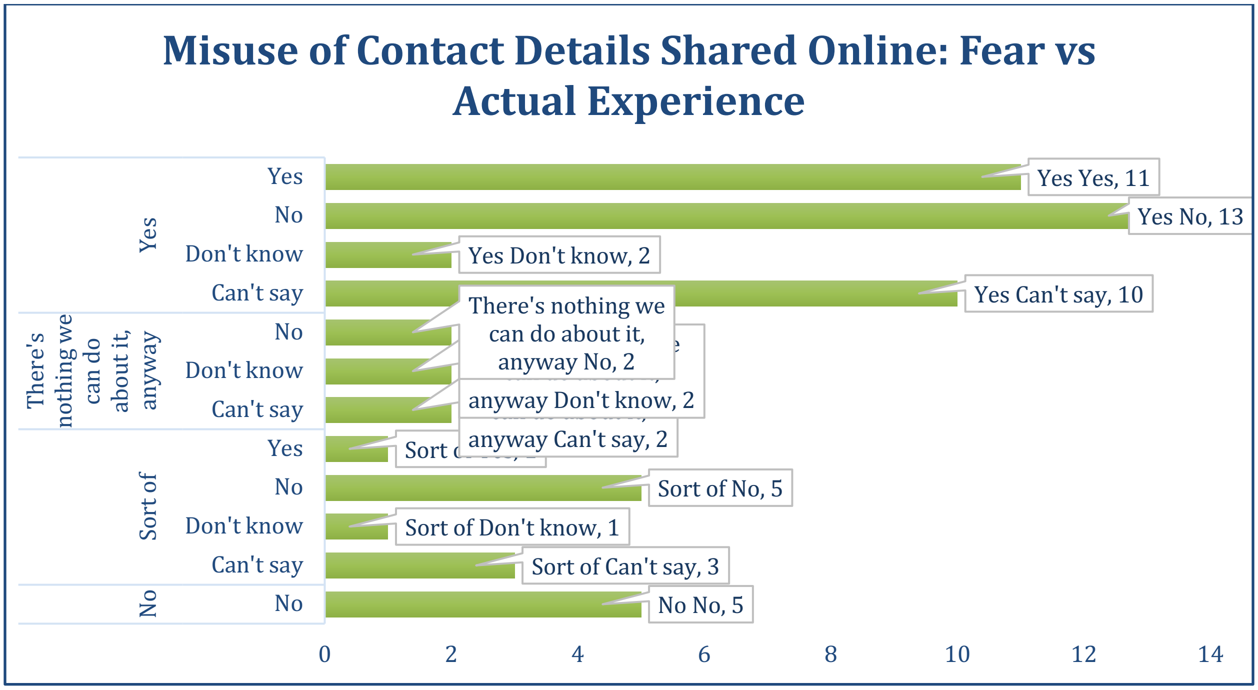


Figure 11: Fear vs Actual Experience of Misuse of Contact Details Shared Online
(Graph created on MS Excel)

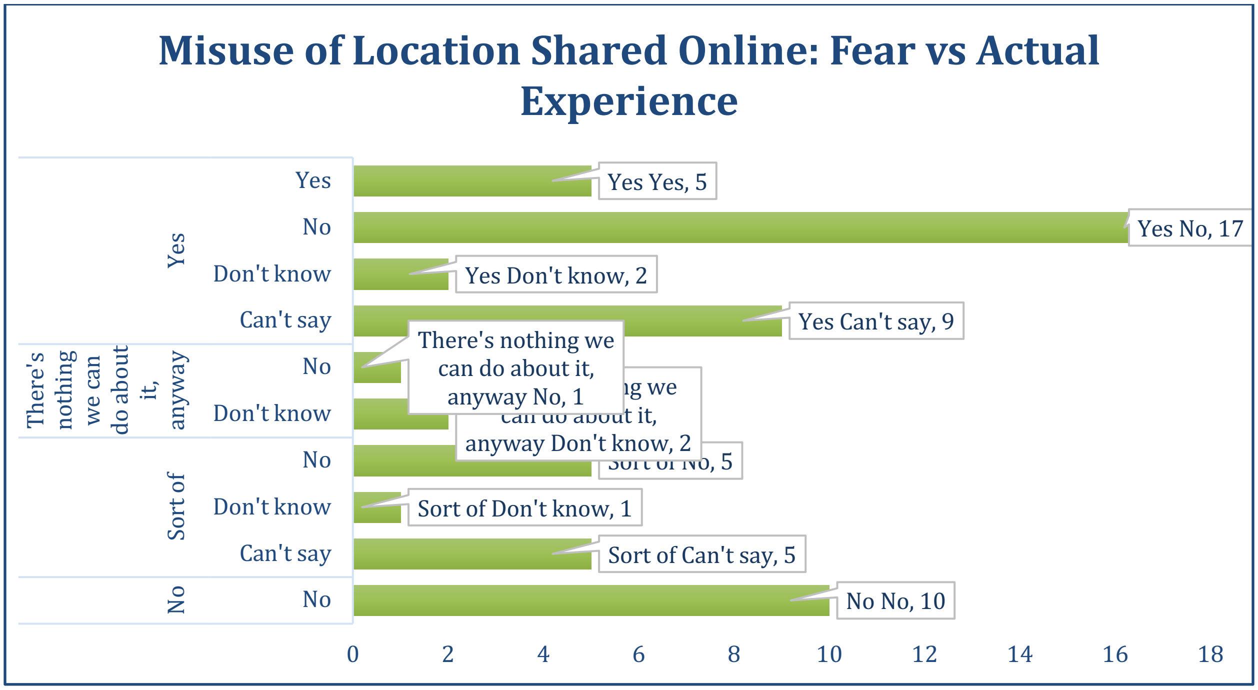


Figure 12: Fear vs Actual Experience of Misuse of Location Shared Online (Graph created on MS Excel)

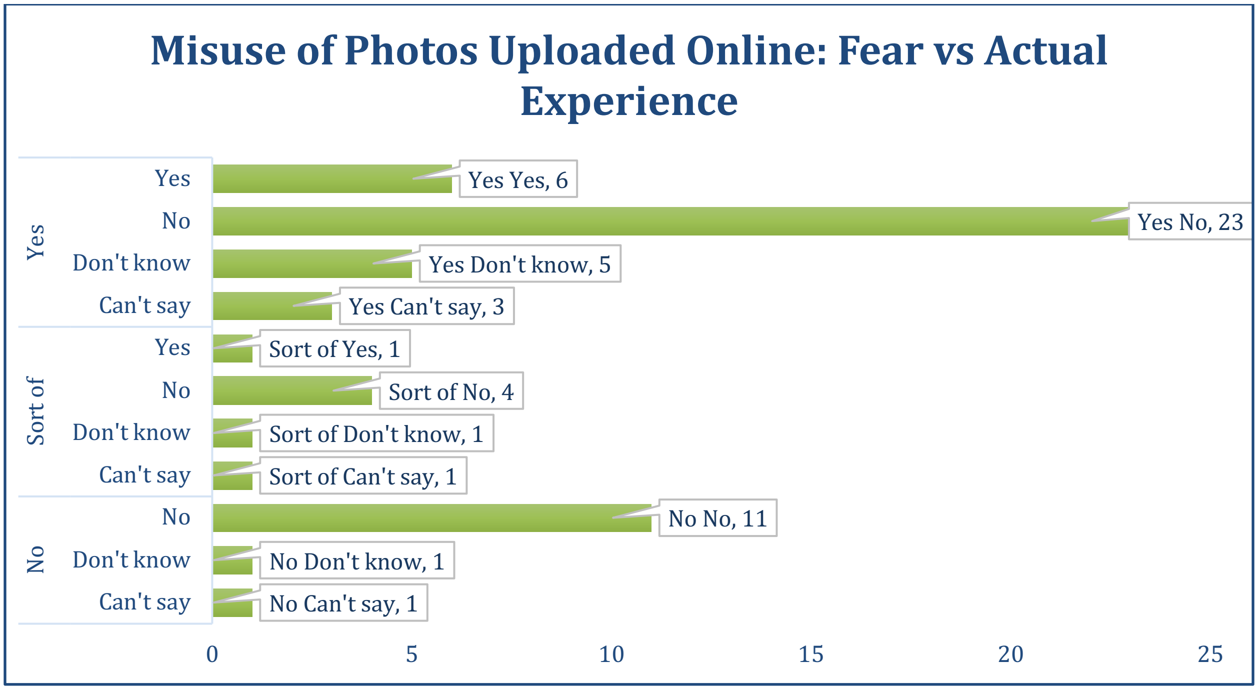


Figure 13: Fear vs Actual Experience of Misuse of Photos Uploaded Online (Graph created on MS Excel)

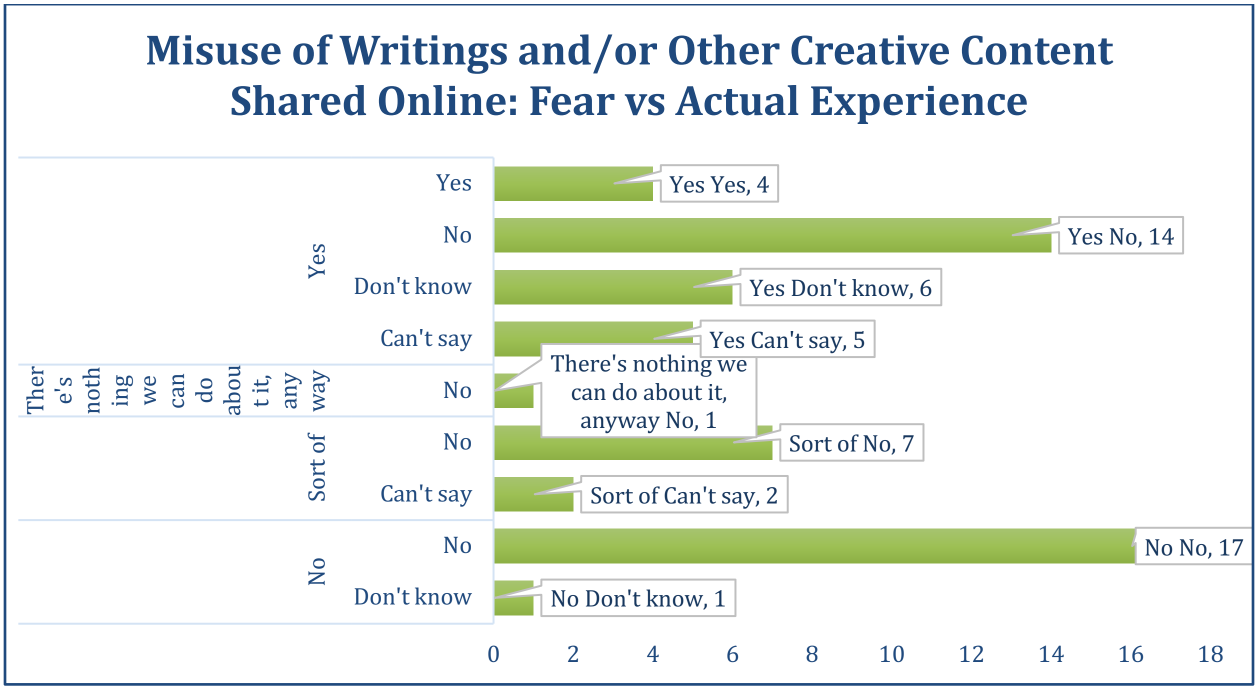


Figure 14: Fear vs Actual Experience of Misuse of Creative Content Shared Online (Graph created on MS Excel)

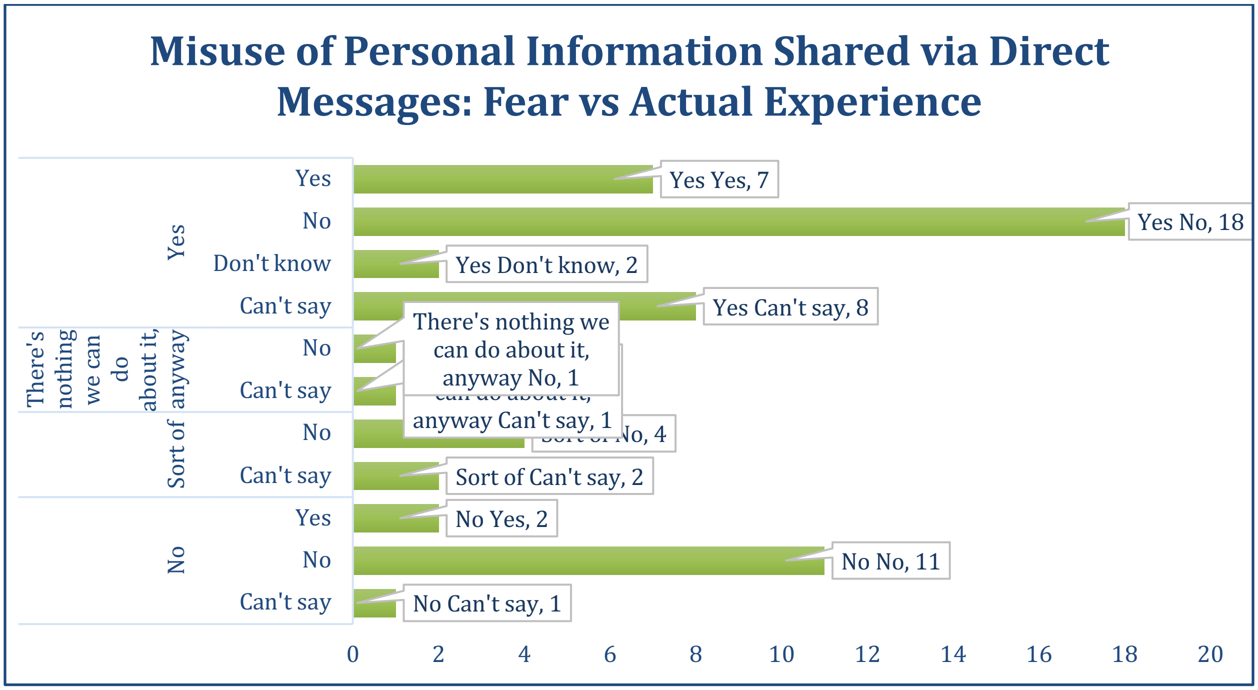


Figure 15: Fear vs Actual Experience of Misuse of Personal Information Shared via Direct Messages (Graph created on MS Excel)

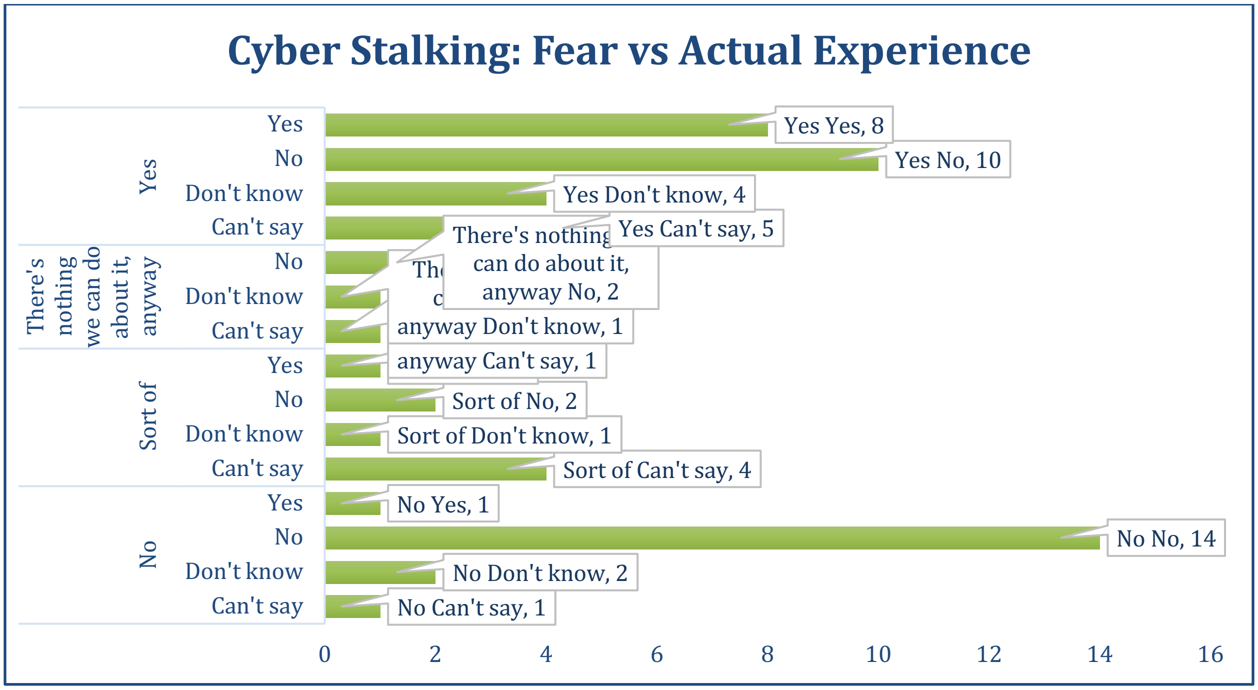


Figure 16: Fear vs Actual Experience of Cyber Stalking (Graph created on MS Excel)

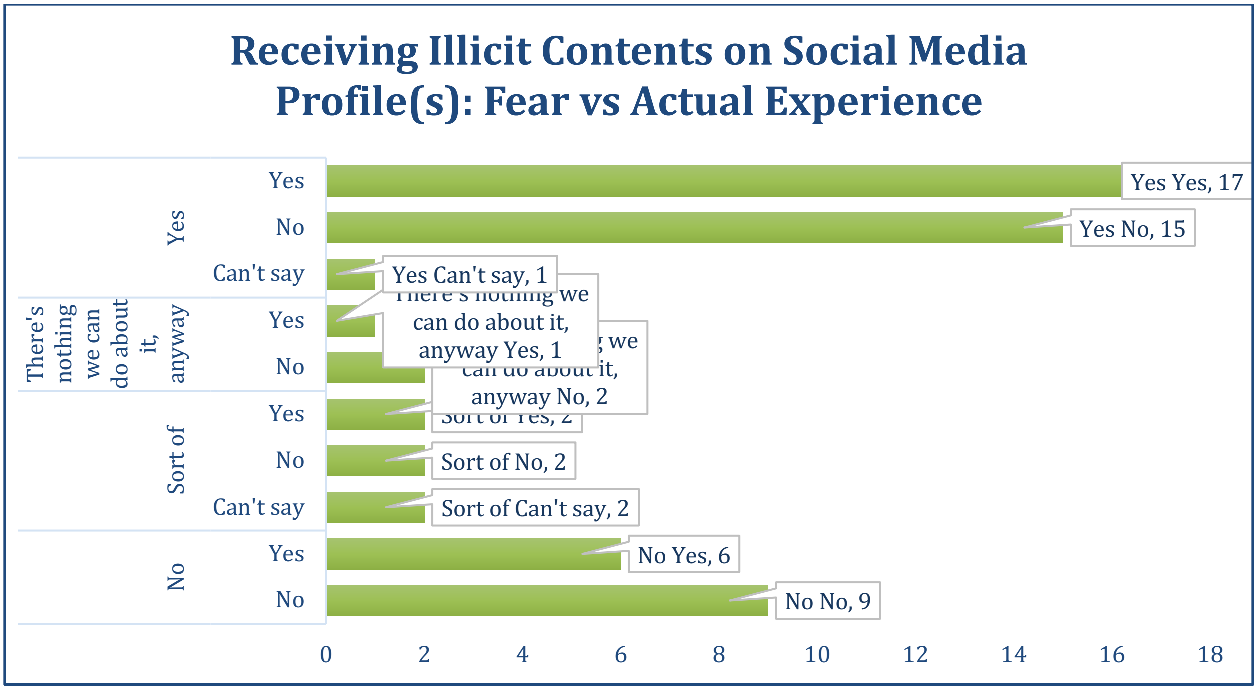


Figure 17: Fear vs Actual Experience of Receiving Illicit Contents on Social Media Profile(s) (Graph created on MS Excel)

i) Most Feared in the Cyberspace:

Subjective feelings of safety in terms of being victims of inchoate cyber-crimes clearly varies across the various social media platforms available online.

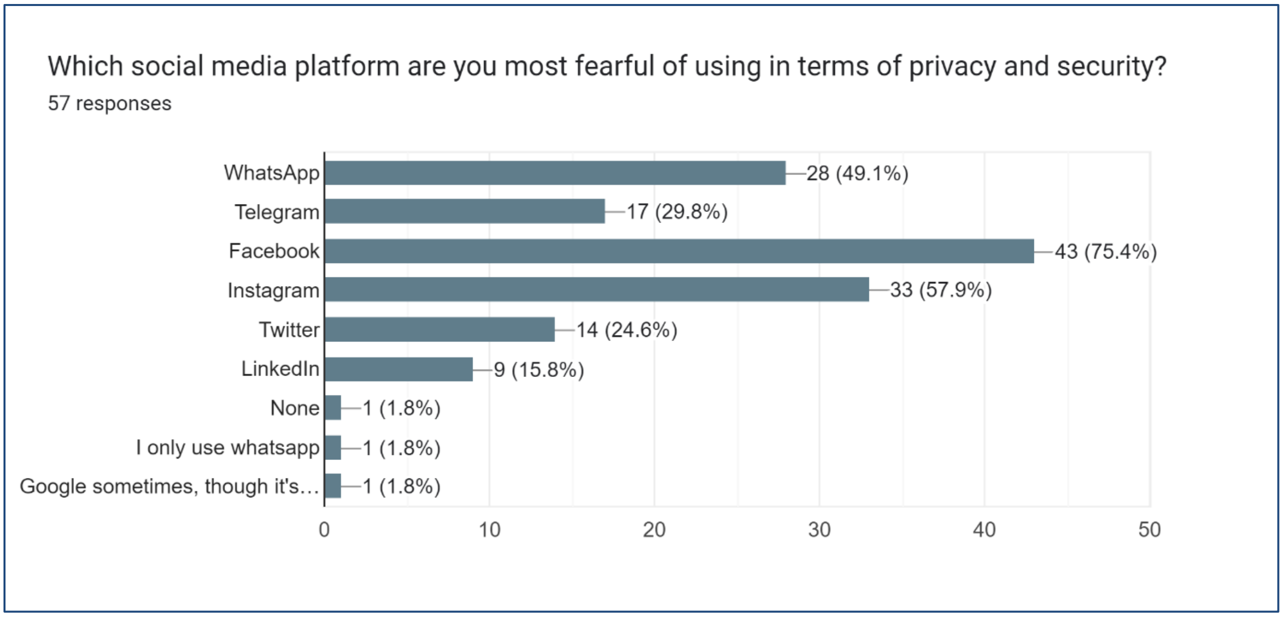
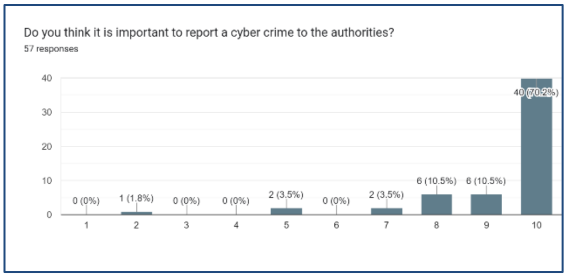


Figure 18: Most Feared Social Media Platform (Graph Downloaded from Google Form Response Sheet)

- According to this survey, the most feared social media platform is Facebook, followed by Instagram and WhatsApp. *It is interesting to note that the most feared platforms are also the most widely used, in contrast to the least feared social media which is LinkedIn.*
- *It is also important to note that the most feared factor in the cyber space, as reported by the respondents, is lack of privacy, which is a widely accepted threat, and yet, as of this date, the legislation does not completely clarify redressal mechanism on this aspect in the cyberspace.*

ii) Reporting of Inchoate Cyber-crimes by Netizens:

The following 3 charts read together shows that a large majority of the respondents do believe in the relevance of reporting cyber-crimes to the concerned authorities, but when actually in a situation to do so, they answer in the negative.



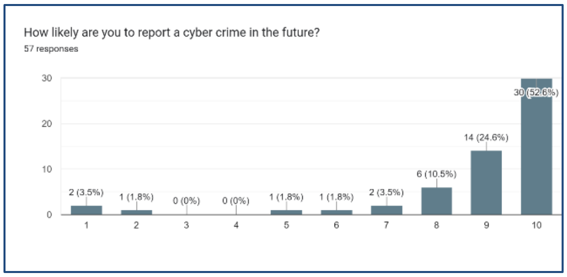


Figure 19: Perceived Importance of Reporting Cyber-crimes (Graph Downloaded from Google Form Response Sheet)

Figure 20: Actual Likelihood of Reporting Cyber-crimes (Graph Downloaded from Google Form Response Sheet)

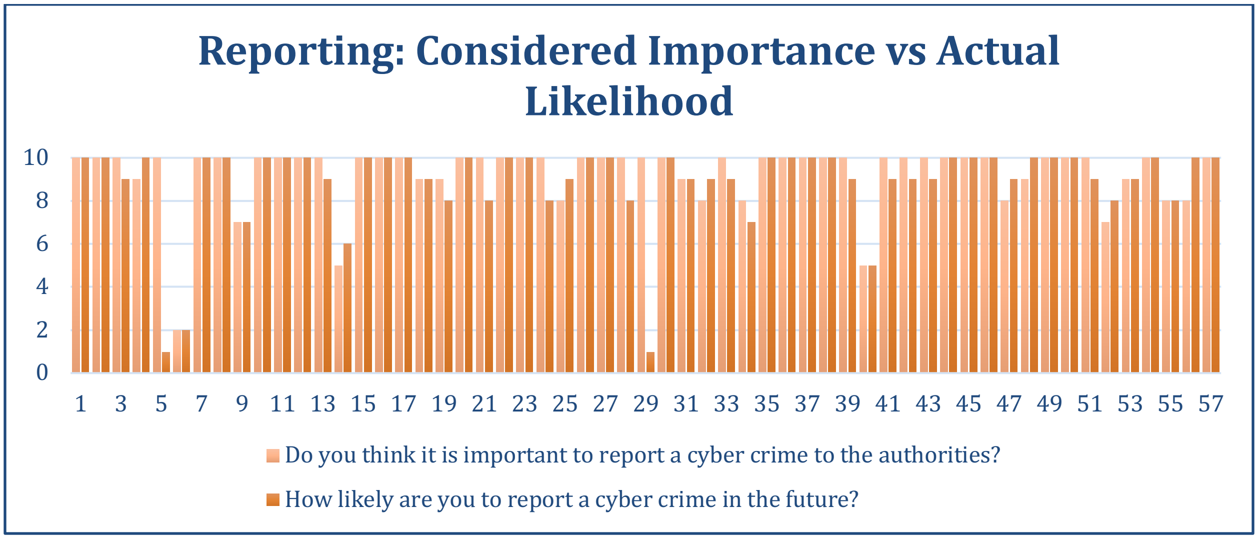


Figure 21: Perceived Importance vs Actual Likelihood of Reporting Cyber-crimes (Graph created on MS Excel)

A comparison of actual incidence of victimisation with whether such incidence was reported to law enforcement is depicted in the following chart:

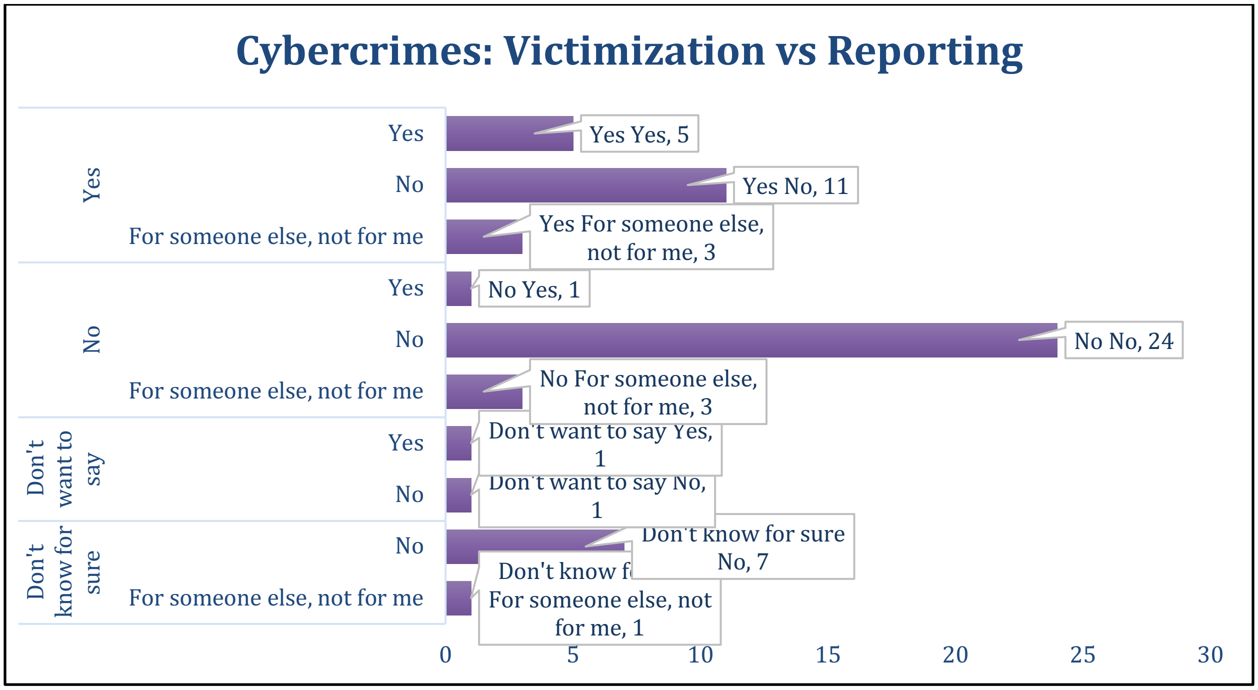


Figure 22: Victimization vs Reporting of Inchoate Cyber-crimes (Graph created on MS Excel)

The first set of legends on the vertical axis refers to victimization of inchoate cyber-crimes while the corresponding set refers to reporting of such cases. Interesting findings include:

i) An odd 3% of respondents who said that they have themselves been victims of such crimes, yet have reported such an offence for someone else and not for their ownselves.

ii) The roughly 7% of participants who report not being sure of whether or not their experience even amounts to an inchoate cyber-crime shows the constant need for raising awareness about what counts as illegal activity in the cyber space as per the law of the land.

The questionnaire also asked the respondents whether they had or would report a cyber-crime on behalf of a victim, if they have such definite knowledge of such criminal activity. The respondents were also asked for the reasons that stop them from reporting inchoate cyber-crimes to the police.

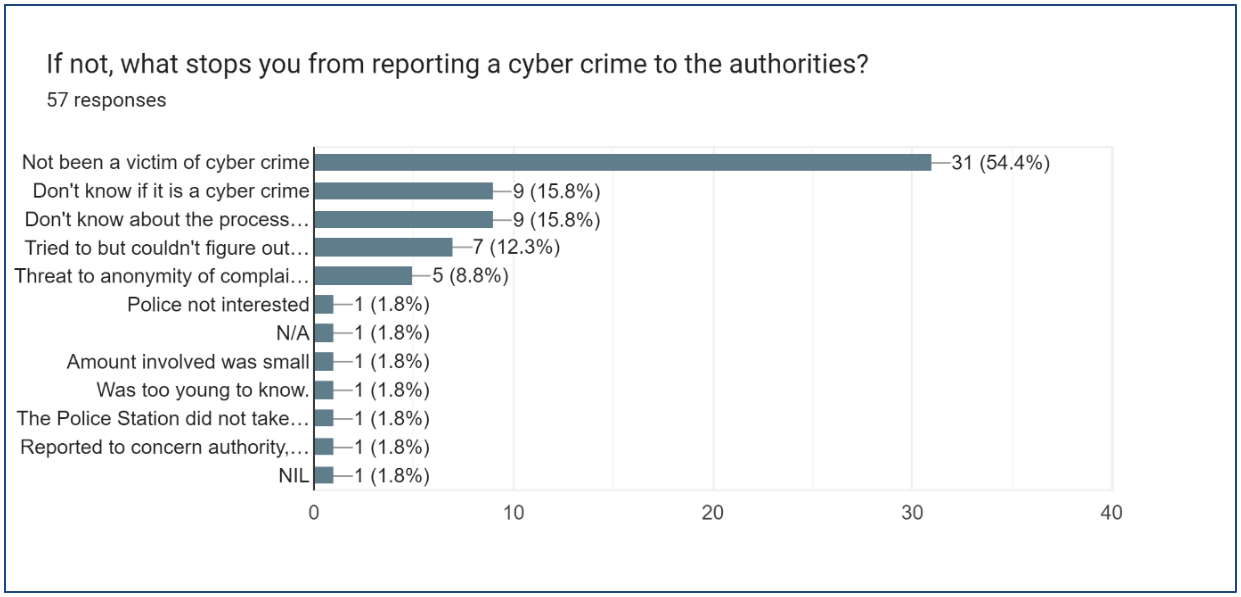


Figure 23: Reasons for Not Reporting Cyber-crimes (Graph Downloaded from Google Form Response Sheet)

As illustrated in this chart, mostly due to lack of awareness about how to file a complaint and previous one-off unfavourable experience with law enforcement, respondents are largely hesitant and even reluctant to report a cyber-crime even when the case arises.

This is an alarming reality that brings us to the last section of our paper where we write about the consequently increased responsibility of law enforcement officers in terms of surveillance and prevention of inchoate cyber-crimes.

E. Analysis of the Research Findings:

Concluding the observations from the dataset with respect to our primary research objectives, it is evident that there is a persistent hesitation in reporting inchoate cyber-crimes, irrespective of the quantum of overall fear of such cyber-crimes reported or even the overall awareness scores. Although a majority of 70.2% visibly think it to be important to report cyber-crimes, only a 52.6% say that they would actually go ahead and report an incidence of cyber-crime if the case arises.

One of the primary aims of a criminological assessment is to connect the details of an incidence of crime with potentially similar pre-crime situations in the society, offline or online, and consequently assist law enforcement in preventing and managing criminal behaviour. In this regard, strictly speaking of inchoate cyber-crimes here, it is crucial to address this gap between awareness and actual likelihood of reporting such cyber-crimes. While increased awareness among the general population is the unquestionable first step in the process, the responsibility of law enforcement as first responders becomes manifold to compensate for the dearth of reporting of real time incidences of inchoate cyber-crimes.

Role of Law Enforcement Agencies

As discussed earlier we must understand that Police or Law Enforcement Agencies are the initial point of contact for commencing any procedure in the Criminal Justice System which consists of Police, Prosecution, Judiciary and Correctional Institutions. Here we explore the role of police in addressing various cases of cyber-crimes in general, and inchoate cyber-crimes in particular, and what are the changes that can be sought into this.

The role and responsibilities of law enforcement agencies as the first point of contact in any criminal activity is considered as one of the vital parts of any criminal investigation to be carried forward. We have witnessed the evolving role of law enforcement, i.e. police organisations, in India and abroad from the early setup of modern police force in 19th Century to the increasingly contact-less post-COVID setup in the 21st century. When the earliest police organisation was setup in 1800's, Sir Robert Peel while setting up of Metropolitan Police in London in 1829 gave 9 principles now known as the Peelian Principles of Policing. These principles were constituted around core principles that are invaluably true to this date. We can state his ideas in the following manner:

1. The basic goal of police is not catching criminals but preventing crime. We have no need to supress rights of citizens if the police can stop crime before it happens.
2. An important key to preventing crime is earning public support. Every community member must share the responsibility of preventing crime, as if they were all volunteer members of the force.
3. The police earn public support by respecting community principles. Winning public approval requires hard work to build reputation, enforcing the laws impartially, hiring officers who represent and understand the community, and using force only as a last resort.[22]

In the 21 st century, we have evolved from witnessing crimes such as robbery, murder to crimes occurring in the virtual world, i.e. the cyber space, and face the urgent need for change in tactics of policing all around the globe; and India is no exception to it. So, now the question remains how do we tackle cyber-crimes in general, and inchoate cyber-crimes in particular, considering the

[22] T.A. Jenkins, Sir Robert Peel (Red Globe Press London, New York, 1999)

practical challenge of an often-obscure chain of evidence being left behind for the police to investigate.

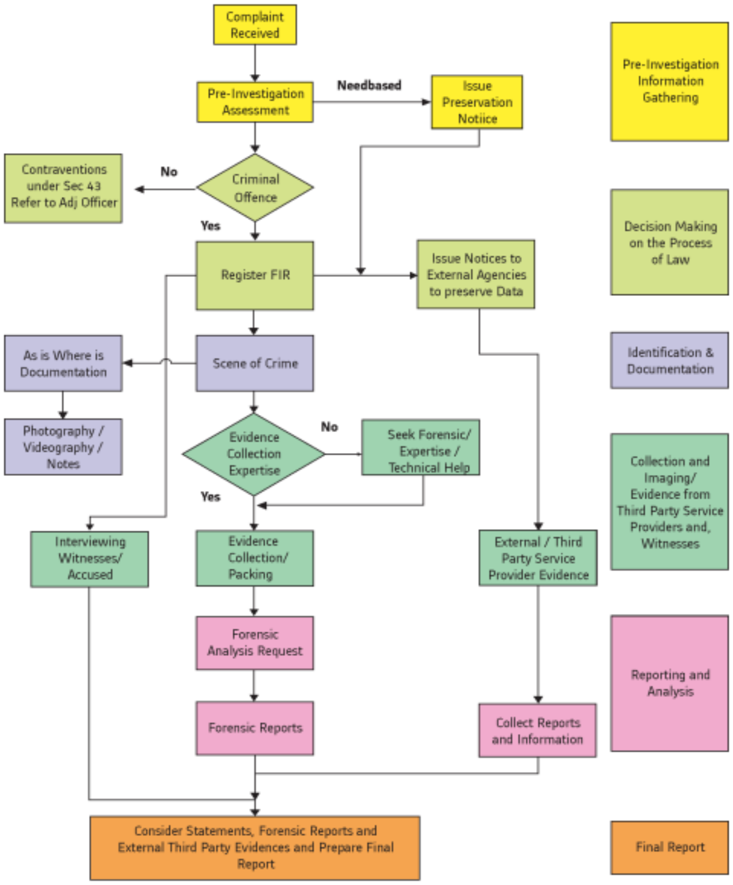
We are aware of the basic structure of police organization in India, including the organisation of different police stations for dealing with different crime-typologies, as well as the hierarchy of ranks, headed by the Director General of Police in each state, followed for increased efficiency and accountability within the law enforcement agencies. The major challenge for Cyber Police Stations is that cyber-crimes do not follow regular, expected jurisdictional norms. While police a may be under the purview of State Government, cyber-crimes and the virtual world transcend all state and even national borders. Thus, the Cyber and Information Security (C&IS) Division, Ministry of Home Affairs (MHA) deals with all the crimes related to cyber space. The duties of this division ranges from cyber security, policies related to cyber space, cybercrime and any actives related to cyber space that affects national security. However, in order to tackle crimes at the local level many state governments have set up their own Cyber Cells too.[23]

This division has launched many schemes that is playing a vital role in changing the way we deal with all crimes related to cyber space. The MHA has started a scheme called Cyber-Crime Prevention Against Women and Children (CCPWC) that deals with all the crimes related to Women and Children in Cyber Space. This scheme involves various components such as Online Cyber Crime Reporting Portal, Forensic Unit, Research and Development Unit, Awareness Creation Unit and Capacity Building Unit. All this unit has their own functions with one common goal to prevent crimes in cyber space, especially inchoate cyber-crimes as mentioned in this paper. This scheme has also facilitated several local programs to help respective state governments to

[23] 2019. *Citizen Manual for National Cyber-crime Reporting Portal*. Indian Cyber-crime Coordination Centre, MHA.

deals with cybercrime in an efficient and effective manner with respect to cyber- crime challenges in their native state communities.[24]

Investigation of digital crimes, what the INTERPOL refers to as “pure cyber-crimes”, is very different from regular crime investigation. This requires that different standards and procedures to be developed for investigation as defined in the Information Technology Act, 2008. A flow chart for investigation of digital crimes from the Jharkhand Police Manual has been included below.[25]


Complaint Received
Pre-Investigation Assessment
Needbased
Issue Preservation Notiice
Pre-Investigation Information Gathering
Contraventions under Sec 43 Refer to Adj Officer
No
Criminal Offence
Yes
Register FIR
Issue Notices to External Agencies to preserve Data
Decision Making on the Process of Law
As is Where is Documentation
Scene of Crime
Identification & Documentation
Photography / Videography / Notes
Evidence Collection Expertise
No
Seek Forensic/ Expertise / Technical Help
Yes
Collection and Imaging/ Evidence from Third Party Service Providers and, Witnesses
Interviewing Witnesses/ Accused
Evidence Collection/ Packing
External / Third Party Service Provider Evidence
Forensic Analysis Request
Reporting and Analysis
Forensic Reports
Collect Reports and Information
Consider Statements, Forensic Reports and External Third Party Evidences and Prepare Final Report
Final Report

Flow Chart for Digital Crime Investigations under ITAA 2008

Source: Jharkhand Police Manual on Digital Crimes

[24] https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme
[25] 2011. *Cyber-crime Investigation Manual*. Data Security Council of India.

Digital crimes can be differentiated as crimes affecting devices and network infrastructure in contrast to cyber-crimes affecting persons and organisations and governments. Hence, a similar protocol for the investigation of cyber-crimes affecting individuals, especially inchoate cyber-crimes as discussed here need to be adopted by the state police manuals to increase subjective feelings of safety in the cyber-space for netizens of India.

The scope of enhancing reporting and investigation of inchoate cyber-crimes proves promising with the increasing partnerships of Information Technology Organizations and Academic Institutions with the State and Central Governments. Such partnerships go a long way in implementing the relevant government schemes and campaigns amidst the local communities across the country, as well as create regular awareness campaigns for civilians and law enforcement officials as required.

LIMITATIONS OF THE STUDY:

- The number of respondents is too few to make any conclusive remarks and thus, considering this as a pilot study, further research is needed in this area.
- Further research is needed to resolve challenges like if we are to criminalize a single comment also in terms of hate speech or harassment and the likes, then would that also consequentially mean that a derogatory off-hand remark made in conversations in the physical space are also to be criminalised? *Since Criminology criminalises a behaviour and not exactly the space in which the behaviour is exhibited, this research stands as only a starting point of addressing such questions within the justice framework.*

CONCLUSION

The Criminal Justice System is called a “System” for every good reason, and it is for us, justice professionals and relevant academicians alike, to make it fairly and justifiably work as such for the establishment of an increasingly safe, less fearful community. A criminological insight into criminality and victimization stands as the needed connecting thread among the various institutions ensuring justice within the social administration framework. With regards to inchoate cyber-crimes and the findings of this research, the authors conclude their findings with the following three suggestions:

1. Categorising potentially harmful criminal behaviour against persons in cyberspace as inchoate cyber-crimes within the legislative framework governing the criminalization and prosecution of cyber-crimes. Since cyber-crimes transcend national boundaries, the cyber laws of one country do not just affect the subjective feeling of safety, in terms of access to legal recourse in the event of a cyber-crime, amongst the citizens of that particular country, but it also decides to the possible legal sanctions against cyber-crimes that are reported in other national jurisdictions as well. Although for crimes in the physical space, the local culture of the land influences the law, in terms of cyber-crimes, it is the global cultural inclusivity perspectives that need to be essentially kept in mind as well.
2. It is important to take serious note of the fact that the fear of inchoate cyber-crimes has negligible effects on netizens in India, if at all. Even more alarming is the hesitation in reporting such offences to the concerned authorities, with or without adequate awareness of what unacceptable online behaviour counts as an offence. This fact stands as prominent evidence of the eminent vulnerability of the victim pool, and the consequent added responsibility of law enforcement in minimizing such online victimization.

3. Technical advancement of law enforcement is crucial to the surveillance and investigation of cyber-crimes. However, a very important piece in the puzzle would be completely overlooked if law enforcement officers are not simultaneously trained to investigate inchoate cyber-crimes as part of their preventive and predictive policing initiatives. Besides, the police are the first point of contact for the victims and that makes them an essential part of the victim assistance network too. An appreciation of this sentiment would help a great deal in preventing repeat victimizations of inchoate cyber-crimes, as well as managing such criminal tendencies before the occurrence of greater harm to the community.

Empowering law enforcement with greater clarity and specificity in the definitions of cyber-crimes and the investigative procedure to be followed for the same, so as to assure netizens of legal recourse to incidents of cyber-crimes in general, and inchoate cyber-crimes in particular, thereby helping build a subjective feeling of safety amongst the general population of Indian netizens is the need of the hour.