The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 13, Issue 3, July- September, 2025
DIP: 18.01.388.20251303, DOI: 10.25215/1303.388
https://www.ijip.in

Research Paper

Humanizing Cybersecurity: Addressing the Psychological Impact of Cybercrime

Ms. Prerana Bhaskar Mahajan[1]*, Dr. P Paul Ramesh[2]

ABSTRACT

The rise of cybercrime in recent years has created significant challenges for individuals, societies, and legal systems worldwide. It is observed that often substantial attention has been given to technological prevention and legal prosecution, the psychological and social effects of cybercrime on victims frequently remain underexplored. This article examines the intersection of technology and crime, focusing on the manipulative use of technological advancements, the psychological impact of cybercrimes, and the inadequacies of current victim support mechanisms. It proposes a victim-centric approach to the legislation. It suggests that the legislation should emphasize mental health support, international cooperation, and awareness campaigns as integral components of cybercrime management and take stringent measures in the legislation making provisions regarding victim compensation, etc. mandatory and not only 'suggested to follow' or 'recommended'.

Keywords: *Cybercrime, Cybersecurity, Psychological Impact, Victims of Cybercrime, Cyber Laws and Policies*

At the beginning of 2024, Police in the United Kingdom started investigating a case of alleged Gang-rape that happened in a metaverse while a 16-year-old girl was playing an immersive game. 59 Such a shocking and gruesome incident highlighted that the internet in every person's hand is a double-edged sword and must be handled with utmost security and precaution. The modern human world is very technology-centric and is increasingly making our lives easy and difficult at the same time. Technology is the application of scientific knowledge for practical purposes, especially in industry. As technology is everywhere from morning to evening, it was anticipated that there would be an interaction between technology and crime. Such a case would pose challenges to the criminal justice system. The creative use of technology can save lives and take lives and it can be invisible and the one handling it could be invisible too.

These technological advances and related crimes have financial, psychological, social and political effects. As the world is getting interconnected and interdependent; the effects of one incident anywhere around the globe have reactions everywhere. The offender present in any part of the globe can harm any other person who is connected via the internet, especially

[1]Forensic Professional, Central Forensic Science Laboratory, Kolkata, DFSS, MHA, Govt. of India
[2]Deputy Director, Scientist 'D', Central Forensic Science Laboratory, Kolkata, DFSS, MHA, Govt. of India
*Corresponding Author

Received: March 17, 2025; Revision Received: September 26, 2025; Accepted: September 30, 2025

in the absence of adequate security measures. These invisible offenders and offences can have a deep psychological, social, economic and political impact on the victim(s). Cybercrime has emerged as a significant challenge in the Indian scenario as well especially with increased internet connectivity and digitalisation. There is increased dependence on digital and interconnected systems for various activities in personal, business-related and even governmental activities and processes. Though the growth has supported financial gains, and ease of operations in India and globally, it has posed an increased risk of cyber threat, especially in a country like India where the diverse demography is using the internet for various activities.

The technological advances in the modern world include smartphones and smart gadgets, synthesis with advanced telecommunication technology like ATMs, self-driving cars, remote-operated electronic devices like fans, lights, 3D printing facilities, connected devices, portable devices and weapons, and the Internet of Things (IoT). Each of the devices and systems can be manipulated to have a counter-productive and even illegal and criminal use of the technology. Some of the examples are as follows-

Table 1: Examples of manipulative use of technology

Technology	**Incident Example**
Smartphones & Smart Gadgets	The 2018 Zomato data breach exposed 17 million users' details (emails, usernames, passwords) (Moudgalya,2018) 49 The 2023 Cybercrime Enterprise named Lemon Group used Pre-infected Android Budget phones to commit crimes (Laxmanan R, 2023) 43
Portable Devices & Weapons	The 2016 Delhi terror plot using smartphones to detonate explosives. (Bhalla,2016) 5 The 2016 Brussels bombings with remote-detonated explosives via smartphones, (BBC, 2016) 4 2024 Pager and Walkie-talkie Explosions in Lebanon (The Hindu Bureau, 2024)68
Electricity & Electronic Devices	The 2017 ATM skimming operation in India, (Patil 2017).54 The 2018 Uber self-driving car fatality raised ethical concerns (Sharma,2018)60 Robbers tricked ATM Machine with a Time-out Error. (Times of India, 2024)78
3D Printing	The 2017 Mumbai case used 3D printing to make firearms (Sivaram, 2017)66 Brian Thompson was murdered by using a 3D-printed Gun (NDTV World, 2024).39
Connected Devices	The 2019 TikTok controversy in India over data theft (Chakraborty, 2019)8 The 2019 Amazon Ring doorbell hack to spy on families. (Hern, 2019)36 Digital Arrest Cases (Business Standard, 2024).51
Self-Driving Cars	The 2021 Indian concerns about autonomous vehicles after the 2018 Uber accident (Chandran, 2021).9 In 2021 Tesla autopilot was targeted by hackers (Wired, 2021). 45 Self-driving car blocking Police Response to shooting. (KTVU, 2023) 42
Internet of Things (IoT)	The 2018 Mirai botnet attack in India using unsecured IoT devices (Basu,2018).3 The 2016 Mirai botnet took down Twitter and Spotify (Perlroth, 2016).

Technology	Incident Example
	55 Mirai IoT Botnet powers record 5.6 tbps DDoS Attacks (2025) 14
E-commerce	The 2017 Snapdeal scam involved fake products (Kumar, 2017),40), (Verma,2018) 87 The Dark web marketplaces use e-commerce for illegal transactions. (Koller, 2013) 40 E-commerce hacking to buy items worth 7 crore at minimal costs (India Today, 2025) 77
E-currencies (Cryptocurrencies)	The 2020 Bitcoin scam in Kochi. (Mohan, 2020).48 The Cryptocurrency funding terrorism in India in 2021(Jain, 2021).38 Use of Cryptocurrencies on the dark web for illegal activities. (Nakashima, 2018) 50 9 drug traffickers were arrested and EUR 27 million in cryptocurrencies seized (Europol, 2024) 31
Data & Cloud Devices	The 2018 Air India data breach exposed 4.5 million customers' details via cloud hacking. (Ganguly, 2018) 34 Engineering group IMI hit by Cyber Attack (Perspective Media, 2025) 56
Virtual Reality (VR)	The 2019 Indian cybercrime ring using VR for ransomware. (Singh, 2019) 65 The 2019 Baltimore ransomware attack affected VR systems (Vincent, 2020).88
Social Media	The 2019 Indian general election fake news campaign (Deshmukh, 2019). 16 The 2018 Mumbai teenager's death was linked to online harassment (Dhingra,2018). 18 Spreading fake news during religious pilgrimage (Times of India, 2025) 21
Websites & Backend Operations	The 2019 SBI data leak exposed 50 million customers' details through backend hacking. (Mishra, 2019) 47 Sensitive DeepSeek data exposed to web (Economic Times, 2025) 32
Artificial Intelligence (AI)	The 2020 AI-generated deepfake job scam in India (Sharma, 2020).61 The 2020 Deepfake TikTok incident. (Vincent, 2020) 88 The AI-powered surveillance and stalking (Dastin, 2018) 13 AI increasingly used for sextortion, scams and child abuse (The Guardian, 2024) 15 3 juveniles booked for morphing, circulating obscene photos of classmates (Hindustan Times, 2024) 17
Intelligence Augmentation (IA)	The 2020 AI-based deepfake job scam in India (Sharma, 2020). 61

It can be observed from Table 1, that Cybercrime is a global phenomenon and is challenging to manage due to the diversity of the cyber laws in different countries. United Nations Office on Drugs and Crime has a separate module and training material for cybercrimes and has served as a secretariat to the negotiations of the latest 2024 UN Convention on Cybercrime. 86. It had different measures to undertake cooperation among state parties to combat cybercrime and countermeasures for misuse of technology. However, it was observed that whenever there is any discussion about the impact of crime, the victim usually gets some attention and sympathy as the effect of the crime is visible in terms of losses and injuries, etc. When it comes to cybercrime, consequently far more discussion has happened about prevention and cyber-security than the losses of victims and the psychological impact of the same. It should be remembered that technology is for humans and not the vice versa. As the

technology is created for human ease and comfort, discomfort and losses incurred by the same should be managed effectively. If not, it defeats the purpose of the creation of technology. In the case of cybercrimes, it is important to accept that whenever there is the emergence of any phenomena in society, it impacts human minds and the changes can be unpleasant.

Psychological Impact of Cybercrimes

According to the report on Understanding Victims of Crime (2017) 20, Victims of crime experience various short- and long-term emotional and psychological effects. Victims of violence describe feelings of shock, loss of trust in society, and guilt at becoming a victim of crime, as they typically feel they could have prevented the incident from occurring. Violent crime can also cause victims to feel a sense of uncertainty and disempowerment and to feel more vulnerable, leading to high levels of worry about personal safety. Violent victimisation has also been found to be linked to the development of symptoms of fear, anxiety, depression or confusion, sadness, anger and stress. When it comes to cyber-crime victims, it is one additional factor in almost all types of cybercrime i.e. invasion of personal space, lack of adequate information and a constant fear as technology like computers, mobile phones, and ATMs are unavoidable in the modern world. The offender in cybercrime is physically invisible most of the time and the cyber-crime happens in the person's personal space may it be their own mobile phone, laptop or even debit/credit card or cryptocurrency.

Exposure to cybercrime invokes reactions and effects of different intensities depending on awareness and knowledge about the situation, demographic characteristics, socio-economic and cultural background, gender, degree of loss, etc. The emotional and psychological impact of cybercrime on victims is manifold. In the Indian scenario, the interplay of different factors can be similar to the global scenario. One of the highlighted effects of cybercrime on victims could be the feeling of learned helplessness. Norton's study revealed that victims' strongest reactions to cybercrime are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to act and a sense of helplessness. According to Hoffman, people (victims of cyber-crime) accept a situation, even if it feels bad (Hoffman S, 2010) 37.

According to research conducted by Pant, R. & Chaubey, U (2024) 53; the coping strategies adopted by the victims of cyber-crime can be positive and negative. Positive coping strategies include emotion-focused therapies like seeking support, mindfulness, physical activity, positive affirmations, and cognitive restructuring whereas problem-focused strategies include, reporting the incident, seeking legal advice, changing passwords and educating oneself. Though these strategies would be helpful, negative strategies like substance use, avoidance, denial, venting aggression, and passivity can have further detrimental effects on the victim's mental health and well-being.

Table 2: Psychological impact of cybercrime on victims- Result of various research/ studies

Cybercrime	Example of Research/ Studies
Emotional Reactions to Cybercrime	Anger, annoyance, cheating, self-blame, and helplessness (Norton, 2010) 37 Person-centred cybercrime has a greater psychological impact as compared to an intensive offender has an enhanced impact. (Ahe,2022) 1

	Higher negative impact on the emotional well-being of victims of person-centred crimes and victims for whom the offender was an acquaintance, and victims whose financial loss was not compensated and a lower negative impact on the emotional well-being for victims with a higher income. (Borwell J, Jansen J & Stol W, 2022) 6 Cybercrime's impact mostly equals or exceeds that of traditional crimes. Disparities especially emerge in terms of higher peritraumatic stress experienced by victims of cyber property crime, and more damage to self-image suffered by victims of both cyber property and cyber sexual crimes. (Borwell J, Jansen J & Stol W, 2025) 7
General Psychological Impact	Negative emotional well-being, loss of trust, PTSD, frustration, aggression, and suicidal ideation (Pant & Chaubey, 2024) 53
Cyberbullying	Sadness, depression, fear, anxiety, stress, isolation, low self-esteem, and aggression (Wan Hassan et al., 2015; Bridging Refugee Youth, 2009; Schneider et al., 2013) 35 Youth victims of cyberbullying are more likely to be engaged in delinquent behaviour (Lee C & colleagues, 2020) 44 Targets of cyberbullying are 5 to 7 times more likely to engage in digital self-harm. (Patchin J.,Hinduja S,2024) 57
Cyberstalking	Suicidal ideation, fear, anger, PTSD, paranoia, insomnia, and social withdrawal (Short et al., 2014; Acquadro et al., 2017; Nobles et al., 2014) 63 Depression, anxiety, fear, irritability, helplessness, low mood, PTSD, and social withdrawal (Drebing et al., 2014; Cripps and Stermac, 2018; Brown et al., 2017) 63
Cyberbullying	Hypersensitivity, emotional tension, anxiety, behavioural changes, isolation, sleep disturbances, attempted suicide, and substance use (IYERS, 2017; DCSF, 2009) 35
Cyber Victimization and Physical/Emotional Impact	Stomach trouble, sleep disorders, anger, fear, confusion, distress, anxiety, and depression (Acquadro et al., 2017; Nobles et al., 2014) 63
Sextortion	Significant harms, and that reporting and help-seeking remain very low due to shame, fear, and negative perceptions of police and digital platforms. (Ray A & Henry N 2025) 58
Psychological Effects of Cyber Victimization	Social withdrawal, anxiety, depression, PTSD, obsessive behaviours, self-harm, and suicidal tendencies (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012) 89
General Emotional Impact (Cybercrime)	Anger, trauma, shame, regret, sadness, distress, deception, disappointment, worry (Ghani N M et al., 2023) 35
Cyberstalking and Mental Health (Adults)	Depression, anxiety, PTSD, fear, anger, self-harm, low self-esteem, loneliness, panic, and sadness (Stevens et al., 2020) 67
Victim Impact of Being Hacked	Anxiety, depression, vulnerability, fear, loss of trust, helplessness, violation of privacy (Palassis et al., 2021) 52
Cyber-Victimization and Chronic Health Conditions	Deterioration of health, new diagnoses, psychological consequences, social isolation, discrimination in case of individuals with chronic illness (Alhaboby et al., 2023) 2
Impact of Stigma in India on Cybercrime Victims	Delayed care, impeded diagnosis, reduced opportunity for recovery, stigma, and discrimination in seeking mental health support (Shidhayea & Kermode, 2013; Gaiha et al., 2020) 62

As Table 2 shows the results of different studies on cybercrime, it is safe to say that cybercrimes seriously impact victims even if it is often called victim-less crime. Some of the

effects like Post Traumatic Stress Disorder (PTSD), Depression, Anxiety, Substance Abuse, etc need serious clinical attention and sometimes even proper medication to manage the effects. The victims may further shy away from using the technology necessary to build their lives, whether in terms of education, career, personal communication, etc. At present, the large group using advanced cyber-technology are adolescents, and young adults and thus the number of cyber-crime victims could be high in the same age group. This age group is precisely the present and future workforce of the country. If this age group becomes sceptical, fearful or is bearing the negative impact of technology due to cybercrime, it is going to affect their mental health and productivity in their personal and professional lives and while looking at the larger picture, will hamper the health of the country and world.

In recent years, social media has been used to create or destroy public image, spread misinformation and/or disinformation, create a public scare and instigate people to do illegal & anti-social activities, trolling, etc. may not directly fall into the purview of cyber laws but has devastating psychological effects on people. Trolling, Online dating scams, and shopping scams are some of the instances where decision-making about the offender becomes challenging as some behaviour is consented to by the victim, and some behaviour can't be termed as harmful and illegal along with the presence of illegal and criminal activity. Such situations are challenging to find answers to and when it comes to the psychological impact of the same, many victim and perpetrator variables like initial financial condition, personality, prior experiences etc. come into play.

Trolling can be defined as a form of negatively perceived communication which can exploit fellow netizens using websites, games or chat mechanisms online. It can take many forms-verbal, non-verbal, platform-specific or general. There were multiple instances where the more severe forms of trolling – including but not limited to repeated harassment and identity-based insults – led to consequences comparable to those of cyberbullying, including heightened anxiety, depression, and withdrawal. The most discussed trolling in media could be referred to as Toxicity i.e. the behaviours that are intentionally malicious and hurt other players. Researchers from different domains like social psychology, gaming psychology, etc are researching it and thus their emphasis and ideas do not always point out a certain direction. The qualitative research done by Cook and colleagues (2023) 10, suggests that the impact of trolling is varied depending on the platform (social media vs. gaming) and intensity (platform-specific vs. general). The same research suggests that a major factor in the participants' opinions regarding toxicity levels was content moderation practices. They were appreciative of automatic tools such as chat filters and automatic detection of profanity on voice chat but stressed that these are not a replacement for human content moderators. Therefore, it can be said that there is a need for more research about the psychological effect of trolling practices especially when they lie on the fence of being criminal activity.

The serious to severe psychological impact is seen in the cases of victims of online dating fraud and scams. According to Wang C (2022) 89 , victims of online dating scams take the emotional toll of a broken relationship. It was found that while not all victims reported psychological difficulties, some experienced relationship breakdowns, and mental health problems. As with victims of scams in general, victims of such scams may experience a loss of self-esteem, self-worth, trust, and confidence. Moreover, a minority have experienced sexual abuse via the Internet. Victims who experienced sexual encounters during or even as a part of dating scams reported similar psychological effects, such as shame, guilt, and sexual assault, as rape victims. Of course, financial victims may suffer more, with victims who lost money having significantly higher levels of an emotional impact than those who

did not. There is still a lack of research on the psychological impact of victims after suffering a scam, as well as a lack of in-depth study on the possible psychological problems of victims. In many cases, even if the victim does not suffer serious property damage, the emotional toll of a broken relationship leads to a higher level of suffering. Although many of these relationships are built online, after a long period of grooming and relationship development, the victim has developed a psychological attachment and affection for the criminals' virtual persona, which often has a severe psychological impact on the victim when the scam is uncovered.

The effects of cyber-crime on the Indian population will have another factor added i.e. stigma regarding overall mental health services. According to Shidhayea R, and Kermode M (2013) 62, stigma towards, and discrimination against, people with mental disorders is an important barrier to mental health service utilization in India. It contributes to delays in seeking care, impedes timely diagnosis and treatment for mental disorders, serves as an impediment to recovery and rehabilitation, and ultimately reduces the opportunity for fuller participation in life. According to the research conducted by Gaiha S and colleagues (2020) 33, most studies (66%) focused on youth training to become health professionals. One-third of young people display poor knowledge of mental health problems and negative attitudes towards people with mental health problems and one in five had actual/intended stigmatizing behaviour. Young people are unable to recognize the causes and symptoms of mental health problems and believe that recovery is unlikely. People with mental health problems are perceived as dangerous and irresponsible, likely due to misinformation and misunderstanding of mental health problems as being solely comprised of severe mental disorders (e.g. schizophrenia). However, psychiatric labels are not commonly used/understood. In such a scenario, the victims of crime especially that of cyber-crime would face more stigma as the crime often involves violated consent, privacy, and other invisible/ victimless crimes.

In recent years, numerous private, public, and mixed-sector organizations in India have been actively working to address cybercrime. These organizations focus on raising awareness among various sections of society, understanding and researching the complexities of cybercrime, supporting the investigation process, and enhancing the skills of investigative agencies. Some have also recognized the negative impact of cybercrimes and are working to provide support and mental health services to victims. However, challenges persist due to the vast geographical expanse of the country, its dynamic demographics, the increasing number of internet users, and the diversity in internet usage across different age groups.

Response from Criminal Justice Administrations

Globally cybercrime has been a point of attention and concern for developed as well as developing nations. Discrepancy in infrastructure in cyber-space and cyber-security are posing challenges in implementing one-fit solutions to all the countries in the world. There were many protocols and treaties were drafted but no single treaty was adopted by the majority number of countries in the United Nations. Some of the notable documents include the United Nations General Assembly (UNGA) Resolution (2000),81 (2003),82 (2019),83 (2021) 84, Global Protocol on Cyber-security and cybercrime (2009) , A Global Treaty on Cybersecurity and cybercrime (Second Edition, 2011), UNGA Convention on Cybercrime (2024) 86, United Nations Office of Drugs and Crime (UNODC) Comprehensive Study on Cybercrime (2013) 85, and Global Programme on Cybercrime training and United Nations Convention against cybercrime (2024) 86. These documents emphasized the importance of

international cooperation, capacity building, and legal framework to fight against cyber-crime.

The European Union adopted the Budapest Convention on Cybercrime (2001) 11 as the initial response to cybercrime. It was followed by rules and protocols like the Council Framework Decision on Attacks Against Information Systems (2005),23 Directive on Attack Against Information Systems (2013), 25 General Data Protection Regulation (GDPR) (2016),26 Directive on Security of Network and Information Systems (NIS Directive) (2016), and (NIS2 in 2022), 28 EU Cybersecurity Act (2019), 29. In response to the growing cybercrime around the globe, the European Union rules were adopted in January 2024, and since then the European Banking Authority (EBA) 30 has also extended its guidelines on money laundering and terrorist financing risk factors including Cybersecurity Advanced Persistent Threat and Security Program (CASPS) version 3. These developments are expected to have a positive impact on the amount of information available to Law Enforcement Agencies in cryptocurrency-related investigations, at least when suspects are located in Europe. These documents form the backbone of the EU's cybercrime and cybersecurity strategy, ensuring robust measures to tackle evolving cyber threats while enhancing international cooperation. They focus more on international cooperation, legal procedures and frameworks and global technical measures with mention of the protection of human rights and privacy in implementing the cyber laws. However, they don't provide any concrete rules, guidelines or policies to handle the mental health challenges or the psychological impact and compensation for the victims faced by victims of cybercrime in significant detail.

All the aforementioned global documents focus on cybercrime's legal, procedural and technical aspects except the Directive on Combating the Sexual Abuse and Exploitation of Children and Child Pornography (2011), 24 which included the measures to provide support to the victims of cybercrime. Therefore, it can be concluded that the major focus on global and European documents, drafts, and resolutions against cybercrime viewed cyber as a national security threat, and the human victim was ignored.

Though often criticized for limited research, unforeseen growth in users, dynamic demography, under-reporting of cases, cultural and gender-related elements at play, less awareness about impact and help provided to internet users, negligence of internet security protocols, less dynamic legislation, people's perspective about cyber-victims, stigmatised mental health issues and the whole therapy and counselling process etc., the Government of India has also taken specific steps to combat cyber-crime including amendments in existing acts and model rules. The Information Technology Act (2000), 69 is a landmark law in India designed to regulate cyber activities such as e-governance, e-commerce, and cybercrime. It is administered by the Indian Computer Emergency Response Team (CERT-In), and the Act provides the foundational legal framework for addressing cybersecurity issues and promoting data protection. It was later amended in 2008,70 through the Information Technology (Amendment) Act, which sought to address shortcomings in the original Act, particularly with the fast-evolving technological landscape. It expanded the definition of cybercrime, validated electronic signatures, and made organizations more accountable for data security breaches, encouraging them to adopt stronger data protection measures. This amendment was applied to the Indian entities and foreign organizations operating in India or are involved in business transactions with Indian entities. Additionally, it addressed emerging threats, such as phishing, by incorporating them into the purview of the Act. Over the years, Indian legislation enforced the Information Technology Rules (2011) 71 and

(2021) 72, The National Cybersecurity Policy (2013), 73 the Reserve Bank of India (RBI) Guidelines (2018) 74, The National Cyber Security Strategy (2020) 75, and the most recent being the Digital Personal Data Protection Act of 2023 (DPDP) 76. These measures are more attentive towards prevention, reporting mechanisms, cybersecurity and punishment of the offenders. Though there was an effort to create relevant legislation and alignment to international developments, the Cyber-laws in India failed to address the psychological impact of cybercrime.

At present, the Indian cyber laws primarily focus on Investigation, Prosecution and prevention of cybercrime with diminutive attention given to the psychological well-being of victims. It was observed that mental health is not a formalized component of victim support mechanisms or compensation schemes. There are helplines designed to assist in reporting cyber-crime but they are not focused on providing psychological counselling or support to the victims of cyber-crime. Few NGOs provide counselling services to cyber-crime victims, but their reach and capacity are limited and they can't fulfil the need. Therefore, it is vital to include mental health support in victim assistance programmes under schemes like the Victim Compensation Fund. There is a need for the creation of specialised helplines and centres for psychological support for victims of cybercrime. There should be awareness among citizens and capacity building among law enforcement and judicial officers to recognize and address the psychological needs of the victims of cybercrime. It is equally important to train mental health professionals in dealing with the victims of cybercrime and integrate their services into the reporting and management mechanism.

DISCUSSION AND CONCLUSION

The fast-paced technological changes can be a boon or bane. Notorious cyber-offenders are a constant threat and a great challenge to policy-makers. It is difficult for a typical user to clasp with the speed of technological changes let alone the changing pattern and magnitude of cyber-crime. The psychological impact of cybercrime is multifaceted including the victim, family, community and society at large. Many of the cybercrime victims have reported difficulties like trust issues, fear of using devices to the extreme effects such as depression and post-traumatic stress disorder, along with the presence of physical, and financial losses in the cases of extortion, online dating scams, etc. Though there was some research carried out about the Psychological impact of cybercrime on its victims; the variables like differences in the cultures of offenders and victims, their age group, gender, attitudes towards mental health and therapy, duration of recovery of the victim, impact of demography on the cybercrime victims, etc are relatively untapped areas especially in case of India.

Effective management of cybercrime can be achieved by giving adequate importance to the human element involved in cybercrimes. The impact of cybercrime can be reduced, especially in cases where the victim is directly involved, such as cyberbullying, cyberstalking, extortion, and cyber arrests. At the policy level, it is crucial to develop both international and national guidelines that emphasize counselling and psychological support for cybercrime victims, along with allocating funds for victim assistance programs, support hotlines, and mental health services. Equally important is the establishment of mechanisms for fair victim compensation. The policy should also include procedures and research aimed at creating awareness campaigns for both citizens and law enforcement officials, ensuring an empathetic approach towards cybercrime victims.

To conclude, it can be said that, there is a need for more comprehensive and informative laws about the hybrid use of technology and cybersecurity. The newly developed legislation should be mandatory and not only designed as 'advice to follow' or 'suggestions'. There is a need for constant research and development in the area of cyber-security and the effects of cyber-crimes. Another important factor to focus on while dealing with cybercrime is its impact on humans- as individuals, as families and groups and society as a whole. In the era of increasing mental health concerns, these measures would be especially necessary. Therefore, along with creating a safe cyber-space, it is equally important to focus on research and finding solutions to deal with the Psychological impact of Cyber-crimes.

REFERENCES

Ahe L (2022), Mental well-being and Cybercrime: The Psychological Impact of cybercrimes on victims, retrieved from: http://essay.utwente.nl/91014/

Alhaboby Z, Evans H, Barnes J, Short E (2023), The Impact of Cybervictimization on the Self-Management of Chronic Conditions: Lived Experiences, Journal of Medical Internet Research 2023, vol. 25, e40227 doi: 10.2196/40227

Basu, K. (2018). The rise of IoT botnets in India: A wake-up call. TechCrunch. Retrieved from https://techcrunch.com/2018/03/20/india-iot-botnet

BBC. (2016). Brussels attacks: How did the bombers carry out their attacks? BBC News. Retrieved from https://www.bbc.com/news/world-europe-35869293

Bhalla, A. (2016). How smartphones are being used in terror attacks. The Hindustan Times. Retrieved from https://www.hindustantimes.com/india-news/smartphones-used-in-terror-attacks/story-hasdfmnsdf

Borwell, J., Jansen, J., & Stol, W. (2022). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. Social Science Computer Review, 40(4), 933-954. https://doi.org/10.1177/0894439320983828

Borwell, J., Jansen, J., & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. International Review of Victimology, 31(1), 156-181. https://doi.org/10.1177/02697580241282782

Chakraborty, R. (2019). The TikTok controversy: Privacy concerns and implications for India. The Economic Times. Retrieved from https://economictimes.indiatimes.com/technology/tiktok-privacy-controversy

Chandran, S. (2021). India's autonomous vehicle regulations: Navigating ethical challenges. The Times of India. Retrieved from https://timesofindia.indiatimes.com/technology/auto/autonomous-vehicle-regulation

Cook CL, Tang SY-C and Lin J-HT (2023) Comparing shades of darkness: trolling victims' experiences on social media vs. online gaming. Front. Psychol. Retrieved from 14: 1163244. doi: 10.3389/fpsyg.2023.1163244

Council of Europe (2001) Budapest Convention on Cybercrime, https://rm.coe.int/16800815 61

Das, S., & Nayak, T. (2023). Impact of cyber-crime: Issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142-153. ISSN 2231-6604.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-idUSKCN 1MK08G.

Daws R (2025), Mirai IoT Botnet Powers record 5.6 tbps DDoS Attacks, IoT News, 22nd January, 2025 https://iottechnews.com/news/mirai-iot-botnet-powers-record-ddos-attack/

Dearden L (2024), AI increasingly used for sextortion, scams and child abuse, says senior UK Police Chief, 24 November, 2024, The Guardian, https://www.theguardian.com/technology/2024/nov/24/ai-increasingly-used-for-sextortion-scams-and-child-abuse-says-senior-uk-police-chief

Deshmukh, P. (2019). Fake news in Indian elections: The role of social media. The Hindu. https://www.thehindu.com/news/national/fake-news-indian-elections.

Deshpande S (2024), Three Juveniles Booked for Morphing, Circulating Obscene Photos of Classmates, August 17, 2024, Hindustan Times,

Dhingra, S. (2018). The tragic case of cyberbullying in Mumbai: Lessons for social media platforms. NDTV. https://www.ndtv.com/india-news/cyberbullying-mumbai

Digest of Cyber Organized Crime. (2022). United Nations. https://www.unodc.org/documents/organizedcrime/tools_and_publications/Digest_of_Cyber_Organized_Crime_2nd_edition_English.pdf

Diniman T, Moroz A (2017), Understanding Victims of Crime: The Impact of the Crime and Support Needs, published by: http://www.victimsupport.org.uk/

Dixit K (2025), FIR against 7 for spreading fake news about Mahakumbh, February 3, 2025, Times of India, https://timesofindia.indiatimes.com/city/lucknow/fir-against-7-for-spreading-fake-news-about-maha-kumbh/articleshow/117867587.cms

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

European Union. (2005). Council Framework Decision on Attacks Against Information Systems. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF

European Union, Directive on Combating the Sexual Abuse and Exploitation of Children and Child Pornography (2011), Retrieved from https://eur-lex.europa.eu/eli/dir/2011/93/oj/eng

European Union. (2013). Directive on Attacks Against Information Systems. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF

European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Union. (2016). Directive on Security of Network and Information Systems (NIS Directive). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

European Union. (2022). NIS2 Directive. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

European Union. (2019). EU Cybersecurity Act. Retrieved from [URL]

European Banking Authority. (2024). Guidelines on money laundering and terrorist financing risk factors, including CASPS version 3. Retrieved from https://www.eba.europa.eu/sites/default/files/2024-01/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf

Europol (2024), 9 drug traffickers arrested and EUR27 million in cryptocurrencies seized, 18 December 2024, Europol, https://www.europol.europa.eu/media-press/newsroom/news/9-drug-traffickers-arrested-and-eur-27-million-in-cryptocurrencies-seized

Etech (2025), Sensitive DeepSeek data exposed to web: cyber firm Wiz report, January 30, 2025, Economic Times, https://economictimes.indiatimes.com/tech/artificial-intelligence/sensitive-deepseek-data-exposed-to-web-cyber-firm-wiz-report/articleshow/117716267.cms

Gaiha, S., Salisbury, T., Koschorke, M., Raman, U., & Petticrew, M. (2020). Stigma associated with mental health problems among young people in India: A systematic review of magnitude, manifestations and recommendations. BMC Psychiatry, 20, 10.1186/s12888-020-02937-x.

Ganguly, S. (2018). Air India data breach: Hackers expose customer details. India Today. Retrieved from https://www.indiatoday.in/technology/news/story/air-india-data-breach

Ghani, N. M., & colleagues. (2023). Cybercrime experience's impact on women's emotions: A case study in Penang. Malaysian Journal of Tropical Geography, 49(2), 48-67, retrieved from https://mjes.um.edu.my/index.php/MJTG/article/view/48910

Hern, A. (2019). Hackers use Amazon's Ring doorbell to spy on families. The Guardian. Retrieved from https://www.theguardian.com/technology/2019/dec/10/hackers-amazon-ring-doorbell

Hoffman S (2010), Norton study: 65 per cent of internet users are cybercrime victims, Retrieved from https://www.crn.com/news/security/227300377/norton-study-65-percent-of-internet-users-are-cybercrime-victims

Jain, R. (2021). Cryptocurrency and its role in terrorism financing in India. Business Standard. Retrieved from https://www.business-standard.com/article/news-ians/cryptocurrency-and-terrorism

Jonko A (2024), Luigi Mangione Case Exposes Danger of 3D Printed Firearms, December 20, 2024, NDTV World, https://www.ndtv.com/world-news/3d-printed-guns-like-the-one-used-by-luigi-mangione-are-a-growing-threat-7296866.

Koller, D. (2013). The Silk Road: Inside the dark web's online drug marketplace. Rolling Stone. Retrieved from https://www.rollingstone.com/culture/culture-news/the-silk-road-186711/

Kumar, S. (2017). The rise of counterfeit products in India's e-commerce market. The Financial Express. Retrieved from https://www.financialexpress.com

KTVU staff (2023), Self-driving car blocks Police responding to San Francisco shooting, June 11, 2023, https://www.ktvu.com/news/self-driving-car-blocks-police-responding-to-san-francisco-shooting

Laxmanan R (2023), This Cybercrime Syndicate pre-infected over 8.9 Million Android Phones Worldwide, The Hacker News; https://thehackernews.com/2023/05/this-cybercrime-syndicate-pre-infected.html

Lee C, Ptchin J W, Hinduja S, Dischinger A (2020), Bullying and Delinquency: Impact of Anger and Frustration, Violence and Victims, Volume 35, Number 4, 2020 retrieved from https://www.researchgate.net/profile/Sameer-Hinduja/publication/340366756_Bullying_and_Delinquency_The_Impact_of_Anger_and_Frustration/links/61d301ddb6b5667157c591ea/Bullying-and-Delinquency-The-Impact-of-Anger-and-Frustration.pdf

Marshal A (2021) A fatal Crash Renews Concerns over Tesla's 'Autopilot' Claims, April 20, 2021, Wired, https://www.wired.com/story/fatal-crash-renews-concerns-teslas-autopilot/

Miralis, N. G., & Miralis, D. (2023). AI-enabled future crime: Study reveals 20 disturbing possibilities. Lexology. Retrieved from https://www.lexology.com/library/detail.aspx?g=93ff642e-0026-4f99-ba79-0fae4114ded5

Mishra, R. (2019). The SBI data breach: What happened and how it affects customers. NDTV. Retrieved from https://www.ndtv.com

Mohan, M. (2020). Bitcoin scam in Kochi: Cryptocurrency as a tool for money laundering. The Indian Express. Retrieved from https://indianexpress.com

Moudgalya, S. (2018). Zomato data breach: What went wrong? TechCrunch. Retrieved from https://techcrunch.com

Nakashima, E. (2018). Cryptocurrency helps fuel illicit trade in the dark web. The Washington Post. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/01/31/cryptocurrency-helps-fuel-illicit-trade-in-the-dark-web/

Nimje S N (2024), You are under digital arrest: all about Rs. 4 Crore fraud in Mumbai, November 26, 2024, Business Standard, https://www.business-standard.com/technology/tech-news/you-are-under-digital-arrest-all-about-rs-4-crore-fraud-in-mumbai-nc-124112600896_1.html

Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. SAGE Open, 1-12. Retrieved from https://doi.org/10.1177/21582440211061556

Pant, R. & Chaubey, U. (2024). Protecting Minds in the Digital Age: A Review Based Study on Psychological Impact of Cybercrime. International Journal of Indian Psychology, 12(3), 2240-2247. DIP:18.01.220.20241203, DOI:10.25215/1203.220

Patil, A. (2017). ATM skimming operations in India: A growing concern. Business Today. Retrieved from https://www.businesstoday.in

Perlroth, N. (2016). Hackers hijack 100,000 webcams and routers to launch cyberattacks. The New York Times. Retrieved from https://www.nytimes.com/2016/10/22/technology/hackers-cyberattack-iot.html

Perspective Media (2025), Engineering Group IMI Latest UK firm to be hit by cyber-attack, 6 February, 2025, Perspective Media, https://www.perspectivemedia.com/engineering-group-imi-latest-uk-firm-to-be-hit-by-cyber-attack/

Patchin J W & Hinduja S (03 May 2024): Adolescent Digital Self-Harm Over Time: Prevalence and Perspectives, Journal of School Violence, DOI: 10.1080/15388220.2024.2349566

Ray A & Henry N (2025), Sextortion: a Scoping review; Trauma, Violence, & Abuse 2025, vol. 26(1) 138 –155, retrieved from https://journals.sagepub.com/doi/epub/10.1177/15248380241277271

Sales, N. J. (2024). A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future? The Guardian, 5 January 2024. Retrieved from https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta

Sharma, N. (2018). The ethics of autonomous vehicles in India: A case study. The Economic Times. Retrieved from https://economictimes.indiatimes.com

Sharma, P. (2020). The rise of AI-powered frauds in India. The Financial Express. Retrieved from https://www.financialexpress.com

Shidhayea, R., & Kermode, M. (2013). Stigma and discrimination as a barrier to mental health service utilization in India. International Health, 5(6), 6-8. Retrieved from https://doi.org/10.1093/inthealth/ihs011

Singh, M., & Sharma, P. (2021). Cyberstalking: A major threat to adolescent well-being. Edu World, X(3), 263-269. ISSN 2319-7129.

Singh P P (2024), Cybercrime in Metaverse, International Journal of Science and Research (IJSR), Volume 13 Issue 2, February 2024 ISSN: 2319-7064 SJIF (2022): 7.942, DOI: https://dx.doi.org/10.21275/MR24130195237

Singh, S. (2019). How cybercriminals use virtual reality for ransomware attacks. The Times of India. Retrieved from https://timesofindia.indiatimes.com

Sivaram, A. (2017). 3D printing and its misuse for illegal weapon production in India. The Hindu Business Line. Retrieved from https://www.thehindubusinessline.com

Stevens, F., Nurse, J. R. C., & Arief, B. (2020). Cyberstalking, cyber harassment and adult mental health: A systematic review. Cyberpsychology, Behaviour, and Social Networking, 23(5), 300-308. https://doi.org/10.1089/cyber.2020.0001

The Hindu Bureau (2024), Lebanon Explosion Heighlights:14 Killed, over 450 Injured, as Devices Explodes Across Lebanon on second consecutive day, September 19, 2024; https://www.thehindu.com/news/international/another-wave-of-explosions-in-beirut-lebanon-in-hezbollah-strongholds-on-september-18-2024/article68656966.ece

The Information Technology Act (2000), (No. 21 OF 2000)

The Information Technology (Amendment) Act, (2008) (No.10 of 2009)

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021.

The National Cybersecurity Policy (2013)

The Reserve Bank of India (RBI) Guidelines (2018)

The National Cyber Security Strategy (2020),

The Digital Personal Data Protection Act of 2023 (DPDP).

Tiwari A (2025), 3 Caught for hacking E-commerce site, buying items worth 7-crores for 'pennies', January 31, 2025, India Today, https://www.indiatoday.in/india/story/hacking-e-commerce-sites-buying-expensive-items-for-few-rupees-men-arrested-in-ahmedabad-

TOI Tech Desk, (2024), How robbers tricked SBI ATM machine with 'Time-out' error to steal money, November 25,2024, https://timesofindia.indiatimes.com/technology/tech-news/how-robbers-tricked-sbi-atm-machine-with-time-out-error-to-steal-money/articleshow/115578241.cms

Tucker, A. (2018). ATM skimming and fraud prevention: How the crime works. PCMag. https://www.pcmag.com/news/atm-skimming-and-fraud-prevention

United Nations (2020), Report of the Secretary General-Roadmap for Digital Co-operation, https://www.un.org/en/content/digital-cooperation-roadmap/

United Nations General Assembly. (2000). Resolution on cybercrime. Retrieved from https://documents.un.org/access.nsf/get?OpenAgent&DS=A/AC.291/L.15&Lang=E

United Nations General Assembly. (2003). Resolution on international cooperation to combat cybercrime. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

United Nations General Assembly. (2019). Resolution on global cybersecurity cooperation. Retrieved from https://documents.un.org/access.nsf/get?OpenAgent&DS=JIU/REP/2021/3&Lang=E

United Nations General Assembly. (2021). Resolution on combating cybercrime globally. Retrieved from https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

United Nations. (2024). Global Programme on Cybercrime training and United Nations Convention against cybercrime. Retrieved from https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf

Verma, N. (2018). The dark web and illegal e-commerce in India. India Today. Retrieved from https://indiatoday.in

Vincent, J. (2020). Deepfake pornography and the future of consent. The Verge. Retrieved from https://www.theverge.com/2020/1/16/21068785/deepfake-pornography-regulation-legal-rights

Wang C (2022), Online dating scam victims Psychological impact analysis, Journal of Education, Humanities and Social Sciences, Volume 4, 2022 Retrieved from https://www.researchgate.net/publication/366662441_Online_Dating_Scam_Victims_Psychological_Impact_Analysis

Zengler, T. (2021). The Pegasus spyware scandal: What we know so far. TechCrunch.Retrieved from https://techcrunch.com/2021/07/20/the-pegasus-spyware-scandal/

Acknowledgment

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Mahajan, P.B. & Ramesh, P.P. (2025). Humanizing Cybersecurity: Addressing the Psychological Impact of Cybercrime. *International Journal of Indian Psychology*, *13*(3)*,* 4248-4262. DIP:18.01.388.20251303, DOI:10.25215/1303.388