The International Journal of
INDIAN PSYCHOLOGY

Review Paper

Protecting Minds in the Digital Age: A Review Based Study on Psychological Impact of Cybercrime

Prof. Rashmi Pant[1], Uma Chaubey[2]*

ABSTRACT

The world is undergoing a technological upheaval in the current times. This rapid advancement and widespread digital integration are leading to an increase in cybercrime by creating new vulnerabilities and opportunities for exploitation. The complexity of modern technology often outpaces security measures, leaving gaps that malicious actors can exploit resulting in increased cyber related crimes. Given the current scenario, there is a chance that this risk will increase over the next few decades disrupting people's psychological and emotional wellbeing. The purpose of the present study is to firstly, identify the prevalence of cybercrime and how does it psychologically impact its victims and secondly, understand various coping strategies that can be used to combat this digital threat. To achieve the objectives of the current study, a number of relevant research articles and books were studied with the help of electronic search engines like, Google Scholar, Springer & Academia which gave insight into the definitions and nature of cybercrime including its major risk factors and psychological impact on victims. The findings of the review point an arrow towards a negative impact of cybercrime on emotional wellbeing. Loss of trust, Post Traumatic Stress Disorder (PTSD), increased frustration and aggression and suicidal ideation were found common among victims of cybercrime. Victims can deal with this worldwide threat by adopting a variety of preventative steps, such as strengthening cyber security, ongoing education, and by using effective problem-solving coping techniques.

A few years ago, it was opined that, if a third world war broke out, it would be fought using technology rather than force. This viewpoint demonstrates how technology has entrenched itself in the fabrication of human life. We're so used to using technology that now we can't separate ourselves from using it. Take, for example, our phones. Humans are glued to their phones just as moths are glued to light. Approximately 62.5% of the world's population or 4.95 billion individuals have access to the internet. This figure is anticipated to rise to 5.3 billion by 2023 (Ahe, 2022). By 2025 the number of mobile devices used globally is estimated to be around 18.22 billion (Sarkar et al., 2023). This shows that people have engaged themselves with gadgets which lead to broad and extended use of technology (Herrerías et al., 2023). This often results in the use of

---

[1]Department of Psychology, I.P. Govt. Girls P.G. College, Haldwani, Uttarakhand, India
[2]Department of Psychology, I.P. Govt. Girls P.G. College, Haldwani, Uttarakhand, India
*Corresponding Author

technology recklessly and leads to several cyber-related crimes. Cybercrime in all its manifestations has grown in frequency and menace. It is impossible to overestimate the effect that cybercrime has on our well-being as we navigate this digital environment.
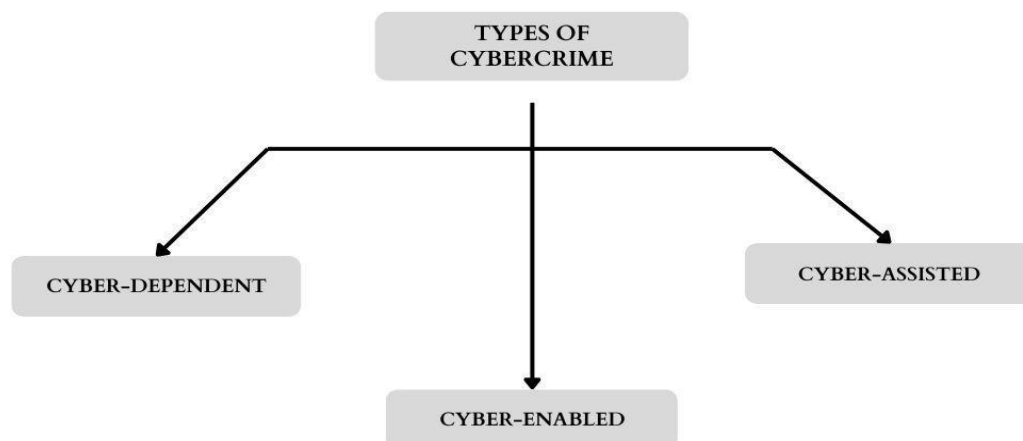
Introduction

There is a broad spectrum of illicit behaviours utilizing technology that are included in cybercrime. Cybercrime can be broad or specific, encompassing both crimes aimed at individuals and crimes aimed at businesses, organizations, and institutions. (Ahe, 2022). These crimes have repercussions that go beyond monetary losses; they can have a significant negative impact on a person's mental and emotional health. Being the victim of an online crime can lead to serious psychological problems for the victim, such as suicidal thoughts, lack of trust, and Post traumatic stress disorder (PTSD), (Ahe, 2022). Furthermore, the stability and security of finances can be greatly impacted by cybercrime. Phishing, identity theft, and other fraudulent internet operations may cause significant financial losses for people and companies. One's general well-being may be impacted by financial pressure these crimes entail, which can also generate stress, sadness, and a sense of powerlessness. Cybercrime, according to Warren Buffet, poses real risks to humanity and is the number one problem with mankind. (Mahesh et. al., 2022)

This review is aimed at providing different perspectives related to the definition of cybercrime, and majorly focuses on the psychology behind cybercrime and its impact on psychological wellbeing of the victims. This paper attempts to spread awareness regarding cybercrime so that valid policies and laws can be enforced for mitigating cybercrime as it is seen that law enforcement has particular difficulties in cyberspace, due to the inherent anonymity of the cyberspace, the malleability of identities, and the inadequacy of national and international legislation to combat cybercrime (Smith, 2013). The crime report evidence landscape shows a substantial discrepancy between the number of cybercrimes that are reported and the percentage of those that result in successful convictions. (Sarkar and Shukla, 2023). This discrepancy shows that proper laws need to be formulated to not let cyber related crimes consume us either, psychologically, financially or socially.

Firstly, for the present review, an extensive search was conducted on the search engines like, Google, Google scholar, ResearchGate and Academia by using key words such as, cybercrime, online harassment, psychological impact, cyberbullying, relevant articles and research papers were identified and useful information were extracted. These databases were selected due to their broad coverage of peer-reviewed research in the social sciences, psychology, and multidisciplinary fields. To guarantee a thorough examination of both historical and modern research, the search was not restricted to any one period of time. Papers were examined from 2004 to 2023 so that the most recent advances and insights could be captured. The method of qualitative synthesis was used to evaluate the retrieved data. Each study's major conclusions were compiled and arranged according to recurring themes and patterns. The application of a thematic analysis made it possible to pinpoint recurrent psychological effects and investigate variations among different categories of cybercrime and victim populations.

The most common definition of cybercrime is the offence done using a computer (Phillips et al., 2022). Researchers have classified cybercrimes into three main types. Cyber-enabled crimes are defined as illicit activities that are made easier or substantially better by the use of computers, the internet, or digital technology.

CLASSIFICATION OF CYBERCRIME

```
                    ┌─────────────────┐
                    │   TYPES OF      │
                    │   CYBERCRIME    │
                    └─────────────────┘
        ┌───────────────────┼───────────────────┐
        ▼                   ▼                   ▼
┌────────────────┐  ┌────────────────┐  ┌────────────────┐
│ CYBER-DEPENDENT│  │ CYBER-ENABLED  │  │ CYBER-ASSISTED │
└────────────────┘  └────────────────┘  └────────────────┘
```

Source: Author's own

These crimes take advantage of technology's ability to carry out conventional crimes or develop brand-new illegal behaviours such as phishing, online fraud, cyberbullying. Cyber-dependent crimes that are exclusive to the use of computers, networks, or other digital technologies are known as cyber-dependent crimes. These crimes would not be feasible without the use of technology, and they notably depend on the existence and operation of cyberspace. The hallmark of cyber-dependent crimes is their unwavering reliance on electronic technology and the internet to carry out their operations such as malware attacks, data intrusion, hacking, ransomware assaults. Wall added one more classification on the list i.e., cyber-assisted crime. Also known as technology-facilitated crimes, these are acts where typical criminal actions are carried out with the assistance of digital technologies or the internet. These offences include the use of technology as a means of organising, carrying out, or disguising illegal activity. Cyber-assisted crimes can incorporate both online and offline components, in contrast to cyber-dependent crimes, which can only happen in a digital setting such as online blackmail. These are some of the many ways used by researchers to classify cybercrime into different categories. These categorizations are significant but there is still a need to establish a clear cut connection between theory and practical application so that these classifications are found useful to support future research endeavours. The nature of cybercrime is constantly evolving with the advancement in technology hence the usefulness of any methodology should lie in its ability. Andrew and Bonta gave a total of eight psychological factors that were responsible for criminal conduct. The factors were divided into, The big four and the moderate four. The "big four," or most significant risk variables for criminal behaviour, were determined to be "antisocial associates," "antisocial personality pattern," "antisocial cognition," and "history of antisocial behaviour." The moderate four factors were "family/marital circumstances," "substance abuse," "leisure/recreation," "school/work,".
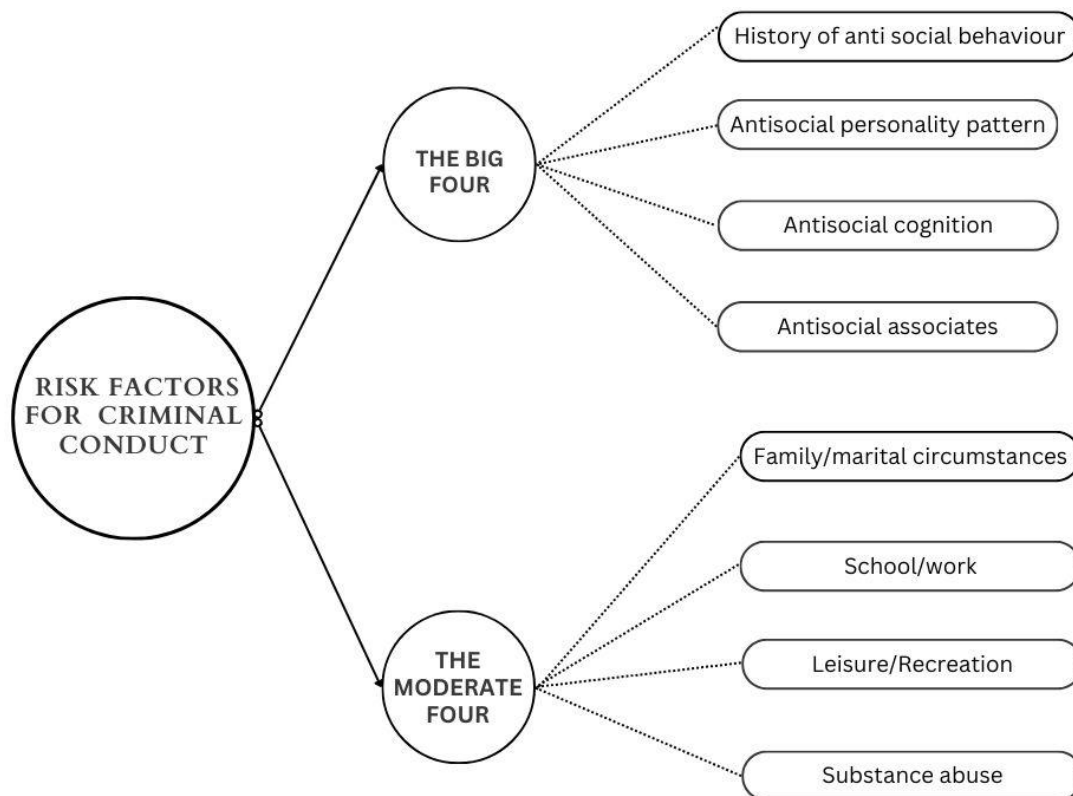
Source: Author's own

Antisocial behaviour is characterized by a general hatred towards people and society in general. People high in antisocial behaviour commit heinous crimes without any guilt or remorse. The characteristics of people with antisocial personality patterns include chronic patterns of deceitfulness, impulsivity, anger, aggression, lack of regret after hurting others, and a persistent inability to follow social standards. People with these personality patterns are frequently linked to various risk-taking behaviors. Individuals may also show a lack of reduced empathy which explains clearly why people engage in cyber stalking or trolling online. Numerous ideas explain why elements in this risk category are relevant. Low arousal theory or sensation seeking theory explains why having antisocial personality patterns might be relevant in engaging in cybercrime. Differential association theory elucidates how antisocial associates or having friends or acquaintances that are involved in criminal activities leads to acquiring criminal behaviour. Not only are criminal tactics acquired in groups, but also the motivations and justifications for illegal actions (Wissink et al., 2023). Antisocial cognitions are values, beliefs, and a personal identity that is conducive. History of antisocial behaviour includes previous engagement in antisocial activities (Andrews and Bonta, 2010).

Literature suggests that, in most cases, the impact of cybercrime on victims is either financial or psychological (Borwell et al., 2021). The psychological impact of cyber-crime is plenty hence, investigating the complicated impacts of cybercrime on victims is crucial as we negotiate the complexity of the virtual world. The implications go beyond the digital sphere into the complex domains of human emotions, from the breakdown of trust to the appearance of dread and worry. According to psychologist Ronnie Janoff-Bulman's Shattered Assumptions Theory, trauma, especially victimization experiences, can disrupt core beliefs people have about the world and themselves. The Shattered Assumptions Theory aids in the explanation of the psychological effects of cybercrime by disrupting

victims' fundamental assumptions regarding control, safety, and it's possible that victims of cybercrime believed their online activity and personal information were secure. When a cyber-attack undermines these presumptions, people might feel less comfortable using digital platforms resulting in loss of trust. The belief in one's own innocence or invulnerability may clash with the remorse felt after becoming a victim of cybercrime.

Victims of person-centered cybercrime, those whose acquaintances are the offenders, and those who do not receive financial loss compensation are more likely to experience a negative emotional impact from cybercrime. (Borewell et al., 2021) In addition to potential long-term financial and psychological repercussions, mental illness may make a victim of cybercrime more susceptible to it. (Monteith et al., 2021). Anxiety may increase in those who become victims of identity theft or online privacy violations. It might be upsetting to worry about money loss, reputational damage, or the abuse of personal information. Cyberstalking has detrimental impacts on many facets of life, including the psychological, social, interpersonal, and financial spheres. It also causes comorbid anxiety and depression. (Worsley et al.,2017) Lack of social support in these situations exacerbates victims' distress; some victims report feeling betrayed and blamed by friends and family. An ongoing sense of annoyance might be brought on by worries about potential cyber threats and the safety of one's online activity or personal data. The sense of helplessness in the face of hackers might intensify this persistent worry. Victims of cyberbullying may have psychological effects including frustration, despair, or even thoughts of suicide. (Frensh et al., 2018.)

The ramifications of cybercrime, including but not limited to identity theft, cyberbullying, online harassment, and financial loss, can significantly affect a person's psychological state and overall well being. These traumatic events can occasionally exacerbate depressive, dismal, and despairing moods, which can then spark suicidal thoughts, despair, helplessness and hopelessness. Increased anxiety, rage, despair, Post Traumatic Stress Disorder symptoms, such as vivid flashbacks of the traumatic event, Intrusive thoughts and experiencing intense distress at symbolic reminders of the trauma are common. Emotional trauma may be experienced by those who have suffered serious privacy violations, such as having private or sensitive information revealed in a data breach. One factor that might lead to anxiety is the dread of possible repercussions, including identity theft. People close to victims of cybercrime are at a significant risk of becoming secondary victims and most of them show symptoms of PTSD. (Wiederhold et al., 2014).

To escape from the trauma, the victims of cybercrime use negative coping techniques such as passivity, alcohol use and avoidance which aggravates their psychological well being. The frequency of cyber stalking is higher in women, and young adult victims are more likely to experience anxiety and despair as a result of using negative coping mechanisms including passivity and avoidance (Begotti et al., 2020). To counter this, healthy coping strategies such as, problem focused coping and emotion focused coping strategies should be used. Educating oneself about the nature of cybercrime, being aware of the various cybercrime frauds managing one's negative emotions by seeking counseling and help, cognitive restructuring of victims and their closed ones, reporting the incident and raising voice and spreading awareness about cyber related crimes are some of the positive coping strategies. While many people and businesses incur enormous losses as a result of cybercrime, which has a major negative influence on both psychological health and wealth, it may be avoided by strengthening network security (Siahaan et al., 2018). The dynamic nature of cyberspace calls for a user awareness training where users are made aware of the emerging threats and new cyber security techniques. Enhancing cyber security by continuously educating oneself

about the best practices, updating all of the apps, operating system, and antivirus software, educating people on the value of preserving sensitive data, comprehending data categorization, and abiding by rules and guidelines while managing data and using a mix of organizational, technological, and personal safeguards to reduce risks and improve cyber security as a whole, is part of fighting cybercrime.
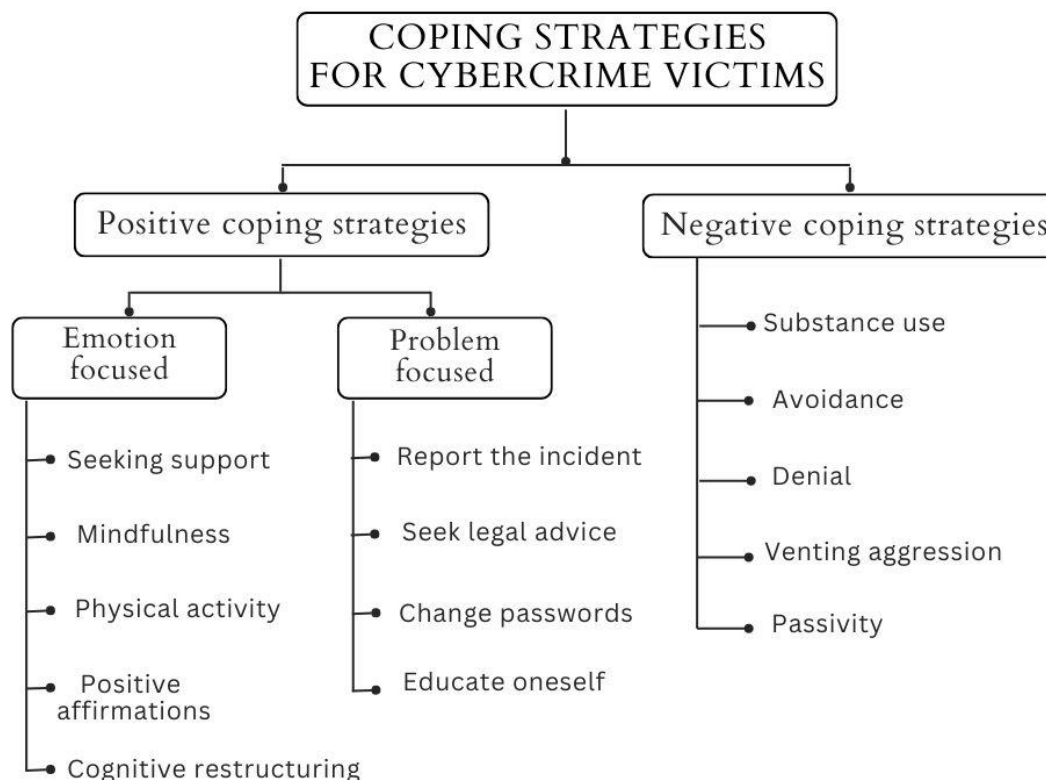
Source: Author's own

DISCUSSION

This study sought to analyze the body of research on the psychological effects of cybercrime in order to offer insight on how these harmful behaviors affect people in general and vulnerable populations in particular. According to our review, victims of cybercrime frequently experience trauma, stress, worry, and despair as a result of the crime's severe psychological effects. Victims of cyber bullying often experience suicidal thoughts, social disengagement, and low self-esteem. In a similar vein, those who become victims of financial fraud or identity theft frequently express elevated tension, anxiety, and a constant feeling of vulnerability. The study emphasizes how crucial social networks and coping strategies are for lessening the psychological effects of cybercrime. The negative consequences on mental health can be considerably lessened by using effective coping mechanisms include reaching out for social support, taking part in stress-relieving activities, and using mental health services. Our findings underscore the need for robust policies and interventions to address the psychological impact of cybercrime. Collaboration between various stakeholders, including law enforcement agencies, mental health professionals, and technology companies, is essential to create a safer digital environment. Although this review offers insightful information about the psychological effects of cybercrime, more research is necessary to delve deeper into some areas. It would be advantageous to conduct longitudinal research looking at the long-term psychological repercussions of various forms of cybercrime. Furthermore, studies examining the efficacy of different coping mechanisms and support networks might help guide the creation of focused therapies. A multimodal

strategy including mental health support, preventive measures, and strong legislative frameworks is needed to address this issue. Through improving digital literacy, raising awareness, and encouraging cooperation among interested parties, we can lessen the psychological effects of cybercrime and build a more secure and encouraging online community for everybody.

CONCLUSION

Cybercrime's psychological effect is a serious and complex problem that needs to be carefully considered by academics, decision-makers, and society at large. Numerous emotional and psychological consequences, such as stress, worry, sadness, trauma, and loss of trust, can affect victims of cybercrime. These effects may have a significant negative influence on people's relationships, sense of security, and general well-being in both online and offline settings. Research can help build focused treatments and victim-centered support services by shedding light on the psychological effects of cybercrime. It can also serve as a roadmap for the creation of laws and regulations meant to combat cybercrime and foster cyber resilience. Future research should focus on the various strategies that we can use to combat cybercrime. Also, more studies should focus on the psychological impact of different types of cybercrimes. Victims must be made aware of healthy coping mechanisms that they should use. A comprehensive and cooperative strategy that incorporates technology solutions, education, legislative frameworks, and personal accountability is crucial in the face of ever-changing cyber threats. We can all work together to create a safer digital environment, lessening the effects of cybercrime and preserving the resilience of our globalized society, by adopting these principles and exercising caution.

REFERENCES

Ahe, L. (2022). Mental Wellbeing and Cybercrime (The Psychological Impact of Cybercrime on the Victim) (Bachelor's thesis, University of Twente).

Altheide, D. L., & Schneider, C. J. (2012). Qualitative media analysis (Vol. 38). Sage publications.

Andrews, D. A., & Bonta, J. (2010). The psychology of criminal conduct. Routledge. Begotti, T., Bollo, M., & Maran, D. (2020). Coping Strategies and Anxiety and Depressive Symptoms in Young Adult Victims of Cyberstalking: A Questionnaire Survey in an Italian Sample. Future Internet, 12, 136.

Borwell, J., Jansen, J., & Stol, W. (2021). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. Social Science Computer Review.

Frensh, W., & Mulyadi, M. (2018). Criminal policy on cyberbullying toward children.

Goldsmith, A., & Wall, D. S. (2022). The seductions of cybercrime: Adolescence and the thrills of digital transgression. European Journal of Criminology.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice.

Janoff-Bulman, R., & Yopyk, D. J. (2004). Handbook of Experimental Existential Psychology. Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports.

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. International Review of Victimology.

Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sci. 2022.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology.

Short, E., Linford, S., Wheatcroft, J., & Maple, C. (2014). The impact of cyberstalking: the lived experience - a thematic analysis. Studies in health technology and informatics.

Siahaan, A. (2018). Impact of Cybercrime on Technological and Financial Developments.

Smith, T. (2021). A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime.

Wiederhold, B. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyber psychology, behavior and social networking.

Wissink, I. B., Standaert, J. C., Stams, G. J. J., Asscher, J. J., & Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. Aggression and Violent Behavior.

Worsley, J., Wheatcroft, J., Short, E., & Corcoran, R. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses.