INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 5 [2025] | Page 203 – 266

THE PSYCHOLOGY OF CYBER CRIME IN INDIA: A DOCTRINAL STUDY ON THE MOTIVATION AND BEHAVIOUR OF CYBER CRIMINAL

-Sunita Khan

ABSTRACT

The researcher in this doctrinal study explores the psychology of cybercriminals focusing on their motivation and behaviors. Cybercrime has become an increasingly pervasive issue in the digital age, with a growing number of individuals falling prey to various forms of online criminal activities. Understanding the psychological drivers behind cyber-criminal behaviour is crucial for developing effective prevention and intervention strategies. This study highlights the key factors influencing cybercriminal behaviour and the psychological traits. The researcher also investigate how cybercriminal motivations and behaviours are shaped by their socio-economic environments, technological advancement and law enforcement efforts. In conclusion the researcher provides insights into complex nature of cybercriminal psychology understanding the need for the comprehensive approach to addressing cyber criminals. The researcher gave some recommendation suggestion and security measures which helps in law reform and cybercrime investigation and developing deter in the mind of cyber criminals.

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND OF THE STUDY

In an increasingly globalized world, cybercrime has emerged as one of the biggest challenges facing the world, affecting people, businesses, and governments. From identity theft and data breaches to online fraud and cyberbullying, the scope of cybercrimes continues to widen in magnitude and complexity. While considerable scholarly and legal focus has been placed on the technical and legal aspects of cybercrime, the psychological foundations that drive people to engage in such activities have so far remained fairly under research in law field. However, cybercrime do not happen in a vacuum; they are usually the outcome of multifaceted psychological, social, and environmental factors, such as anonymity, felt impunity, cognitive distortions, thrill-seeking, and even psychopathology.

This study attempts to close the gap between cyber law and criminal psychology through doctrinal legal analysis augmented by psychological theory. It aims to examine how thinking, personality, motivations, and behavioural tendencies make their respective contributions to the perpetration of cybercrimes like hacking, cyber stalking, online deception, and digital harassment. In analysing the psychological motivations for cybercrimes, this research hopes to strengthen the comprehension of legal systems, guide preventive measures, and aid more successful enforcement and rehabilitative policies. In many cases, perpetrators may be motivated by a desire for control, recognition, revenge, thrill-seeking, ideological commitment, or financial gain. Others may suffer from personality disorders, exhibit anti-social tendencies, or be influenced by peer dynamics in online communities. Ultimately, the incorporation of psychological insights into legal discourse may not only advance the interpretation and application of cyber legislation but also reflect a more balanced approach to justice in the era of cyberspace.

1.2 RATIONALE AND IMPORTANCE OF THE STUDY

The researcher could focus on understanding the psychological drivers, such as age, power, revenge, thrill seeking behind cybercrime and explore how motivations differ

across types of cybercrimes such as hacking, fraud, ransomware etc. Finding common behavioural patterns of cyber criminals and investigate ole of personality traits in cyber-criminal behaviour to improve prevention and intervention strategies.

The main importance of the study is:

- By understanding cybercriminal motivations and behaviour, better prevention must be taken.
- The study could gave a better understanding of criminal behaviour common in cyber criminals which may help in law reforms.
- The main findings of the study guide policymakers in creating effective laws and regulations to deter cybercrime.

1.3 RESEARCH OBJECTIVES

The primary objective of this research is:-

1. To identify the psychological motivations and factors that drive individuals to engage in cybercrime.
2. Analyse the role of psychological factors in the perpetration of cybercrime.
3. To find the impact of cybercrime on victims and society.
4. To propose preventive strategies and policy recommendations based on a psychological understanding of cybercrime.

1.4 RESEARCH QUESTIONS

The researcher in this study gave answers to some of the research questions:

1. What are the primary psychological motivations behind individuals' involvement in cybercrime?
2. What are the common behavioural traits and profiles of cybercriminals in India?
3. How do psychological disorders or mental health conditions relate to cybercriminal activity?

4. What psychological effects (e.g., anxiety, depression, PTSD) do cybercrimes have on individual victims?

1.5 METHODOLOGY AND SOURCES OF DATA

The study adopts a Doctrinal research methodology, primarily relying on Library based analysis of legal and psychological literature, Statutes, case laws and commentaries. It is an analytical and theoretical study, aimed at understanding the psychological motivation behind cybercrime and its legal and social impact.

The sources of data on which the research is relying on are:

- Statutory provisions, especially the Information Technology Act, 2000 and its amendments.
- Judicial decisions from Indian courts pertaining to cybercrime.
- Scholarly articles, books, reports, and journals in criminology, psychology, and cyber law.
- Case studies and empirical findings from previous research conducted in India and globally.
- The study uses a qualitative, analytical method to interpret psychological theories in the context of legal texts and real-world cases.

1.6 SCOPE AND LIMITATIONS

The scope of this research paper will able to give the deep and productive knowledge regarding the Psychological motivation and behaviour of cyber criminals and the common traits and profiles of cyber criminals in India.

LIMITATIONS

The Limitations on the research of psychological motivation and behaviour are:

- Cybercrimes committed within or having a significant connection to India.
- The psychological and behavioural aspects of offenders rather than victims.

- Legal responses to cybercrime as applicable in India, with limited comparative references.

CHAPTER 2: CONCEPTUAL AND THEORETICAL FRAMEWORK

2.1 DEFINITION AND MEANING OF CYBER CRIME

Cybercrime is a broad and generic term that refers to crimes committed using computers and the Internet, and can generally be defined as a subcategory of computer crime. If this sounds strange, consider that whether someone commits Internet fraud or mail fraud, both forms of deception fall under a larger category of fraud. The difference between the two is the mechanism that was used to victimize people. Cybercrime refers to criminal offences committed using the Internet or another computer network as a component of the crime. Computers and networks can be involved in crimes in several different ways:

- The computer or network can be the tool of the crime (used to commit the crime).
- The computer or network can be the target of the crime (the "victim")
- The computer or network can be used for incidental purposes related to the Crime (for example, to keep records of illegal drug sales)

Although it is useful to provide a general definition to be used in discussion, criminal offences consists of specific acts or omissions, together with a specified culpable mental state. To be enforceable, laws must also be specific. These definition should be as narrow as possible, but legislators don't always do a good job of defining term (and sometimes don't define them at all, leaving it up to law enforcement agencies to guess, until the courts ultimately make a decision).[1] (Shinder & cross, 2008.)

[1] Shinder, D. L., & cross, M. (n.d.). Scene of the cybercrime (2nd ed.). Elsevier.

2.2 CATEGORIES AND TYPES OF CYBER CRIMES

The term Cybercrime has its broader aspect in the wold of Technology. Cybercrime encompasses a broad spectrum of illicit activities where computers or computer networks play a pivotal role as instruments, targets, or venues for criminal endeavours. This term covers a wide range of offenses, from hacking and cyber invasions to distributed denial-of-service (DoS) attacks and other malicious exploits. Additionally, it includes traditional crimes that leverage computers or networks to facilitate illegal actions, effectively merging the physical and digital realms of criminal activity.

CATEGORIES OF CYBER CRIMES

There are a lot of Cyber Crime categories; these categories include different terminology and iconography that create controversy over the computer attacker terms.

1. DATA CRIME: Data Interception, Data Modification, and Data Theft are called Data Crime. An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. Data Theft used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this

information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

2. NETWORK CRIME: Unauthorized Access and Virus Dissemination are called Network Crime. "Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality. Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Osman 4 Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

3. RELATED CRIME: Aiding and Abetting Cyber Crimes, Computer-Related Forgery and Fraud and Content-Related Crimes are called Related Crime. There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. Computer forgery and computer-related fraud constitute computer-related offenses. Cyber-sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries.[2] (Goni, 2021)

TYPES OF CYBER CRIMES

There are different types of Cyber Crime. 1. Hacking, 2. Virus dissemination, 3. Logic bombs, 4. Denial-of-Service attack, 5. Phishing, 6. Email bombing and spamming, 7. Cyber Terrorism, 8. Cyber stalking, 9. Data diddling, 10. Identity Theft and Credit Card Fraud, 11. Salami slicing attack, 12. Software Piracy, 13. Cyber Terrorism,, 14. Sale of

[2] Goni, O. (2021). Cyber Crime and Its Classification. International Journal of Electronics Engineering and Applications, 10(2), 01–17.

illegal articles, 15. Pharming 16.TOR Network 17. Unauthorized Access. 18. Computer Vandalism. 19. Cyber Defamation 20. Online Gambling 21. Intellectual Property crime. Now we discuss some of the types of Cybercrime:

1. Hacking: Hacking refers to the unauthorized access to a computer system or account, compromising computer resources without the owner's express or implied permission. This act involves intentionally causing wrongful loss or damage to the public or individuals by destroying, deleting, or altering information in a computer system, diminishing its value or utility, or affecting it injuriously. Hacking encompasses various forms of cybercrime, including damage to computer systems, email hacking, tampering with computer source documents, unauthorized access or data breaches, and website defacement. These malicious activities can have significant consequences, including data loss, financial damage, and compromised security. In a famous case Sony India Private Ltd. V. Harmeet Singh &Anr.(2005)[3], the accused hacked into Sony's online music portal and offered pirated music for download, causing financial damage to the company. The case was filed under the Information Technology Act, 2000, and the Indian Penal Code. It was one of the first cases dealing specifically with intellectual property theft through hacking in India.
2. Virus dissemination: Computer sabotage involves unauthorized access to computer systems, where malicious programs such as viruses, worms, or logic bombs are introduced to disrupt normal functioning. This form of cybercrime includes unauthorized modification, suppression, or erasure of computer data or functions, causing harm to the system. Malicious code, designed to cause damage or steal information, comes in various forms, including viruses, worms, and Trojan programs. Viruses replicate and spread to other systems, worms self-replicate without user interaction, and Trojan programs disguise themselves to allow unauthorized access. These malicious activities can lead to significant harm, including data loss, system disruption, and compromised security.

[3] Sony India Private Ltd. V. Harmeet Singh & Anr.,119 DLT 565 (2005)

3. Logic bombs: A logic bomb is a type of malicious code embedded in software that remains dormant until specific conditions are met. When triggered, a logic bomb virus executes a destructive action, such as deleting files or disrupting critical systems. Unlike traditional malware, a logic bomb does not propagate actively but rather lies in wait for its pre-defined activation event.
4. Denial-of-Service attack: A Denial of Service (DoS) attack aims to overload a website or network, degrading its performance or making it inaccessible. A successful attack can result in partial or complete system unavailability, consuming time and resources to analyse, defend, and recover. A Distributed Denial of Service (DDoS) attack is a more potent form of DoS, originating from multiple sources. DDoS attacks generate more traffic and are harder to distinguish from legitimate traffic due to their distributed nature, making them more challenging to defend against. This can lead to significant disruptions and economic losses for the targeted organization.
5. Cyber Terrorism: Cyber terrorism involves using computers and networks to spread information or incite fear, anxiety, and violence. Like traditional terrorism, its impacts can be severe. Through internet technologies and social media, cyber terrorism can disseminate propaganda, undermine credibility, facilitate sabotage, manipulate public opinion, disrupt law and order, damage infrastructure, and even lead to loss of life. Its effects can be far-reaching, making it a significant concern for individuals, organizations, and governments worldwide. By leveraging digital platforms, cyber terrorists can amplify their reach and amplify the fear and disruption they seek to create.[4] (Ibrahim et al., n.d.)
6. Cyber Pornography: Child Pornography is a field of cybercrime, which entails recorded videos or images of minor children is spreading through large network medium. It made an evil impact on the minors and make there self-provocative to indulge in crime. It destroys a minor's life inn a heinous manner.

[4] Ibrahim, S., Nnamani, D. I., & Okosun, O. (n.d.). Types of Cybercrime and Approaches to Detection.

7. Phishing: Phishing is a type of cyber-attack where attackers create fake webpages or messages to deceive users into revealing personal information. This attack combines social engineering and technical methods to trick users into divulging sensitive data. Phishing is often carried out through email spoofing or instant messaging, targeting individuals who are unaware of social engineering tactics and internet security best practices. These attacks can compromise personal accounts, including social media, email, and financial accounts, highlighting the importance of understanding phishing tactics and taking measures to protect online privacy and security.[5] (Gupta, S., Singhal, A., & Kapoor, A., 2016)
8. Cyber Defamation: Cyber defamation, or online defamation, occurs when false or derogatory statements are made about someone on the internet or through digital communication channels like social media, emails, or instant messaging. It involves spreading false information that harms an individual's or organization's reputation. Online, defamation can manifest as false accusations, malicious gossip, or untrue statements shared on social media or other platforms. This can be done intentionally or unintentionally and can affect both individuals and organizations, highlighting the importance of being mindful of online content.[6] (Khan, Shaikh,& Singh, 2023).

2.3 PSYCHOLOGICAL PERSPECTIVES ON CRIME AND CRIMINAL BEHAVIOUR

Crime is a social phenomenon with ethical, legal and psychological parameters. So multitudinous criminogenic causes are attributed to the incidence of crime. Criminal behaviour, therefore is behaviour which violates a criminal code. This legal definition encompasses a great variety of acts which may range from homicide to a traffic violation. According to Sutherland and Cressey (1968) “criminal behaviour is behaviour in violation of the criminal law. No matter what the degree of immorality, reprehensibility

[5] Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE

[6] Khan, N., Shaikh, A., & Singh, M. V. P. (2023). Understanding of cyber defamation and its impact: a critical analysis. Dogo Rangsang Res J, 13, 168-173

or indecency of an act, it is not considered a crime unless it is prohibited by criminal law. Behaviour to be called ‘Criminal’ there must be harm, conduct, mens rea (crime intent) and prescribed punishment.”

Psychological theories of crime and criminality examine how mental processes of individuals, personality, and developmental history lead to illegal behaviour. Psychological theories offer explanations for how cognition, emotion, and environment interact in forming criminal behaviour. Here are the principal psychological explanations:

PSYCHODYNAMIC THEORY

Based on Freudian psychoanalysis, this theory asserts that unconscious conflicts during early childhood determine behaviour. The psyche is made up of three structures:

Id: Basic wants (e.g., aggression, immediate pleasure).

Ego: Intermediates between id and world, reconciling wants with social norms.

Superego: Conscience; weak superego may not repress criminal impulses.

Early trauma, neglect, or insecure attachment may cause bottled-up feelings (e.g., anger, fear) to be expressed as criminal activity in adult life. For instance, Bowlby's attachment theory attributes early maternal separation to antisocial behaviour. People who've experienced trauma, abuse, or neglect in their childhood might struggle with unresolved conflicts that can resurface later in life, potentially leading to criminal behaviour. Unaddressed emotions like frustration or anger can manifest in violent or illegal actions. This perspective suggests that early life experiences play a significant role in shaping behaviour and decision-making.

BEHAVIOURAL THEORY

Behavioural theory focuses on how environmental influences and learned experiences shape human behaviour. Proposed by psychologists such as John B. Watson and B.F.

Skinner, this theory argues that all behaviour, including criminal behaviour, is learned through interactions with the environment. People develop certain behaviours because they are reinforced or rewarded, while behaviours that result in punishment are typically avoided. This perspective highlights learned behaviour through interactions with the environment:

Operant conditioning: Criminal behaviour is rewarded (e.g., money, social standing) or deterred by punishment.

Observational learning: Imitating criminal behaviour observed in family, peers, or media.

Behavioural treatments, including cognitive-behavioural therapy (CBT) in corrections, seek to exchange criminal responses for prosaically ones using reinforcement techniques.

COGNITIVE THEORY

Cognitive theory focuses on how individuals perceive, process, and interpret their social environment. This theory is primarily concerned with cognitive distortions—erroneous thought patterns that lead to maladaptive behaviours, including criminal acts. Cognitive theorists argue that individuals commit crimes because of faulty thinking processes, such as justifying their actions or minimising the harm they cause to others. Highlights distorted thinking styles and decision-making processes:

Moral reasoning deficits: Inability to judge actions through an ethical lens (e.g., Kohlberg's stages of moral development).

Cognitive distortions: Justifying crime via irrational beliefs (e.g., "I deserve this").

Executive dysfunction: Poor impulse control and planning, linked to prefrontal cortex abnormalities.

These deficits may stem from inadequate social conditioning or neuro developmental issues.[7](Murthy, 2022)

PERSONALITY TRAITS

Certain traits increase criminal propensity:

Eysenck's biosocial theory: High neuroticism (instability of emotions) and extraversion (sensation-seeking) are associated with poor conditioning to norms of society.

Psychopathy: High on callousness, manipulativeness, and low on empathy.

Impulsivity: Acting without forethought, usually associated with low self-control.

LEARNING AND RATIONAL CHOICE

Social learning theory: Acquired through imitation and reinforcement in social groups.

Rational choice theory: Reasoned cost-benefit calculation, whereby crime is selected if perceived rewards exceed risks.

MENTAL HEALTH AND DEVELOPMENTAL INFLUENCES

Most mentally ill persons are not criminals, but certain mental disorders such as antisocial personality disorder and conduct disorder correlate with aggression and rule-violation. Childhood adversity (e.g., abuse, neglect) interferes with emotional control and makes one more susceptible to criminality.

Psychological explanations for crime emphasize the contribution of unresolved trauma, maladaptive learning, cognitive distortions, and personality predispositions. Nevertheless, criminal behaviour is complex with genetic, social, and environmental influences. Treatments such as CBT, anger management, and early childhood

[7] Murthy, A. N. (2022). Psychological Theories and Criminal Bhaviour. Symbiosis Law School, Hydrabadh,

intervention strive to treat these psychological underpinnings, albeit their effectiveness differs.[8] (Ivins, W. M., 1911)

2.4 THEORIES OF CYBER CRIME

Computer crime, also known as cybercrime, refers to criminal activities that are conducted through the use of computers or other digital technologies. Criminologists have developed a number of theoretical domains to explain why individuals engage in computer crime, including:

1. Rational Choice Theory – This theory suggests that individuals engage in computer crime because they believe it is a profitable and low-risk activity. In other words, they weigh the potential benefits of committing a crime against the potential risks of getting caught and punished. According to this theory, cybercriminals are assumed to be rational actors who make informed decisions based on their goals and available information. The theory is attributed by several eminent criminologists like Cesare Beccaria, Jeremy Bentham, and Gary Becker.

2. Social Learning Theory – Albert Bandura is the main exponent of Social Learning theory. This theory argues that individuals learn to engage in computer crime through observing the behaviours of others, particularly those who are close to them. They may also be influenced by media portrayals of hackers as glamorous and successful. Individual learn motivations and justifications for their actions through social interactions and observations. American Sociologist Edwin Sutherland applied social learning theory to the study of crime and deviance.

3. Strain Theory – This theory posits that individuals engage in computer crime when they experience strain or pressure in their lives, such as economic hardship or social exclusion, lack of Opportunities. Computer crime may provide a way for them to

[8] Varshney, M., Kumar, A., Ganguli, R., Umer, S., Sonkar, S. S., & Molla, N. (2023). Ethical Hacking: Enhancing Cybersecurity Through Offensive Security Practices. 44(4)

alleviate their stress or gain a sense of power and control. American Sociologist Robert K. Merton in his theory of Anomie, outline the principles of Strain Theory.

4. Routine Activities Theory – Two American criminologists, Lawrence Cohen and Marcus Felson are known for their famous work of Routine Activity theory. This theory suggests that computer crime occurs when there is a convergence of three factors: a motivated offender, a suitable target (such as a vulnerable computer system), and the absence of capable guardians (such as effective cyber security measures).Rational Activities Theory posits that cybercriminals take advantage of opportunities that arises from the routine activities of individuals and organizations.

5. Self-Control Theory – This theory proposes that individuals who engage in computer crime have low levels of self-control, which makes them more likely to act impulsively and make decisions without considering the consequences.

Overall, these criminological theories help us understand the various motives, opportunities, and situational factors that contribute to computer crime. By better understanding the underlying causes of this type of criminal behaviour, public and private sectors can develop more effective strategies for preventing and responding to cybercrime.[9] (Sultana, 2024)

[9] Sultana, Arifa (2024).A short note on Theories of Cyber Crime.(Ibrahim et al., n.d.)

CHAPTER 3: PSYCHOLOGICAL MOTIVATIONS OF CYBER CRIMINALS

3.1 INDIVIDUAL MOTIVATIONS: PERSONAL GAIN, REVENGE, POWER, AND THRILL

1. Personal Gain: Cybercrimes are driven by various motivations. Financial gain is a primary driver, with malware and other tools used to access sensitive information, such as bank account details. Some individuals engage in cybercrime as a form of protest or to cause damage, often through hacking and website defacement. Additionally, research suggests that more unorthodox motivations exist, including satisfying intellectual curiosity or challenge, general maliciousness, revenge, establishing respect and power online, and even boredom. By examining the function of programs and tools used, it's possible to infer the motivations behind these crimes. Understanding these motivations is crucial for developing effective strategies to prevent and combat cybercrime.[10] (Cyber Crime: A Review of the Evidence Chapter 1: Cyber-Dependent Crimes, n.d.)

2. Revenge: Revenge is an avenging motivation, usually triggered when a person feels they have been harmed. psychologically, the motivation for revenge is associated with a just world belief and wanting to restore justice or convey pain to the person who has hurt them. revenge behaviour may give a short-term feeling of satisfaction or fairness, but the sensation often does not last long, sometimes creating a cycle of repeated revenge behaviours. Evolutionarily, revenge might have helped deter future injury by signalling consequences for wrongdoing. The desire for revenge often arises after setbacks, rejection, or perceived injustice. For some, this emotion fuels self-improvement—such as working harder after a breakup or professional disappointment, not just to "get even," but to prove detractors wrong and boost self-esteem. When harnessed positively, revenge can drive individuals to greater achievements and personal growth, transforming negative feelings into a catalyst for success.

[10] Cybercrime: A review of the evidence Chapter 1: Cyber-dependent crimes. (n.d.)

3. Power: The power need entails a desire to control, influence, or have power over others or situations. power motivation can be expressed as gaining new power, sustaining existing power, or restoring lost power. This motivation is typically associated with feelings of competence and autonomy—essential elements of self-determination theory—enhancing motivation when people feel responsible and competent in their behaviour. Power-seeking may, in some instances, become more pronounced if initial behaviours fail to meet the latent need.

4. Thrill: Thrill-seeking, or seeking excitement and arousal, is an intrinsic type of motivation in which the activity is the reward. Thrill-seeking people tend to pursue new, risky, or extreme experiences for the emotional rush they offer. It may involve activities that are chaotic or seek attention, like igniting fire or performing dangerous acts, just for the thrill or attention. Thrill-seekers would gradually increase their behaviours as past experiences have less stimulating effect.[11] (smith, 2023)

3.2 SOCIAL AND CULTURAL FACTORS INFLUENCING CYBER CRIME

The prevalence of cybercrime is significantly influenced by various social and economic factors. Individuals from disadvantaged socioeconomic backgrounds, facing financial hardships, or lacking opportunities may be more inclined to engage in cybercrime as a means of financial gain or as a response to their circumstances. Additionally, social factors such as peer pressure, cultural norms, and community influences can also play a crucial role in shaping an individual's likelihood of participating in cybercrime. Understanding these underlying factors is essential to developing effective strategies for prevention, intervention, and mitigation of cybercrime.

[11] Smith, C. D. (2023). "The Thrill of It": An Examination of Environmental and Individual Antecedents of Thrilling Perceptions of Criminal Behaviour. UNIVERSITY OF CALIFORNIA.

SOCIAL FACTOR INFLUENCING CYBER CRIME

1. Family Environment and Upbringing: Family upbringing and community influences play a significant role in shaping an individual's likelihood of engaging in cybercrime. When families fail to instil strong moral values or prioritize financial gain over ethics, it can create an environment where cybercrime is more likely to flourish. The normalization of internet fraud within families and communities can further entrench these behaviours, as individuals may receive support or encouragement from those around them.
2. Moreover, a lack of guidance and supervision can leave individuals vulnerable to cybercrime influences, while socioeconomic factors such as poverty and financial stress can drive people to seek illicit means of financial gain. To combat the rise of cybercrime, it's essential to promote strong moral values, provide education and guidance on safe internet practices, and foster a supportive environment that rejects cybercrime. By addressing these underlying issues and working together, we can help prevent cybercrime and create a safer online environment. (Nmeme & Obiakor, 2024)
3. Economic Status and Unemployment: High rates of poverty and unemployment serve as strong motivators for individuals to turn to cybercrime as a means of livelihood. Economic hardship often outweighs individual characteristics, making financial need a primary driver behind cybercrime involvement. When people face significant financial difficulties, they may become more desperate and willing to take risks, including engaging in illicit online activities. The promise of financial gain can be particularly enticing in environments where legitimate opportunities for economic advancement are scarce. As a result, addressing the socioeconomic root causes of cybercrime, such as poverty and unemployment, is crucial for developing effective prevention and intervention strategies that can help reduce the prevalence of cybercrime and promote a safer online environment. [12](Fereshteh Momeni, 2024)

[12] Fereshteh Momeni. (2024). The impact of social, cultural, and individual factors on cybercrime. Educational Administration: Theory and Practice, 30(5), 10152–10159.

4. Peer Influence*:* Peer groups play a significant role, especially among youth, in encouraging cybercrime. The desire for social acceptance or pressure from friends can lead individuals to engage in illegal online activities. When peers glorify or normalize cybercrime, it can create a sense of FOMO (fear of missing out) or pressure to conform, making it more likely for individuals to participate. This influence can be particularly strong in social circles where cybercrime is seen as a viable or exciting option. As a result, peer groups can become a gateway to cybercrime, highlighting the importance of promoting positive online behaviours and providing alternatives to cybercrime involvement.[13] (Oyenuga, n.d.)

CULTURAL FACTOR INFLUENCING CYBER CRIME

1. Cultural Attitude toward Crime*:* Cultural context plays a significant role in shaping how cybercrime is defined, perceived, and justified. In some cultures, certain cybercrimes may be viewed as acts of honour or resistance, rather than criminal behaviour. For instance, software piracy might be more accepted in cultures that prioritize sharing and communal access to resources. Additionally, some hackers may perceive their actions as beneficial to society, adopting a "Robin Hood" mentality where they see themselves as redistributing wealth or exposing corporate or government wrongdoing. This cultural relativism highlights the complexity of addressing cybercrime globally, as what is considered illegal in one culture might be justified or even celebrated in another.[14] (Holden et al., 2015)
2. Ethical Attitudes and Social Attitudes*:* Ethical attitudes within a culture can significantly influence the prevalence of cybercrime, often outweighing the impact of economic development. In some societies, cybercrime has become institutionalized and normalized, with community and family support playing a

[13] Oyenuga, A. (n.d.). "LUCRATIVE AND HIDDEN": FACTORS INFLUENCING CYBERCRIME INVOLVEMENT AMONG YOUTH IN METROPOLITAN LAGOS.

[14] Holden, N., Michailova, S., & Tietze, S. (2015). The Routledge Companion to Cross-Cultural Management (1st ed.). Routledge.

crucial role in reducing the stigma associated with such acts. This cultural acceptance can manifest in various forms, such as software piracy being viewed as a minor infraction or online fraud being justified as a means to achieve financial gain. As a result, addressing cybercrime requires a deep understanding of the cultural context and ethical attitudes that shape individual behaviour, highlighting the need for targeted awareness and education initiatives to promote a culture of cyber security and ethical online conduct. [15](Fereshteh Momeni, 2024)

3. Legal and Social Definition: The definition and enforcement of cybercrime exhibit significant cultural variability worldwide. What constitutes a crime in one country may be perfectly legal or even socially acceptable in another, reflecting diverse cultural norms and values. For instance, online pornography laws differ drastically across countries, with some nations imposing strict regulations while others are more permissive. Furthermore, socio-political and cognitive factors shape how cybercrimes are policed, influencing law enforcement priorities and strategies. This cross-cultural disparity underscores the complexity of addressing cybercrime globally, necessitating international cooperation and a nuanced understanding of local contexts to effectively combat cybercrime.[16] (Holden et al., 2015)

3.3 ECONOMIC AND PSYCHOLOGICAL STRESS AS A DRIVER OF CYBER CRIME

The interplay between economic and psychological stress and cybercrime is a growing concern globally, including in India. Financial hardship and emotional vulnerabilities create an environment conducive to cybercriminal activity. During economic downturns, individuals facing financial strain may turn to cybercrime as a means of survival or to supplement lost earnings, while organizations experience a rise in insider threats. The expansion of digital platforms in India has created more opportunities for financially motivated cybercrime, especially for those seeking quick financial fixes.

---

[15] Fereshteh Momeni. (2024). The impact of social, cultural, and individual factors on cybercrime. Educational Administration: Theory and Practice, 30(5), 10152–10159.

[16] Holden, N., Michailova, S., & Tietze, S. (2015). The Routledge Companion to Cross-Cultural Management (1st ed.). Routledge.

ECONOMIC STRESS AND CYBERCRIME

- Economic downturns and financial crises, such as inflation and the rising cost of living, have been directly linked to increases in cybercrime. During periods of economic hardship, individuals facing job insecurity or reduced income may turn to cybercrime as a means of financial survival or to supplement lost earnings.
- Organizations have observed a rise in insider threats during economic downturns. Employees, pressured by financial needs, may engage in activities like data theft, embezzlement, or facilitating external attacks for monetary gain. In critical sectors, up to 35% of decision-makers reported an increase in internal cybercrime linked to economic strain.
- The expansion of digital platforms and e-commerce in India, while beneficial, has also created more opportunities for financially motivated cybercrime, especially as more people seek quick financial fixes in times of stress. [17](The Economics of Civil Justice, 2013)

PSYCHOLOGICAL STRESS AND CYBERCRIME

- Psychological triggers such as fear, anxiety, low self-esteem, loneliness, and the desire for quick solutions can make individuals more susceptible to engaging in, or falling victim to, cybercrime.

- Emotional manipulation by cybercriminals often exploits these vulnerabilities. Techniques such as social engineering prey on trust, urgency, and emotional distress, leading individuals to participate in illegal online activities or become unwitting accomplices.
- Social pressure and conformity, particularly among youth or peer groups, can also drive individuals toward cybercrime, especially when combined with economic desperation or a lack of digital literacy.

---

[17] The Economics of Civil Justice: New Cross-country Data and Empirics (OECD Economics Department Working Papers). (2013). Organisation for Economic Co-Operation and Development (OECD).

- In regions with limited access to digital education, such as rural areas of Uttar Pradesh, low digital literacy exacerbates psychological vulnerabilities, making individuals easier targets for cybercriminals.[18] (Raj & Singh, 2024)

3.4 ROLE OF ANONYMITY AND LACK OF PHYSICAL PRESENCE IN CYBER CRIME

Anonymity and the Lack of Physical Presence in Cyberspace playing as Enablers of Cybercrime. The nature of cyberspace—defined by anonymity and the absence of physical proximity—significantly enhances the capabilities of cybercriminals while complicating law enforcement efforts. These features enable perpetrators to evade detection, frustrate jurisdictional enforcement, and cause enduring harm to victims. The roles of these factors are:

I. ROLE OF ANONYMITY IN CYBERCRIME

1. Facilitating Harmful Behaviour

Anonymity removes the immediate risk of social or legal repercussions, allowing perpetrators to act with impunity. Through fake profiles, pseudonyms, or encrypted communication tools, offenders engage in a range of harmful activities including cyberbullying, online harassment, hate speech, and sexual exploitation.

- Example*:* The Australian eSafety Commission reports that a majority of image-based abuse complaints involve anonymous social media accounts. Similarly, child sexual abuse material (CSAM) is often distributed via anonymised platforms, making intervention and prevention difficult.

[18] Raj, S., & Singh, D. V. (2024). Exploring Psychological Triggers and Vulnerabilities Leading to Digital Arrests in Cybercrime Cases: A Comparative Study in Uttar Pradesh. 14(4).

- Anonymity also facilitates social engineering schemes such as cat fishing, impersonation, and grooming, where perpetrators create false identities to manipulate or exploit victims.

2. Evading Accountability

Technological tools like VPNs, Tor browsers, and end-to-end encrypted messaging apps obscure the origin and identity of users. These tools hinder forensic investigations by masking IP addresses and encrypting communications.

- According to a report by INDONET, cybercriminals routinely exploit these technologies to avoid detection and reoffend by simply creating new anonymous accounts after suspension or exposure. [19](GeorgeF. du Pont, 2001)

3. Challenges for Victims and Regulators

The persistence of anonymous abuse leads to psychological trauma among victims, who fear re-victimization without a clear avenue for redress.

- For digital platforms, enforcing terms of service becomes difficult without verifiable identities, and legal systems struggle with jurisdictional limitations, especially when crimes span multiple countries. [20](Armstrong & Forde, 2003)

II. ROLE OF LACK OF PHYSICAL PRESENCE IN CYBERCRIME

1. Cross-Border Jurisdictional Conflicts

Cybercrime frequently crosses international borders, creating legal ambiguities. A perpetrator in one jurisdiction may commit crimes against individuals or institutions in another, complicating the prosecution process.

---

[19] GeorgeF. du Pont. (2001). Criminalization of True Anonymity in Cyberspace, The. Michigan Telecommunications and Technology Law Review, 7(1).

[20] Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. Information Management & Computer Security, 11(5), 209–215.

- Example*:* A hacker in Country A breaching servers located in Country B raises questions about which nation's legal standards should apply. Although international instruments like the Budapest Convention on Cybercrime aim to harmonize enforcement, inconsistent implementation hampers effectiveness.

2. Difficulty in Evidence Collection

The intangible nature of digital crime scenes poses substantial challenges. Law enforcement must rely heavily on digital evidence—IP addresses, metadata, and server logs—which are often encrypted or routed through multiple countries.

- The lack of standard global protocols for chain-of-custody and digital forensics further undermines investigatory reliability.

3. Exploiting Legal Loopholes

Cybercriminals often base operations in jurisdictions with lax cybercrime laws or limited law enforcement capacity.

- Example: Tanzania's Cybercrimes Act of 2015 grants expansive investigatory powers to police without requiring judicial oversight, raising concerns about misuse while simultaneously failing to deter cybercrime due to weak enforcement mechanisms .[21](Murphey, 2024)

Anonymity and the absence of physical presence fundamentally shift the risk calculus for cybercriminals. These factors embolden harmful behaviour, hinder legal accountability, and expose gaps in national and international regulatory frameworks. Addressing these challenges requires to:

- Improved cross-border legal harmonization,
- Stronger digital identity verification systems,

[21] Murphey, C. (2024). Understanding cybercrime. European Parliamentary Research Service.

- Enhanced international cooperation for evidence gathering and prosecution.

3.5 CASE STUDIES ON CYBER CRIMINAL MOTIVATION IN INDIA

India’s rapidly expanding digital ecosystem has led to a surge in cybercrime, with motivations ranging from financial gain to political activism. The following case studies and statistical insights illustrate the diverse motives driving cybercriminal activity in the country.

1. Pune Citibank MphasiS Call Center Fraud
some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cybercrime cases that raised concerns of many kinds including the role of "Data Protection". The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".
ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000. Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2. SONY SAMBANDH.COM Case
India saw its first cybercrime conviction in 2013. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint about online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated, and Arif Azim was arrested. Investigations revealed that Arif Azim while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the colour television and the cordless headphone, in this one of a kind cyber fraud case. In this matter, the CBI had evidence to prove their case, and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cybercrimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort

sends out a clear message to all that the law cannot be taken for a ride. [22](Sarmah et al., n.d.)

3. The Bank NSP Case

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

4. Parliament Attack Case

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.[23] (Parewa & Mordia, n.d.)

5. Andhra Pradesh Tax Case

[22] Sarmah, A., Sarmah, R., & Baruah, A. J. (n.d.). A brief study on Cyber Crime and Cyber Law's of India. 04(06).

[23] Parewa, D. K., & Mordia, D. D. (n.d.). Trends and Patterns: Analysing Cybercrime Statistics in India

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.[24] (Tiwari et al., 2023)

By analysing the above most important case laws we can say cybercrime in India sis driven by complex issues of motivations, including financial gain, emotional or personal grievances, ideological causes and psychological factors. Organized cybercrime groups often prioritize financial motives, whereas individual attackers may be driven by personal vendettas or emotional triggers. Hacktivists, on the other side, are motivated by ideological beliefs, using cyber-attacks as a means to promote their aims. Psychological factors like curiosity, thrill-seeking, revenge mentality or unemployment factor play crucial role in occurring cybercrime, influencing others to engage in malicious activities.

As a nation of taking prevention, India has been evolving its laws to address these diverse motivations. The Information Technology Act, 2000 and relevant provisions of Indian Penal Code provide primary legal framework for handling cybercrime. However, effective prevention and enforcement require more than just legal provisions. Increased awareness about cyber threats, enhanced psychological profiling of offenders are important in combating cybercrime. By understanding the motivations behind the

[24] Tiwari, S., Rai, S. K., & Sisodia, V. (2023). Analysis of Cybercrime against Indian Youth on Social Media. 13(4).

cybercrimes, law enforcement agencies can better anticipate, prevent and investigate cybercrimes, creating a safe environment.

CHAPTER 4: BEHAVIOURAL PATTERNS OF CYBER CRIMINALS

4.1 PROFILING CYBER CRIMINALS: AGE, GENDER, SOCIO-ECONOMIC STATUS

Understanding the individuals behind cybercrimes is essential for effective prevention, law enforcement, and policy-making. This chapter explores the multifaceted dimensions of cybercriminal profiles, including demographic traits, psychological characteristics, and typologies, while also analysing emerging trends and the influence of social engineering tactics.

Cyber Criminal profiling is usually used in investigation of difficult-to-detect crimes (especially when there are indications that an offence, or a series of offences were committed by a person having a mental disorder). Criminal profiling can also be used in cases where there are several suspects; more intensive search is done for the person who corresponds to the established profile. At the general level, profiling is the classification of individuals according to their characteristics, i.e. whether they are "constant" (such as gender, age, ethnic origin, and height) or "variable" (such as habits, choice and other behavioural elements). Profiling can be a legitimate tool to apprehend suspected offenders after a criminal offense has been committed. Profiling can also be based on deliberate assumptions derived from experience and training, focusing on behaviour rather than racial, ethnic or religious characteristics. For example, police officers can work with profiles that contain instructions to search for people who repeatedly visit certain sites, that behave unpredictably or nervously, or who repeatedly make large purchases using only cash.[25] (Kipane, 2019)

[25] Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. SHS Web of Conferences, 68, 01009.

Age: Cyber criminals are far younger than the rest of the criminal population. In the US, for instance, the average age of someone caught committing cybercrime is 19, as opposed to 37 for all other offenses. In the UK, the average age of a cyber-criminal is only 17, reflecting a trend of teenagers and young adults dominating cybercrimes. This younger demographic is in direct contrast to the cyber security industry as a whole, which has an average age of more than 40.

Gender: The gender breakdown of cyber criminals is more evenly split than in most other crime types. Recent research suggests that a minimum of 30% of cyber criminals are female, with some dark web forum analyses suggesting the number could be up to 40%. This is a considerably higher percentage than that of females in the overall prison population (4–8% in UK, Russia, and US) and even greater than that of women employed in the cyber security field. The underground of cybercrime seems to be quite gender-neutral, with proficiency and expertise taking precedence over gender.

Socio- Economic Status: The socio-economic aspect has an important role to play in engaging in cybercrime. Studies indicate a direct link between poor economic growth, widespread unemployment, and lower levels of education and heightened cybercrime prevalence, especially in the developing world. In India, for instance, the majority of cybercrime victims are from the middle socio-economic class (53.34%), followed by the upper class (30%) and the lower class (16.66%). Urban regions are more hit than rural areas, possibly because they enjoy greater internet penetration and online accessibility. On a macro level, lower-GDP-per-capita and higher-unemployment-rate nations or areas typically suffer more from cybercrime, as financial insecurity can lead individuals to turn towards criminal online activity.[26] (Ilievski & Bernik, 2008)

[26]Ilievski, A., & Bernik, I. (2008). SOCIAL-ECONOMIC ASPECTS OF CYBERCRIME. Innovative Issues and Appoaches in Social Science, 9(3), 8–22.

4.2 PSYCHOLOGICAL TRAITS AND BEHAVIOURAL PATTERNS OF CYBER CRIMINALS

The psychology of cybercriminals has identified several key personality traits and behaviours that are commonly exhibited by individuals who engage in cybercrime. These traits include narcissism, which can manifest as a grandiose sense of self-importance and a lack of empathy for others; Machiavellianism, characterized by manipulative and exploitative behaviour; and low self-control, which can lead to impulsive and reckless actions online. Additionally, some cybercriminals may display a lack of empathy, making it easier for them to engage in harmful behavior without remorse. Furthermore, certain types of cybercrime, such as online stalking or cyberbullying, may be linked to addictive behaviours, where individuals become fixated on their online activities and struggle to control their impulses. Understanding these psychological factors can help in developing more effective strategies for preventing and addressing cybercrime.

PSYCHOLOGICAL TRAITS AND BEHAVIOUR IN CYBERCRIMINALS

ANONYMITY

The perception of being anonymous online can lead to a sense of freedom from accountability. This can result in individuals feeling more comfortable engaging in behaviours they might avoid in person. Anonymity can also contribute to a sense of disinhibiting, leading to increased impulsivity and risk-taking. [27](Van De Weijer & Leukfeldt, 2017)

NARCISSISM

Characterized by an inflated sense of self-importance and a need for admiration. Individuals with narcissistic tendencies may use online platforms to seek validation and

[27] Van De Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. Cyberpsychology, Behavior, and Social Networking, 20(7), 407–412.

attention. This can manifest in behaviours such as excessive self-promotion, grandiosity, and a lack of empathy for others.

IMPULSIVITY

Impulsive individuals may act on instinct without fully considering the consequences of their actions. In the context of cybercrime, impulsivity can lead to reckless behavior, such as engaging in hacking or online harassment without thinking through the potential repercussions. Impulsivity can also contribute to a lack of self-control, making it more challenging for individuals to resist the temptation of engaging in cybercrime.

OTHER RELEVANT TRAITS

Machiavellianism: A tendency to manipulate and exploit others for personal gain.

Lack of Empathy: Difficulty understanding and relating to the feelings and perspectives of others.

Low Self-Control: Struggling to regulate one's own behaviour, leading to impulsive and reckless actions.

Understanding these psychological traits can provide valuable insights into the motivations and behaviours of individuals who engage in cybercrime. [28](Kamaluddin et al., 2015)

4.3 CYBER CRIMINAL TYPOLOGY: HACKERS, FRAUDSTERS, CYBER STALKERS, AND ORGANIZED CYBER CRIME GROUPS

Cybercrime is the broad spectrum of illegal acts carried out electronically. Knowing the typology of cyber criminals, including hackers, fraudsters, cyber stalkers, and organized cybercrime groups, clarifies their intentions, tactics, and threats.

---

[28] Kamaluddin, M. R., Shariff, N. S. M., Othman, A., Ismail, K. H., & Saat, G. A. M. (2015). Linking psychological traits with criminal behaviour: A review. ,. ASEAN Journal of Psychiatry, 16(2), 13–25.

Hackers: Hackers are talented individuals who break into systems, frequently taking advantage of vulnerabilities to access the system without permission. There are various kinds of hackers:

- Black-hat hackers participate in evil deeds for personal benefit or disruption.
- White-hat hackers test and enhance security systems under authorization.
- Hacktivists employ hacking for political or social cause promotion.

Their activities may involve data stealing, malware dissemination, website defacement, or service disruption.

Fraudsters: Fraudsters utilize deception to engage in crime like identity theft, financial fraud, and phishing scams. Most common techniques include:

Phishing: The sending of false emails or messages to deceive victims into exposing sensitive information.

Internet fraud: Involves a variety of scams, such as online purchasing fraud, bank fraud, and credit card fraud.

Their financial motivation is usually the main one, many of them targeting individuals and organizations for theft of money. [29](Albanese, 2022)

Cyber Stalkers: Cyber stalkers harass, intimidate, or threaten victims using digital media, many times leaving them emotionally distressed. Methods involve:

- Repeated unwanted messages sent to the victim.
- Monitoring online behaviour.
- Spreading malware in order to spy on victims.

Motives can vary from personal grudges to bids to blackmail or libel.

---

[29] Albanese, J. S. (2022). A Typology of Cybercrime: An Assessment of Federal Prosecutions. Journal of Criminal Justice and Law, 6(1).

ORGANIZED CYBER CRIME GROUPS

These are organized groups that systematically commit cybercrime, frequently based across borders. Types of groups:

Type I: Primarily operate online, carrying out cybercrimes like mass hacking, ransomware attacks, and data breaches.

Type II: Operate both online and offline, employing cyber tools to enable conventional crimes (e.g., drug dealing, people trafficking).

Type III: Employ information technology primarily to enable offline criminal activity.

Specially organized groups are extremely sophisticated, utilizing sophisticated tools, labour division, and occasionally providing cybercrime-as-a-service (such as Ransomware-as-a-Service).

Their operations have the capacity to destabilize organizations, economies, and even national security.[30] (McDevitt et al., 2022)

4.4 ROLE OF SOCIAL ENGINEERING IN CYBER CRIMINAL BEHAVIOUR

Social engineering is a central tactic in modern cybercrime, exploiting human psychology rather than technical vulnerabilities to deceive individuals and organizations. By manipulating individuals into divulging sensitive information or performing certain actions, cybercriminals can gain unauthorized access to systems, data, and financial resources.[31] (Regent University, Virginia Beach, Virginia, USA & Choi, 2023)

[30] McDevitt, J., Levin, J., & Bennett, S. (2022). Hate Crime Offenders: An Expanded Typology. Journal of Social Issues, 58(2).

[31] Regent University, Virginia Beach, Virginia, USA & Choi, 2023

TYPES OF SOCIAL ENGINEERING ATTACKS

Phishing: Fraudulent emails, messages, or websites that trick victims into revealing sensitive information.

Pretexting: Creating a fictional scenario to gain the trust of victims and obtain sensitive information.

Baiting: Leaving malware-infected devices or storage media in public areas to exploit curiosity and trust.

Quid Pro Quo: Offering services or benefits in exchange for sensitive information or access.

ROLE OF SOCIAL ENGINEERING IN CYBER CRIMINAL BEHAVIOUR

The important roles are:

1. Psychological Manipulation: Social engineering involves manipulating victims into performing actions or divulging confidential information. Techniques include phishing (fraudulent emails), vishing (voice phishing), smishing (SMS phishing), baiting, and impersonation.
2. Brand Impersonation and Fraud: Cybercriminals frequently abuse trusted brand identities to create fake websites, apps, and domains, tricking users into sharing sensitive data or making fraudulent payments. Brand abuse alone is projected to account for nearly ₹9,000 crore of cybercrime losses in India in 2025.
3. AI-Driven Attacks: The use of artificial intelligence has made social engineering attacks more convincing and harder to detect. AI is used to craft highly personalized phishing emails, deepfake voice calls, and AI-generated chatbots, increasing the success rate of scams.

4. Targeting Vulnerable Groups: Elderly citizens and less tech-savvy users are frequently targeted through scams that exploit trust or fear, such as fake law enforcement calls or fraudulent investment schemes.
5. Remote Work and Social Media Exploitation: The rise in remote work has created new vulnerabilities, with attackers leveraging personal devices and unsecured networks. Social media is also mined for personal information to create highly targeted spear-phishing campaigns.
6. Scale and Impact: Social engineering is implicated in a majority of high-value scams. In 2024, India saw over 17 lakh cybercrime complaints, with a significant portion linked to social engineering tactics. The financial sector, retail, and e-commerce are especially vulnerable. (Chantler & Broadhurst., 2008)

SOCIAL ENGINEERING IN THE INDIAN CONTEXT

In India, the role of social engineering in cybercrime has been particularly pronounced due to a combination of digital illiteracy, lack of awareness, and over trust in digital communications. Common social engineering scams in India include:

1. OTP scams: Victims are tricked into sharing one-time passwords, often under the pretext of verifying an account.
2. Fake job offers: Scammers send fraudulent employment offers to collect application fees or steal identities.
3. KYC update frauds: Attackers claim to be from banks and ask for documents or OTPs to “update” the customer’s KYC.
4. Tech support scams: Often originate from fake call centres pretending to be representatives of reputed companies.
5. WhatsApp impersonation: Hackers use the identity of a known contact to request money or sensitive information.

A study by the Indian Cyber Crime Coordination Centre (I4C) revealed that social engineering accounts for over 60% of online financial frauds, highlighting its widespread usage. (Chitrey et al., 2012)

4.5 TRENDS AND EVOLUTION OF CYBER CRIMINAL BEHAVIOUR IN INDIA

India’s digital revolution—fuelled by increasing internet penetration, smartphone use, and government initiatives like Digital India—has dramatically altered the landscape of crime. As more individuals and businesses migrate online, so too have criminal elements, leading to the rapid evolution of cybercriminal behaviour. This section examines the emerging trends, evolving techniques, and regional patterns that characterize cybercrime in the Indian context.

CHAPTER 5: LEGAL AND INSTITUTIONAL RESPONSE TO CYBER CRIME IN INDIA

5.1 CYBER LAWS IN INDIA: INFORMATION TECHNOLOGY ACT, 2000 & AMENDMENTS

India's cyber legal framework is primarily governed by the Information Technology Act, 2000 (IT Act), enacted to provide legal recognition to electronic commerce and to address cybercrime. The IT Act is a dynamic legislation that has evolved through amendments to address emerging digital threats.

Objective of this Act: The main objectives of this Act are:

I. Promote efficient delivery of government services electronically or facilitate digital transactions between firms and regular individuals.
II. Impose penalties upon cybercrimes like data theft, hacking, identity theft, cyber stalking and so on, in order to create a secure cyber landscape.
III. Formulate rules and regulations that monitor the cyber activity and electronic mediums of communication and commerce.
IV. Promote the expansion and foster innovation and entrepreneurship in the Indian IT/ITES sector.

MAJOR PROVISIONS OF THE ACT

The major provisions of this Act are:

1. Legal Recognition of Electronic Records and Digital Signatures (Sections 4-10A)

a. Grants legal validity to contracts formed through electronic means,
b. Recognizes digital signatures as equivalent to physical ones,
c. Establishes mechanisms for the certification and authentication of digital documents.

2. Regulation of Certifying Authorities (Sections 17-34)

Framework for appointing and regulating Certifying Authorities responsible for issuing digital certificates.

3. Corporate Responsibility (Section 43A)

Holds companies accountable for negligent handling of sensitive personal data, requiring them to implement reasonable security practices.

4. Cyber Offenses and Penalties (Sections 65-74)

The Act criminalizes several cyber activities, including:

a. Section 65: Tampering with computer source documents,
b. Section 66: Hacking and unauthorized access,
c. Section 66C: Identity theft and misuse of digital signatures or passwords,
d. Section 66D: Cheating by impersonation using computer resources (used extensively in phishing and job fraud cases),
e. Section 67: Publishing or transmitting obscene material electronically,
f. Section 67A & 67B: Punishments for sexually explicit content and child pornography.

5. Adjudication and Appellate Process

I. Empowers Adjudicating Officers to settle disputes involving claims up to ₹5 crores,
II. Constitutes the Cyber Appellate Tribunal (CAT) to hear appeals.

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The major amendment which are mainly made in the Information Technology (Amendment) Act, 2008 are:-

1. NEW OFFENSES AND PENALTIES

Cybercrimes: The act introduced new offenses such as identity theft, cyber terrorism, cheating by personation, violation of privacy, and transmitting sexually explicit content, along with specific penalties for each.

Cyber Terrorism: Section 66F was introduced to address cyber terrorism, providing for stricter penalties than other offenses.

2. DATA PROTECTION AND PRIVACY

Sensitive Personal Information (SPI): Section 43A was added to prohibit the unauthorized disclosure of "sensitive personal information," enhancing privacy safeguards.

Negligence in Handling SPI: The act provided for damages to be paid by companies that negligently handle SPI, causing wrongful loss to individuals.

Breach of Contract: Section 72A was inserted, criminalizing the disclosure of information in breach of a lawful contract.

3. INTERMEDIARY LIABILITY

Clarification of Liability: The act clarified the liability of intermediaries, such as internet service providers and social media platforms, for unlawful activities conducted through their platforms.

"Due Diligence" for Intermediaries: Cyber cafes were defined as intermediaries, and they were required to exercise "due diligence" to prevent the use of their platforms for illegal activities, according to one source.

4. ELECTRONIC RECORDS AND EVIDENCE

Legal Recognition: The act provided for the legal recognition of electronic records and transactions, facilitating electronic commerce and document filing.

Electronic Signatures: The introduction of electronic signatures, replacing the term "digital signature," enabled the use of electronic records and signatures in court proceedings.

5.2 ROLE OF LAW ENFORCEMENT IN TACKLING CYBER CRIMES

Law enforcement agencies play a crucial role in tackling cybercrime by preventing, detecting, investigating, and prosecuting cyber-related offenses. This involves using specialized units, digital forensics, and collaborating with various stakeholders to build a strong digital ecosystem for tackling cybercrime. They also focus on raising public awareness about cybercrime prevention and reporting. The role of law enforcement which help in combating cybercrime are:

1. PREVENTION AND DETECTION

Law enforcement agencies can proactively identify and block malicious accounts, SIM cards, and other digital assets used in cybercrime, like digital arrest and blackmailing. They can also act as an early warning system for proactive cybercrime prevention and detection, ensuring the safety and security of citizens. Building awareness through various channels, like social media, SMS, radio, and public campaigns, is also crucial for preventing cybercrimes. Using tools like the National Cyber Crime Reporting Portal allows citizens to report cybercrimes, which helps law enforcement in prevention and investigation.

2. INVESTIGATION AND ENFORCEMENT

Specialized cybercrime units within police departments are equipped with the skills and technology to trace digital footprints, gather evidence, and apprehend cybercriminals. They conduct thorough investigations, including digital forensic analysis of computers and other devices used by suspects, to gather evidence. These investigations involve identifying the nature of the cybercrime, tracing the perpetrator, and building a case against them. Effective investigation also includes securing warrants for access to devices, gathering information, and analysing data to build a strong case.

3. PROSECUTION AND LEGAL ACTION

Adequate legal frameworks are crucial for prosecuting cybercriminals and deterring potential offenders. Law enforcement works closely with prosecutors and judges to ensure the proper prosecution of cybercrimes, ensuring justice for victims. They utilize various legal tools, including asset forfeiture, to deprive criminals of their ill-gotten gains and compensate victims.

4. COLLABORATION AND COORDINATION

Law enforcement agencies need to work in coordination with other stakeholders, like the private sector, telecommunication providers, and international bodies like Interpol, to tackle cybercrime effectively. Joint cyber coordination teams (JCCTs) are established to enhance the coordination framework among law enforcement agencies of states and UTs, particularly in cybercrime hotspots. Sharing intelligence, best practices, and resources among law enforcement agencies and other stakeholders is crucial for combating cybercrime.

5. CAPACITY BUILDING

Training programs for law enforcement personnel, judicial officers, and prosecutors on cybercrime awareness, investigation, and forensics are essential. Establishing cyber forensic-cum-training laboratories and national cyber forensic laboratories provides the necessary support for evidence handling and analysis. By effectively performing these

roles, law enforcement agencies play a vital role in creating a safer digital environment for everyone.[32](Holden et al., 2015)

5.3 CHALLENGES IN PROSECUTING CYBER CRIMINALS

Prosecuting cybercriminals presents numerous challenges, primarily due to the digital nature of the crimes, which makes evidence volatile, difficult to trace, and often obscured by encryption and anonymity. Additionally, jurisdictional issues arise when crimes span international boundaries, and legal frameworks may not keep pace with rapidly evolving technology[33](Ajayi, 2016). The main challenges which are faced by the law maintaining agencies are:

1. THE NATURE OF DIGITAL EVIDENCE

Volatility and Modifiability: Digital evidence is easily changed, deleted, or concealed, making it difficult to preserve and use in court.

Data Volume: The sheer volume of digital data can make it difficult to find and analyse relevant evidence.

Technical Expertise: Law enforcement agencies often lack the specialized training and resources to collect, preserve, and analyse digital evidence effectively.

2. JURISDICTIONAL ISSUES

Cross-Border Crimes: Cybercrimes can occur in one country but impact victims in another, making it difficult to determine which jurisdiction should prosecute.

Varying Laws: Different countries may have varying definitions of cybercrime and different penalties, leading to inconsistencies in prosecution.

---

[32] Holden, N., Michailova, S., & Tietze, S. (2015). The Routledge Companion to Cross-Cultural Management (1st ed.). Routledge.

[33] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1–12.

International Cooperation: Effective prosecution often requires cooperation between different countries, which can be complex and time-consuming.

3. ANONYMITY AND ENCRYPTION

VPNs and Dark Web: Cybercriminals use tools like VPNs and the dark web to hide their identities and activities.

Encryption: Encryption protects communication and data, making it difficult for law enforcement to access and analyse evidence.

4. LEGAL FRAMEWORKS AND ENFORCEMENT

Outdated Laws: Existing laws may not adequately address new types of cybercrime or emerging technologies.

Lack of Training: Law enforcement and legal professionals may lack the specialized knowledge and skills needed to investigate and prosecute cybercrimes.

Extradition Challenges: Extradition can be difficult, especially when crimes are not perceived as serious in the other country's legal system.

5. PRIVACY AND DATA PROTECTION

Data Access: Privacy laws, such as GDPR, can limit law enforcement's access to data needed for investigations.

Data Security: Cybercriminals often target and compromise data protection measures, making it more difficult for law enforcement to obtain evidence.

6. MOTIVATION AND TACTICS

Economic Gains: Cybercriminals often pursue financial gains, such as stealing money, data, or intellectual property.

Sophistication: Cybercriminals are often highly skilled and use sophisticated tactics to evade detection.

Ransom ware: Ransom ware attacks, including double extortion and ransom ware-as-a-service, pose significant challenges for law enforcement and victims.[34] (Lunia & Gupta, 2024)

Addressing these challenges requires some of the reformative actions, including:

Strengthening legal frameworks: Updating laws to keep pace with technology and address emerging cybercrime threats.

Improving training and resources: Providing law enforcement agencies with the necessary training and resources to investigate and prosecute cybercrimes effectively.

Enhancing international cooperation: Promoting collaboration between countries to share information, investigate crimes, and pursue cybercriminals.

Investing in cyber security: Improving cyber security measures to protect individuals, organizations, and critical infrastructure from cyber-attacks.

Promoting public awareness: Educating the public about cybercrime risks and how to protect themselves online.[35](Obuobisa, n.d.)

5.4 JUDICIAL APPROACH TO CYBER CRIME CASES IN INDIA

The judiciary in India plays a crucial role in interpreting and enforcing laws related to cybercrime. As cybercrime continues to evolve with technological advancements, Indian courts have had to navigate new legal challenges, including issues of jurisdiction, anonymity, admissibility of electronic evidence, and the psychological motivations of

[34] Lunia, U., & Gupta, J. K. (2024). Cyber Crime and the Challenges of Prosecution and Prevention. International Journal of Law Management and Humanities, 7(4), 1038–1052.
[35] Obuobisa, M. Y. A. (n.d.). CHALLENGES FACED REGARDING CYBER CRIME AND THE RULE OF LAW IN CYBERSPACE FROM THE PERSPECTIVE OF A PROSECUTOR IN GHANA.

offenders. While the legislative framework is primarily governed by the Information Technology Act, 2000, the judiciary has, over time, shaped the understanding and application of cyber laws through various landmark rulings.

This chapter critically analyses how Indian courts have responded to cybercrime cases, the consistency in their reasoning, the gaps in legal interpretation, and the extent to which psychological and victim-centric perspectives have been incorporated into judgments.

1. RECOGNITION OF CYBERCRIME AS A SERIOUS OFFENSE

Indian courts have consistently acknowledged the gravity of cyber offenses, especially in cases involving privacy violations, harassment, and financial fraud. For instance:

State of Tamil Nadu v. Suhas Katti (2004)[36]: This was one of the earliest cyber stalking cases in India where the accused was convicted under Sections 469 and 509 of the IPC and Section 67 of the IT Act. The swift trial (just seven months) reflected the judiciary's proactive stance on cyber harassment and its impact on the victim's dignity.

Avnish Bajaj v. State (NCT of Delhi) (2008)[37]*:* In this case involving the sale of pornographic material on the Baazee.com platform, the court dealt with intermediary liability under the IT Act. The judgment emphasized the need for corporate entities to be vigilant in monitoring online content, setting important legal precedent.

2. UPHOLDING FREEDOM OF SPEECH VS. CURBING CYBER ABUSE

In the digital context, the judiciary has had to balance freedom of expression with the need to curb cyber abuse:

[36] State of Tamil Nadu v. Suhas Katti C.C. No. 4680 of 2004
[37] Avnish Bajaj v. State (NCT of Delhi)116 (2005) DLT 427 (Delhi HC)

SHREYA SINGHAL V. UNION OF INDIA (2015)[38]

The Supreme Court struck down Section 66A of the IT Act as unconstitutional, holding that it was vague and violated the right to free speech under Article 19(1)(a). However, the Court upheld other provisions that criminalize sending offensive messages via communication services, showing its intent to punish genuine cases of cyber abuse while protecting constitutional freedoms.

3. CHALLENGES IN DEALING WITH PSYCHOLOGICAL MOTIVATIONS

Although courts have acknowledged the psychological trauma suffered by victims, especially in cyber stalking, online defamation, and morphing cases, they have rarely explored the mental state or motivations of the offenders in detail. This reflects a gap in judicial reasoning where:

- Offender intent is assumed rather than analysed;
- Little consideration is given to psychological evaluations or expert testimony;
- Sentencing focuses more on deterrence than rehabilitation.

There is a pressing need for courts to incorporate criminological and psychological perspectives, especially in cases involving juveniles or first-time offenders, where reformative justice may be more appropriate.

4. ROLE OF JUDICIARY IN VICTIM PROTECTION AND COMPENSATION

The Indian judiciary has occasionally shown sensitivity to victims' rights:

- Courts have directed police to provide protection to victims of cyber harassment.
- In civil suits, damages have been awarded for defamation or privacy breaches.

[38] Shreya Singhal v. Union of India (2015) 5 SCC 1

- However, there is no uniform practice of awarding compensation under cyber laws, and victim protection measures are largely ad hoc.

There is a strong case Prajjwala v. Union of India[39], The Supreme Court directed intermediaries and law enforcement to remove sexually explicit content and provide safeguards for victims, indicating a victim-sensitive approach to cyber offenses, for adopting a victim-centric approach, including anonymity during proceedings, psychological support, and rehabilitation orders.

5. ADMISSIBILITY OF ELECTRONIC EVIDENCE

Courts have also played a decisive role in interpreting Section 65B of the Indian Evidence Act, which deals with the admissibility of electronic records. Key rulings include:

ANVAR P.V. V. P.K. BASHEER (2014)[40]

The Supreme Court clarified that electronic evidence is admissible only if it meets the conditions laid down under Section 65B, including the requirement of a certificate. This ruling emphasized the need for technical compliance in cybercrime prosecution, although it has posed practical challenges for investigators.

ARJUN PANDITRAO KHOTKAR V. KAILASH KUSHANRAO GORANTYAL (2020)[41]

The Court reaffirmed the importance of the Section 65B certificate and elaborated on the scope of exceptions, which has significant implications in cybercrime trials.

[39] Prajjwala v. Union of India,W.P. (Crl.) No. 36 of 2004
[40] Anvar P.V. v. P.K. Basheer(2014) 10 SCC 473
[41] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal(2020) 7 SCC 1

CHAPTER 6: PREVENTIVE STRATEGIES

6.1 ROLE OF AWARENESS AND DIGITAL LITERACY IN CRIME PREVENTION

The increasing sophistication of cybercrimes has exposed a critical vulnerability rooted not just in technology or law, but in human awareness and digital literacy. Proactive education and awareness-building are now recognized as the most effective defences against cyber threats, empowering users and deterring offenders more effectively than legal penalties alone.

1. BRIDGING THE KNOWLEDGE GAP

User Vulnerabilities: Many cybercrimes incidents stem from users' lack of knowledge about safe online practices, privacy protection, and legal recourse. Vulnerable groups—such as children, the elderly, and rural populations—are particularly at risk due to limited cyber security education.

Digital Literacy Initiatives: Targeted digital literacy programs significantly reduce cybercrime risk by equipping individuals with practical skills and awareness to recognize and avoid threats. These initiatives create an informed citizenry less susceptible to exploitation.

2. EMPOWERING INDIVIDUALS AS THE FIRST LINE OF DEFENCE

Active Defence: Digital literacy transforms users into proactive defenders of their digital environments. Skills such as recognizing phishing, managing privacy settings, and reporting incidents are crucial.

Self-Regulation: Educated users are less dependent on law enforcement and more likely to practice digital hygiene, such as updating software and securing networks, fostering a culture of shared responsibility for cyber safety.[42] (Mgs. Luis Antonio Villalta

[42] Mgs. Luis Antonio Villalta Gavilanes1, Mgs. Leonardo Orleans Labre Villalta2, Mgs. Adriana et al., 2024

Gavilanes1, Mgs. Leonardo Orleans Labre Villalta2, Mgs. Adriana et al., 2024)3. Awareness as a deterrent against cybercrime

Preventing offenses: awareness programs targeting potential offenders—especially youth—highlight the legal and ethical consequences of cyber misconduct. This reduces offenses committed out of ignorance or peer influence.

Ethical digital behaviour: digital literacy initiatives that emphasize cyber laws, penalties, and the psychological impact on victims can deter cyber offenses by embedding ethical norms and informed decision-making from an early stage.

4. ROLE OF EDUCATIONAL INSTITUTIONS AND GOVERNMENT

Schools and universities: integrating cyber ethics and digital civility into curricula, conducting workshops, and collaborating with experts are effective strategies for early intervention.

Government initiatives: national campaigns and subsidized courses, especially in regional languages, broaden the reach of digital literacy and awareness, particularly among marginalized communities.

5. ROLE OF MEDIA AND CIVIL SOCIETY

Amplifying awareness: media and ngos play a critical role by broadcasting real-life case studies, promoting victim support, and encouraging positive online behavior through campaigns and public service announcements.

6. INTEGRATION WITH LEGAL FRAMEWORKS

Policy and corporate responsibility: statutory mandates for awareness initiatives, corporate user education guidelines, and court-directed awareness sessions for juvenile offenders can bridge the gap between legal remedies and preventive education.

Digital literacy and cyber awareness are not optional but foundational pillars of cybercrime prevention. They empower citizens, deter offenders, and reduce the burden on legal and enforcement systems. In the digital age, a legally literate and digitally aware population is the most effective safeguard against cyber threats—making knowledge the true currency of protection and justice. (Musaddag Elrayah & Saima Jamil, 2023)

6.2 ETHICAL HACKING AND CYBER SECURITY MEASURES

ETHICAL HACKING

Ethical hacking, often referred to as white-hat hacking, is the process of deliberately probing and testing computer systems, networks, or applications to identify vulnerabilities that malicious actors could exploit. Unlike black-hat hackers who aim to breach systems for illegal purposes, ethical hackers operate within legal boundaries and with explicit authorization from the organization they are testing. Their ultimate goal is to improve cyber security defences and ensure that systems remain resilient against attacks.

The primary purpose of ethical hacking is to identify and fix vulnerabilities before cybercriminals can exploit them. Ethical hackers simulate real-world cyber-attacks to expose weaknesses in a system's infrastructure, such as outdated software, weak passwords, unpatched vulnerabilities, or improper configurations. By doing so, they provide organizations with detailed reports outlining the security gaps and recommending necessary fixes to strengthen defences.

Common ethical hacking techniques include penetration testing, where hackers attempt to breach a system as a real attacker would, and vulnerability scanning, which involves using automated tools to identify potential security flaws. Additionally, ethical hackers often utilize social engineering techniques, such as phishing simulations, to test how susceptible employees are to manipulation and how well an organization's security culture is enforced.

Ethical hackers rely on a variety of specialized tools that help them gather information about a target, identify weaknesses, and test exploitability in order to perform their assessments. As detailed in an article published by The Cyber Express, ethical hackers conduct these simulated attacks to "showcase how cybercriminals could breach a network and the potential consequences of such breaches. The insights gained from these simulated attacks empower organizations to identify and address vulnerabilities, bolster security measures, and safeguard sensitive data effectively."

In essence, ethical hacking provides organizations with a proactive approach to securing their digital assets. By identifying and addressing vulnerabilities before they become threats, ethical hackers play a crucial role in safeguarding sensitive data and ensuring robust cyber security defences.[43](Varshney et al., 2023)

CYBER SECURITY MEASURES

Cyber security measures are technical and organizational precautions designed to protect computer systems and networks from cyber-attacks and unauthorized access. These measures encompass various strategies, from basic hygiene practices like strong passwords to advanced tools like firewalls and intrusion detection systems. The measures we must take to protect our self are;

- Strong Passwords: Using unique, complex passwords is a fundamental security practice.
- Firewalls: Firewalls act as a barrier, filtering network traffic and blocking unauthorized access.
- Antivirus Software: Antivirus software detects and removes malware, protecting systems from malicious threats.

[43] Varshney, M., Kumar, A., Ganguli, R., Umer, S., Sonkar, S. S., & Molla, N. (2023). Ethical Hacking: Enhancing Cybersecurity through Offensive Security Practices. 44(4).

- Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring multiple forms of verification, like a password and a code from a mobile device.
- Regular Software Updates: Updating software and operating systems patches vulnerabilities and enhances security.
- Data Backups: Regularly backing up data ensures that you can recover important information in case of a cyber-attack or data loss.
- Network Security: Securing networks involves measures like implementing strong passwords, firewalls, and intrusion detection systems.
- Employee Training: Educating employees about cyber threats and best practices can significantly reduce the risk of human error.
- Incident Response: Having a plan in place to respond to and recover from cyber incidents is crucial.
- Encryption: Encrypting data protects it from unauthorized access by making it unreadable without a decryption key.
- Access Control: Controlling access to data and systems limits who can access sensitive information.
- Security Awareness: Raising awareness about cyber security threats and best practices can help individuals and organizations protect themselves.
- Threat Detection and Response: Implementing tools and processes to detect and respond to cyber threats in real-time is essential.
- Disaster Recovery: Having a plan to recover from a major system failure or data loss is crucial.[44](Lunia & Gupta, 2024)

6.3 ROLE OF GOVERNMENT, PRIVATE SECTOR, AND CIVIL SOCIETY IN CYBER CRIME PREVENTION

In combating cybercrime, the government, private sector, and civil society each play distinct yet interconnected roles. Governments establish legal frameworks and

[44] Lunia, U., & Gupta, J. K. (2024). Cyber Crime and the Challenges of Prosecution and Prevention. International Journal of Law Management and Humanities, 7(4), 1038–1052.

regulations, while the private sector implements security measures and develops technology solutions. Civil society organizations, such as NGOs, play a crucial role in raising public awareness, advocating for policy changes, and providing support to victims.[45] (Kipane, 2019)

GOVERNMENT'S ROLE

1. Legal Frameworks: Governments create and enforce laws that define cybercrime and provide mechanisms for investigation and prosecution. The Information Technology Act, 2000, in India, for example, serves as the primary legal framework for cybercrime.
2. Policy Development: Governments develop national cyber security strategies, setting goals and priorities for addressing cyber threats.
3. Law Enforcement: Law enforcement agencies, like the Indian Cyber Crime Coordination Centre (I4C), are responsible for investigating and prosecuting cybercrimes.
4. Public Awareness: Governments often launch awareness campaigns to educate the public about cybercrime risks and how to protect themselves.
5. International Cooperation: Governments collaborate with other countries and international organizations to share information and coordinate efforts to combat cybercrime.

PRIVATE SECTOR'S ROLE

1. Security Measures: Private companies implement security technologies and practices to protect their systems and data from cyber-attacks.
2. Technology Development: The private sector develops new security tools and technologies to detect and prevent cybercrimes.
3. Incident Response: Private companies are responsible for responding to cyber-attacks that compromise their systems and data.

---

[45]Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. SHS Web of Conferences, 68, 01009.

4. Reporting Cybercrimes: Private companies may report cybercrimes to law enforcement agencies and other relevant stakeholders.
5. Collaboration with Government: The private sector collaborates with government agencies on cyber security initiatives and policy development.

CIVIL SOCIETY'S ROLE

- Awareness and Education: Civil society organizations raise public awareness about cybercrime risks and empower individuals to protect themselves.
- Advocacy: Civil society organizations advocate for policy changes and reforms that address cybercrime and promote cyber security.
- Victim Support: Civil society organizations provide support and assistance to victims of cybercrime, such as counselling and legal assistance.
- Research and Analysis: Civil society organizations conduct research on cybercrime trends and develop tools and resources for preventing and responding to cyber threats.
- Transparency and Accountability: Civil society organizations play a role in promoting transparency and accountability in cyber security governance.
- Public Dialogue: Civil society organizations facilitate public dialogue and collaboration between governments, the private sector, and civil society on cybercrime issues.

6.4 NEED FOR PSYCHOLOGICAL REHABILITATION OF CYBER CRIMINALS

The conventional method of enforcing cybercrime has been predominantly retributive and deterrent, with an emphasis on penalties in the form of fines, imprisonment, and technology bans. Yet, psychological motivations underlying cybercrime frequently reveal that most of the criminals—particularly juveniles, first-time criminals, and those motivated by compulsive or ideological reasons—would profit considerably from psychological treatment as opposed to purely punitive penalties. With the intricate interplay between emotional, cognitive, and social elements that go into perpetuating

cybercrimes, rehabilitation is not only a moral obligation but also a strategic legal requirement.

1. PSYCHOLOGICAL DRIVERS NEED SPECIFIC INTERVENTIONS

Most cybercrimes are perpetrated in isolation, and without a full appreciation of their fallout. The perpetrators can be plagued by:

1. Addictive internet browsing or compulsive behaviour
2. Low emotional intelligence or lack of empathy
3. Impulse control disorders or narcissistic tendencies
4. Social isolation or peer pressure on the internet

Rehabilitation is capable of counteracting these underlying cognitive and behavioural distortions, discouraging recidivism.

2. SHORTCOMINGS OF PUNITIVE METHODS ALONE

Detention of cybercriminals or imposition of fines merely accomplishes little in:

1. Altering behavioural patterns
2. Shattering criminal digital subcultures
3. Arming offenders with ethical digital literacy

This is particularly the case with juvenile cyber offenders and young adults, who can be more guided by online groups than criminal motive.

3. AVOIDING RECIDIVISM THROUGH BEHAVIOURAL THERAPY

Cybercriminals, especially hackers and con artists, tend to offend again as a result of a mix of technical expertise, absence of remorse, and ongoing access to the internet. Successful rehabilitation programs that include:

1. Cognitive Behavioural Therapy (CBT)

2. Moral Reasoning Training
3. Digital ethics instruction

Anger management and empathy skills development may offer long-term behavioral change.[46](Office, n.d.)

4. INTERNATIONAL EVIDENCE SUPPORTING REHABILITATION

A number of nations have already started incorporating psychological support in cybercrime management:

1. Germany and the Netherlands have launched correction programs with an emphasis on psychosocial counselling for cyber criminals.
2. In the UK, rehabilitation through mentorship schemes has cut crime rates among juvenile online criminals.
3. Singapore's Cyber Wellness program aims to educate youth on good digital behaviour.

These programs demonstrate that rehabilitation can be more effective in reintegration than punishment alone.

5. INDIAN CONTEXT: THE GAP TO BE FILLED

Present legal provisions like the Information Technology Act, 2000 and the Indian Penal Code in India have no organised framework for the rehabilitation of cyber offenders. There is no provision for:

1. Psychological evaluation at investigation or sentencing time
2. Forced therapy or counselling for convicted offenders
3. Community-based correctional programmes specifically designed for digital offences

[46] Office, M. P. P. (n.d.). GUIDELINES TO FIGHT CYBERCRIMES AND PROTECT VICTIMS.

Incorporating psychological rehabilitation would align Indian cyber law with restorative justice principles and provide a humane alternative that promotes reform over retribution. Rehabilitation must become a central component of criminal justice policy. Legal reforms should mandate:

- Psychological screening of cyber offenders
- Mandatory counselling and digital ethics training
- Establishment of interdisciplinary rehabilitation centres involving law, psychology, and cyber forensics
- Special attention to juveniles and first-time offenders, ensuring they are not criminalized for life due to digital immaturity

In essence, the digital age requires a digitally intelligent legal system—one that not only punishes but also transforms. Psychological rehabilitation of cybercriminals stands as a critical step toward this transformation.[47](Nidham Othman et al., 2024)

[47] Nidham Othman, S., Fadhil Alziboon, M., Dawood, M., Jameel Sachet, S., & Moroz, I. (2024). New rehabilitation against electronic crimes by young people.

CHAPTER 7: CONCLUSION AND SUGGESTIONS

7.1 CONCLUSION

In conclusion the researcher has provided valuable insights into the psychology of cybercrime in India, highlighting the complex interplay of motivations, behaviours, and psychological factors that drive cybercriminal activity. Cybercriminals in India are driven by a mix of personal, psychological, social, and economic motivations.

Common reasons include financial gain, revenge, thrill-seeking, ideological expression, and a desire for power or recognition. The findings underscore the need for a comprehensive approach to addressing cybercrime, one that takes into account the unique psychological and behavioural characteristics of cybercriminals operating in the Indian context.

By understanding the primary motivations behind cybercrime, including financial gain, thrill-seeking, and revenge, law enforcement agencies and policymakers can develop targeted strategies to prevent and intervene in cybercrime.

Additionally, the study's findings on the role of psychological factors, such as personality traits and emotional regulation, in shaping cybercriminal behaviour can inform the development of mental health interventions and support services for individuals at risk of engaging in cybercrime. Unemployment, academic failure, peer pressure, and lack of family support were seen as indirect psychological drivers pushing individuals towards online crime.

Although the Information Technology Act, 2000 provides a legal foundation, it insufficiently addresses the behavioural aspects of cybercrime. Law enforcement agencies also face challenges due to lack of training in psychological profiling and cyber investigation techniques.

Ultimately, this research contributes to a deeper understanding of the psychological underpinnings of cybercrime in India, providing a foundation for evidence-based policies and interventions to mitigate this growing threat.

As the digital landscape continues to evolve, it is essential to prioritize research and collaboration in this area to stay ahead of emerging cyber threats and ensure a safer digital environment for all. Understanding the mind behind the crime is essential for building a resilient and responsive digital society.

7.2 SUGGESTIONS

After analysing all the factor motivation and psychological traits the researcher gave suggestion which will the others in near future.

1. Incorporate Psychological Evaluation in Cybercrime Investigations: Law enforcement should work with forensic psychologists to create psychological profiles of cyber offenders and assess recidivism risks.
2. Amendments to IT Act for Rehabilitation Provisions: Introduce statutory provisions for psychological counselling and rehabilitation of first-time or juvenile cyber offenders.
3. Mandatory Digital Literacy Programs: Schools, colleges, and workplaces should include cyber ethics, digital responsibility, and the psychological impact of online actions in their curricula.
4. Strengthen Cyber Forensics and Training: Invest in training police officers, prosecutors, and judges in cyber psychology and online behavioural analysis.
5. Establish Interdisciplinary Research Centres: Promote academic and institutional collaboration between law schools, psychology departments, and tech institutes to conduct research on cybercriminal behaviour.
6. Integration of Cyber Psychology in Legal Curriculum: Introduce modules on cyber psychology, digital behaviour, and forensic psychology in the syllabi of law schools, police academies, and judicial training institutes to sensitize legal professionals about the mental processes behind cyber offences.

7. Mental Health Support for Juvenile Offenders: Mandate counselling and mental health evaluation for juveniles involved in cybercrime. Partner with child psychologists and NGOs to design rehabilitation programs that focus on emotional intelligence, empathy, and responsible digital conduct.
8. Cybercrime Victim Support Helpline with Psychological Assistance: Set up a national helpline offering both legal guidance and psychological support to victims of cybercrime, especially in cases of cyberbullying, revenge porn, doxing, or financial scams.

REFERENCES

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1–12. https://doi.org/10.5897/JIIS2015.0089

Albanese, J. S. (2022). A Typology of Cybercrime: An Assessment of Federal Prosecutions. Journal of Criminal Justice and Law, 6(1).

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. Information Management & Computer Security, 11(5), 209–215. https://doi.org/10.1108/09685220310500117

Cybercrime: A review of the evidence Chapter 1: Cyber-dependent crimes. (n.d.).

Fereshteh Momeni. (2024). The impact of social, cultural, and individual factors on cybercrime. Educational Administration: Theory and Practice, 30(5), 10152–10159. https://doi.org/10.53555/kuey.v30i5.4716

Goni, O. (2021). Cyber Crime and Its Classification. International Journal of Electronics Engineering and Applications, 10(2), 01–17. https://doi.org/10.30696/IJEEA.X.I.2022.01-17

GeorgeF. du Pont. (2001). Criminalization of True Anonymity in Cyberspace, The. Michigan Telecommunications and Technology Law Review, 7(1).

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE

Holden, N., Michailova, S., & Tietze, S. (2015). The Routledge Companion to Cross-Cultural Management (1st ed.). Routledge. https://doi.org/10.4324/9780203798706

Ibrahim, S., Nnamani, D. I., & Okosun, O. (n.d.). Types of Cybercrime and Approaches to Detection.

Ilievski, A., & Bernik, I. (2008). SOCIAL-ECONOMIC ASPECTS OF CYBERCRIME. Innovative Issues and Appoaches in Social Science, 9(3), 8–22. http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2016-no3-art1

Kamaluddin, M. R., Shariff, N. S. M., Othman, A., Ismail, K. H., & Saat, G. A. M. (2015). Linking psychological traits with criminal behaviour: A review. ,. ASEAN Journal of Psychiatry, 16(2), 13–25.

Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. SHS Web of Conferences, 68, 01009. https://doi.org/10.1051/shsconf/20196801009

Khan, N., Shaikh, A., & Singh, M. V. P. (2023). Understanding of cyber defamation and its impact: a critical analysis. Dogo Rangsang Res J, 13, 168-173

Lunia, U., & Gupta, J. K. (2024). Cyber Crime and the Challenges of Prosecution and Prevention. International Journal of Law Management and Humanities, 7(4), 1038–1052. https://doij.org/10.10000/IJLMH.118109

McDevitt, J., Levin, J., & Bennett, S. (2022). Hate Crime Offenders: An Expanded Typology. Journal of Social Issues, 58(2).

Murphey, C. (2024). Understanding cybercrime. European Parliamentary Research Service.

Murthy, A. N. (2022). Psychological Theories and Criminal Bhaviour. Symbiosis Law School, Hydrabadh, 10.

Nidham Othman, S., Fadhil Alziboon, M., Dawood, M., Jameel Sachet, S., & Moroz, I. (2024). New rehabilitation against electronic crimes by young people. https://doi.org/10.5281/ZENODO.13732745

Nmeme, E., & Obiakor, N. (2024). Unpacking the Impact of Cybercrimes and Socio-Cultural Dimensional Developments in Nigeria. Journal of International Economic Relations and Development Economics, 4(1), 1-8

Obuobisa, M. Y. A. (n.d.). CHALLENGES FACED REGARDING CYBER CRIME AND THE RULE OF LAW IN CYBERSPACE FROM THE PERSPECTIVE OF A PROSECUTOR IN GHANA.

Office, M. P. P. (n.d.). GUIDELINES TO FIGHT CYBERCRIMES AND PROTECT VICTIMS.

Oyenuga, A. (n.d.). "LUCRATIVE AND HIDDEN": FACTORS INFLUENCING CYBERCRIME INVOLVEMENT AMONG YOUTH IN METROPOLITAN LAGOS.

Parewa, D. K., & Mordia, D. D. (n.d.). Trends and Patterns: Analysing Cybercrime Statistics in India.

Raj, S., & Singh, D. V. (2024). Exploring Psychological Triggers and Vulnerabilities Leading to Digital Arrests in Cybercrime Cases: A Comparative Study in Uttar Pradesh. 14(4).

Sarmah, A., Sarmah, R., & Baruah, A. J. (n.d.). A brief study on Cyber Crime and Cyber Law's of India. 04(06).

Shinder, D. L., & cross, M. (n.d.). Scene of the cybercrime (2nd ed.). Elsevier.

Smith, C. D. (2023). "The Thrill of It": An Examination of Environmental and Individual Antecedents of Thrilling Perceptions of Criminal Behavior. UNIVERSITY OF CALIFORNIA.

Sultana, Arifa (2024).A short note on Theories of Cyber Crime.(Ibrahim et al., n.d.)

The Economics of Civil Justice: New Cross-country Data and Empirics (OECD Economics Department Working Papers). (2013). Organisation for Economic Co-Operation and Development (OECD). https://doi.org/10.1787/5k41w04ds6kf-en

Tiwari, S., Rai, S. K., & Sisodia, V. (2023). Analysis of Cybercrime against Indian Youth on Social Media. 13(4).

Van De Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. Cyberpsychology, Behavior, and Social Networking, 20(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Varshney, M., Kumar, A., Ganguli, R., Umer, S., Sonkar, S. S., & Molla, N. (2023). Ethical Hacking: Enhancing Cybersecurity Through Offensive Security Practices. 44(4).