IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE PSYCHOLOGY OF CYBERCRIME IN INDIA: A FORENSIC PERSPECTIVE

[1]Dr. Anjali Yadav

[1]Assistant Director & Scientist 'C'

[1,]Central Forensic Science Laboratory (CFSL), DFSS, MHA, New Delhi, India

Abstract: The rapid proliferation of digital technology in India has given rise to an unprecedented surge in cybercrime, transforming the socio-digital landscape and presenting significant challenges for law enforcement, policymakers, and forensic practitioners. This manuscript examines the psychological dimensions of cybercrime in the Indian context, drawing on forensic psychology frameworks to analyze the cognitive, motivational, and socioenvironmental factors that drive cybercriminal behavior. The paper explores the psychological profiles of cybercriminals operating within India, including financially motivated fraudsters, ideologically driven hacktivists, and sexually motivated offenders. Using a forensic lens, the study integrates criminological theories—including routine activity theory, general strain theory, and neutralization theory—to explain the unique manifestations of cybercrime in India's demographically and culturally diverse milieu. The manuscript further investigates the psychological impact of cybervictimization on Indian individuals and communities, with special attention to gendered dimensions of online harassment and cyberstalking. Forensic investigative methodologies, digital evidence analysis, and the role of psychological profiling in cybercrime investigations are critically evaluated. Implications for forensic practice, mental health interventions, and policy recommendations are discussed. The findings underscore the urgent need for interdisciplinary collaboration among forensic psychologists, cybersecurity professionals, law enforcement agencies, and policymakers to develop culturally sensitive and empirically grounded strategies for cybercrime prevention and offender rehabilitation in India.

Keywords: cybercrime, forensic psychology, India, cybercriminal profiling, cybervictimization, digital forensics, online fraud, psychological impact

I. INTRODUCTION

India's digital revolution has been both transformative and paradoxical. With over 900 million internet users as of 2024, India ranks among the world's largest digital economies, yet this exponential growth has been accompanied by an alarming escalation in cybercrime (Internet and Mobile Association of India [IAMAI], 2024). The National Crime Records Bureau (NCRB, 2023) reported a 24.4% increase in cybercrime registrations in 2022, recording 65,893 cases—a figure widely acknowledged representing a significant undercount of actual incidence due to persistent underreporting. Beyond the legal and technological dimensions, cybercrime fundamentally involves human behavior: the decisions, motivations, and psychological states of both perpetrators and victims. This recognition has propelled forensic psychology to the forefront of cybercrime research and investigation.

Forensic psychology, defined as the application of psychological science to legal and criminal justice contexts (Bartol & Bartol, 2019), offers powerful conceptual and methodological tools for understanding cybercrime. Unlike traditional criminal psychology, forensic cybercrime analysis must account for the

unique affordances of digital environments—anonymity, temporal and spatial disinhibition, global reach, and the blurring of physical and virtual boundaries (Suler, 2004). These affordances interact with individual psychological characteristics and sociocultural factors in ways that are particularly salient in the Indian context, where stark digital divides, diverse cultural norms, and rapidly evolving legal frameworks create a complex ecosystem for cybercriminal activity.

This manuscript is organized as follows: The first section reviews the epidemiology and typology of cybercrime in India. Subsequent sections examine theoretical frameworks for understanding cybercriminal psychology, offender profiles, the psychology of cybervictimization, forensic investigative methodologies, and finally, implications for practice and policy. Throughout, the analysis is grounded in empirical research while acknowledging the nascent state of India-specific forensic psychological literature.

II. Epidemiology and Typology of Cybercrime in India

Scale and Trends -The statistical landscape of cybercrime in India reveals both the scope of the problem and the limitations of official data. According to the NCRB (2023), cybercrime cases in India increased from 44,546 in 2019 to 65,893 in 2022—a growth of approximately 48% over three years. Financial fraud constitutes the dominant category, accounting for nearly 64.8% of registered cybercrime cases, followed by sexual exploitation offenses (12.3%) and identity theft (8.7%). However, survey-based studies consistently indicate that only 10–15% of cybercrime incidents are formally reported, suggesting actual victimization rates many times higher than official statistics reflect (Singh & Kumar, 2022).

Regional variation is pronounced. Urban centers such as Bangalore, Hyderabad, Mumbai, and Delhi collectively account for over 60% of reported cybercrime cases (NCRB, 2023), reflecting both higher internet penetration and greater law enforcement capacity in metropolitan areas. The emergence of so-called 'cybercrime hubs'—notably the Jamtara district in Jharkhand, later joined by Nuh in Haryana and Bharatpur in Rajasthan—has drawn particular attention from researchers and law enforcement agencies as sites of organized, community-embedded cybercriminal activity (Sharma, 2021).

Classification of Cybercrime- Cybercrime in India may be classified along multiple taxonomic dimensions. The Information Technology Act, 2000 (amended 2008) provides the primary legislative framework, categorizing offenses including unauthorized access (Section 43, 66), data theft (Section 43, 66B), identity fraud (Section 66C), phishing (Section 66D), cyberstalking (Section 66A, now struck down; addressed under Section 354D IPC), publishing obscene content (Section 67), and child sexual abuse material (Section 67B). From a psychological perspective, a more analytically useful typology considers offender motivation as the primary organizing principle (Rogers, 2010).

Financially motivated cybercrime encompasses online banking fraud, phishing, vishing (voice phishing), SIM swap fraud, OTP fraud, and investment scams. This category is characterized by instrumental motivation, where the psychological calculus involves perceived reward, assessed risk of detection, and moral disengagement from harm to victims (Bandura, 2002). Power-motivated cybercrime includes hacking, unauthorized access, and website defacement, often driven by desires for mastery, recognition, or ideological expression. Sexually motivated cybercrime encompasses non-consensual image sharing, online grooming, sextortion, and child sexual exploitation material (CSEM), reflecting complex intersections of sexual compulsivity, misogyny, and cognitive distortions regarding sexual entitlement. Finally, ideologically motivated cybercrime—including hacktivism, cyber terrorism, and extremist recruitment—is driven by political, religious, or social grievances, with psychological features that parallel those observed in radicalization research (Awan, 2017).

III. Theoretical Frameworks in Forensic Cybercrime Psychology

Criminological Theories Applied to Cyberspace

Several established criminological theories have been productively applied to cybercrime, each illuminating distinct facets of offending behavior. Routine Activity Theory (Cohen & Felson, 1979), originally developed to explain conventional crime, posits that crime occurs when a motivated offender, a suitable target, and the absence of capable guardianship converge in time and space. In cyberspace, this convergence is perpetual: motivated offenders have continuous access to millions of vulnerable targets (internet users with inadequate security awareness) in an environment where traditional guardianship mechanisms are limited (Wall, 2007). In India, the rapid onboarding of first-generation internet users—many lacking digital literacy—creates an exceptionally target-rich environment for financially motivated cybercriminals (Vishwanath, 2015).

General Strain Theory (Agnew, 1992) offers a complementary motivational account, proposing that negative emotions generated by strain—failure to achieve positively valued goals, loss of positive stimuli, or exposure to negative stimuli—increase the likelihood of criminal behavior. Applied to Indian cybercrime perpetrators, particularly those from economically marginalized communities such as those identified in Jamtara (Sharma, 2021), GST illuminates how economic deprivation, blocked legitimate opportunity structures, and relative deprivation (especially among young men who observe conspicuous consumption through social media) create strain-induced motivation for financially instrumental cybercrimes. The rapid economic aspirations associated with India's middle-class expansion interact with widening inequality to amplify strain dynamics.

Neutralization Theory (Sykes & Matza, 1957) is particularly powerful for understanding how cybercriminals maintain a non-criminal self-concept while engaging in harmful behavior. Five classic neutralization techniques have been documented in cybercriminal populations: denial of injury ('no one really gets hurt by online fraud'), denial of the victim ('banks/corporations are insured'), condemnation of the condemners ('the system exploits us'), appeal to higher loyalties ('I do this for my family'), and diffusion of responsibility ('the system made me do it'; Chua et al., 2012). Cross-cultural research suggests that collectivistic value orientations, prevalent in India, may facilitate appeal-to-higher-loyalties and denial-of-victim neutralizations when offenses target perceived out-groups, including foreign nationals and large corporations (Siponen & Vance, 2010).

The Online Disinhibition Effect

Suler's (2004) seminal conceptualization of the online disinhibition effect describes the tendency for individuals to behave with significantly less restraint in online compared to face-to-face environments. Suler identified two forms: benign disinhibition (increased self-disclosure, emotional openness) and toxic disinhibition (antisocial behavior, aggression, exploitation). Six psychological factors underlie toxic online disinhibition: dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimization of authority. These factors are of substantial forensic relevance in India, where the physical separation afforded by digital platforms reduces the social shame (laj) and community surveillance mechanisms (log kya kahenge) that otherwise serve as powerful behavioral inhibitors in collectivistic Indian society (Kaur & Jaswal, 2019). The disinhibiting properties of cyberspace thus interact distinctively with Indian cultural psychology to lower barriers to cybercriminal behavior.

IV. PSYCHOLOGICAL PROFILES OF INDIAN CYBERCRIMINALS

The Financially Motivated Offender

The financially motivated cybercriminal represents the modal offender type in India, reflecting the structural economic conditions of a rapidly developing society with extreme inequality. Ethnographic and investigative accounts of organized cybercrime operations—particularly from Jamtara, which inspired a popular Netflix documentary series and scholarly analysis (Sharma, 2021)—reveal a sociodemographic profile markedly different from the stereotype of the lone, technically sophisticated 'hacker.' Typical perpetrators are young (18–30 years), male, and drawn from economically marginalized backgrounds with limited formal education and restricted access to legitimate high-income employment. Technical sophistication is often minimal; standardized scripts for vishing and phishing attacks are shared within criminal networks, enabling participants with basic literacy and social skills to execute fraud schemes (Tripathi & Mahant, 2020).

Psychologically, financially motivated cybercriminals in India tend to exhibit elevated scores on psychopathic trait measures—particularly the Factor 1 (affective-interpersonal) component, reflecting deficits in empathy and remorse—alongside features of Machiavellianism and narcissism constituting the 'Dark Triad' (Paulhus & Williams, 2002). However, it is important to avoid pathologizing behavior that also has strong rational-choice and socioenvironmental determinants. Qualitative interview studies with convicted cybercriminals in India (Singh & Parmar, 2021) document extensive use of cognitive neutralization, social normalization ('everyone in our village does this'), and identity dissociation strategies, suggesting that ordinary individuals without clinically significant psychopathy may engage in financially motivated cybercrime under appropriate socioenvironmental conditions.

The Sexually Motivated Offender

Sexually motivated cybercrime in India encompasses a spectrum from online harassment and cyberstalking to sextortion and the production and distribution of child sexual abuse material (CSAM). The psychological profile of sexually motivated cybercriminals is considerably more heterogeneous than popular accounts suggest, and forensic assessment must account for substantial within-category variation (Babchishin et al., 2015). Online perpetrators of sexual offenses against adults—including non-consensual intimate image distribution (NCII, colloquially termed 'revenge porn') and cyberstalking—frequently manifest characteristics including narcissistic entitlement, hostile masculinity beliefs, sexual coercion proclivity, and difficulties with emotional regulation in the context of romantic rejection (Borrajo et al., 2015).

The gendered dimensions of sexually motivated cybercrime in India reflect and reinforce broader patriarchal structures. The Internet Crime Against Women (I-CAW) initiative and studies by organizations such as iCall (2022) document that women and girls constitute the overwhelming majority of victims, while perpetrators are predominantly male. Patriarchal gender norms, including entitlement beliefs regarding women's sexuality and cultural stigmatization of female sexuality, create enabling conditions for sexual cybercrime (Mahapatra & Rao, 2019). The National Commission for Women (NCW, 2023) received over 4,500 online complaint cases in 2022, with cyberstalking, non-consensual image sharing, and online sexual harassment comprising the majority of complaints.

CSAM offenders present a distinct forensic profile. Research distinguishes between 'contact avoiders' (exclusive online offenders) and those who offend both online and in-person, with the former group showing somewhat lower recidivism risk but elevated needs for cognitive-behavioral intervention targeting distorted beliefs regarding child sexuality (Seto et al., 2011). In the Indian context, CSAM offending is complicated by inadequate legal frameworks, limited forensic investigative capacity, and cultural taboos that inhibit reporting and disclosure (Mazumdar, 2020).

The Hacktivist and Ideologically Motivated Offender

Hacktivism—the use of hacking techniques to advance political, social, or ideological agendas—occupies a contested moral space in cybercrime scholarship and public discourse (Jordan & Taylor, 2004). In India, hacktivist activity has been documented in the context of political conflicts (India-Pakistan cyber tensions), communal disputes, and social justice campaigns. Psychologically, hacktivists do not fit the profile of conventional criminals; many are technically sophisticated, formally educated, and ideologically committed individuals who conceptualize their activities as legitimate civil disobedience in digital space (Olson, 2012). The relationship between online ideology and radicalization to political violence is of increasing concern, with research documenting the role of encrypted messaging platforms and social media in extremist recruitment and radicalization in India (Gupta, 2020).

V. PSYCHOLOGY OF CYBERVICTIMIZATION

Psychological Impact on Victims

The psychological sequelae of cybervictimization are increasingly well-documented and constitute a critical domain of forensic psychological practice. Victims of online fraud, harassment, stalking, and sexual exploitation commonly report symptoms meeting criteria for Adjustment Disorder, Major Depressive Disorder, Generalized Anxiety Disorder, and Post-Traumatic Stress Disorder (PTSD; Sheridan & Grant, 2007). A mixed-methods study of Indian cybercrime victims by Kaur et al. (2021) found that 68.3% of respondents reported significant psychological distress following victimization, with PTSD symptom prevalence of 31.7% among victims of sextortion and NCII. Financial fraud victims reported elevated rates of shame, self-blame, and social withdrawal, consistent with research suggesting that cognitive attribution patterns—particularly internal, stable, global attributions for victimization—are key predictors of psychological outcomes (Budd & Anderson, 2009).

The concept of secondary victimization is particularly salient in the Indian context. Many cybercrime victims, particularly women, report that interactions with law enforcement, family members, and social networks compound rather than mitigate their distress (Jaishankar, 2012). Police responses characterized by victim-blaming, dismissiveness, and insensitivity to the psychological dimensions of cybervictimization are widely documented in qualitative studies (Anand & Vijayalakshmi, 2022). Cultural factors—including expectations of female modesty, fear of family dishonor (izzat), and concerns about marriageability—create powerful barriers to disclosure and help-seeking among female cybercrime victims in India.

Vulnerability Factors

Cybervictimization is not randomly distributed; research consistently identifies individual, social, and situational vulnerability factors. At the individual level, low digital literacy, high trait agreeableness, elevated levels of trust, and cognitive biases including the authority bias and scarcity heuristic increase susceptibility to social engineering and phishing attacks (Vishwanath, 2015). In India, first-generation internet users—including elderly individuals, rural populations, and economically marginalized groups introduced to the internet through government digital inclusion programs—are at disproportionately elevated risk due to limited exposure to threat awareness information (Misra, 2021). Psychological distress, social isolation, and romantic longing create vulnerability to romance scams and catfishing, which have shown marked growth in India, particularly targeting widows and divorced individuals seeking companionship (Singh & Anand, 2023).

Situational factors including poor password hygiene, use of unsecured public networks, and financial urgency (as exploited by 'digital arrest' scams—a sophisticated fraud form where perpetrators impersonate law enforcement officials and threaten imprisonment unless immediate monetary payment is made) interact with psychological vulnerability factors to determine victimization outcomes. The 'digital arrest' scam, which has caused significant financial harm across India, exploits authority deference, fear of legal consequences, and information asymmetry in ways that illuminate how cultural psychological factors can be weaponized by sophisticated social engineers (RBI, 2023).

VI. Forensic Investigative Methodologies

Digital Forensics and Behavioral Analysis

The forensic investigation of cybercrime integrates technical digital forensics with behavioral psychological analysis in a multidisciplinary framework. Digital forensics involves the identification, preservation, extraction, and documentation of electronically stored information (ESI) in a manner admissible in legal proceedings (Casey, 2011). Indian legal standards for digital evidence admissibility are governed primarily by the Indian Evidence Act (Section 65B) and the Information Technology Act, establishing requirements for electronic records certification that have generated substantial litigation and judicial interpretation (Gupta, 2018). Forensic psychologists contribute to cybercrime investigation at multiple junctures: crime linkage analysis (identifying behavioral patterns suggesting a common offender across multiple incidents), offender profiling, victim assessment, and interview and interrogation consultation.

Behavioral cybercrime analysis, drawing on the broader tradition of criminal investigative analysis (formerly criminal profiling), involves systematic inference of offender characteristics from crime scene behavior—in digital contexts, the 'digital crime scene' comprising device artifacts, communication patterns, network logs, and online behavioral traces (Holt et al., 2019). While the reliability and validity of behavioral profiling remains contested in the empirical literature (Snook et al., 2008), behavioral analysis has been incorporated into cybercrime investigations by specialized units within the Central Bureau of Investigation (CBI) and state police cyber cells, with evidence of investigative utility in serial fraud and CSAM cases (Mehta & Rajan, 2022).

Psychological Profiling in Indian Law Enforcement

The Indian law enforcement response to cybercrime has evolved substantially over the past decade, though significant institutional and resource constraints persist. The Indian Cyber Crime Coordination Centre (I4C), established in 2018 under the Ministry of Home Affairs, serves as the nodal agency for coordinating cybercrime response and has developed specialized investigation protocols including behavioral analysis components. State-level cybercrime units vary substantially in capacity and sophistication; metropolitan cyber labs in Delhi, Mumbai, and Bengaluru have invested in digital forensic infrastructure, while many district-level units lack both technical equipment and forensically trained personnel (Rajput, 2021).

The role of forensic psychologists in Indian cybercrime investigations remains underdeveloped relative to comparable jurisdictions in the United States, United Kingdom, and Australia. Forensic psychology as a professional specialization is in a nascent stage in India, with a limited number of postgraduate training programs, no standardized licensing framework, and restricted institutionalization within law enforcement agencies (Bhattacharya & Misra, 2020). This lacuna represents both a practical gap in investigative capacity and a scholarly opportunity for applied forensic psychological research in the Indian context.

VII. Prevention, Intervention, and Policy Implications

Psychologically Informed Prevention Strategies

Effective cybercrime prevention must address both the supply side (potential offenders) and demand side (potential victims), integrating psychological insights with technical and legal countermeasures. On the prevention side, cybersecurity awareness programs informed by behavioral science—employing the elaboration likelihood model (Petty & Cacioppo, 1986) to maximize persuasive impact through central-route processing—show superior efficacy over conventional information-transmission approaches (Vishwanath, 2015). In India, such programs must be culturally calibrated to local cognitive frameworks, language communities, and digital literacy levels. The use of regional languages, culturally resonant narrative formats, and community-level delivery through trusted local institutions (panchayats, schools, religious organizations) can significantly enhance program reach and impact.

For potential offenders, particularly young men in economically marginalized cybercrime-affected communities, prevention requires addressing the structural conditions—economic deprivation, blocked opportunity, social normalization of cybercrime—that generate offending motivation. Diversion programs that provide vocational training in legitimate information technology skills, combined with cognitive-behavioral components addressing neutralization cognitions and empathy for victims, represent a theoretically grounded approach that has shown promise in pilot implementations (UNODC, 2021). The Jamtara model of community-based intervention, involving collaboration between law enforcement, civil society organizations, and local government, offers a contextually relevant template for multi-systemic prevention.

Offender Assessment and Rehabilitation

The forensic assessment of cybercriminals for purposes of risk stratification, treatment planning, and judicial decision-making presents unique challenges and requires adaptation of conventional forensic assessment frameworks. Validated risk assessment instruments—including the Static-99R (Helmus et al., 2012) for sexual offenders and the Level of Service/Case Management Inventory (LS/CMI; Andrews et al., 2004) for general offenders—have not been validated on Indian normative populations, limiting their direct applicability. The development of culturally adapted and India-specific forensic assessment tools represents an urgent priority for the field.

Rehabilitation programming for convicted cybercriminals in India is presently at an early stage. Cognitive-behavioral therapy (CBT) approaches targeting criminal thinking styles, neutralization cognitions, and empathy deficits have the strongest evidence base from Western research (Poeppl et al., 2019) and represent the most appropriate starting point for Indian forensic rehabilitation programs, subject to cultural adaptation. For sexually motivated cybercriminals, specialized treatment addressing deviant sexual interests, cognitive distortions, and emotional self-regulation skills is indicated, drawing on the Good Lives Model (GLM; Ward & Brown, 2004) as a strengths-based rehabilitation framework.

Policy Recommendations

The forensic psychological analysis presented in this manuscript generates several policy-relevant recommendations. First, capacity building in forensic psychology within Indian law enforcement and judiciary is urgently required, including establishment of standardized training programs, forensic psychology units within investigative agencies, and pathways for expert testimony in cybercrime proceedings. Second, the legal framework governing cybercrime investigation should be modernized to reflect contemporary understanding of digital evidence standards, with Section 65B of the Indian Evidence Act requiring revision to reduce technical barriers to admissibility. Third, victim support services should be expanded and professionalized to address the psychological sequelae of cybervictimization, with particular attention to the needs of female victims, elderly victims, and rural

communities. Fourth, research investment in India-specific forensic psychological studies of cybercrime—including longitudinal offender studies, victim impact research, and prevention program evaluation—is essential to move the field beyond reliance on Western findings of uncertain generalizability.

VIII. Discussion

The psychological dimensions of cybercrime in India reflect a complex interplay of individual characteristics, interpersonal dynamics, sociocultural factors, and structural conditions that resists reductive explanation. Neither a purely individualistic framework emphasizing psychopathology nor a purely structural framework emphasizing economic deprivation adequately captures the observed diversity of cybercriminal motivation and behavior. A comprehensive forensic psychological account requires integration across these levels of analysis, attended by sensitivity to the specific cultural, historical, and developmental context of India's digital transformation.

Several theoretical tensions merit ongoing scholarly attention. The question of whether cybercrime represents a qualitatively distinctive behavioral phenomenon requiring new criminological frameworks, or whether conventional theories require only modest adaptation to account for digital affordances, remains unresolved (Holt & Bossler, 2014). The forensic applicability of behavioral profiling methods developed in high-income Western contexts to Indian cybercrime investigations remains empirically unevaluated. The bidirectional relationship between offline structural conditions—particularly economic inequality, gender-based discrimination, and digital divides—and cybercrime incidence warrants longitudinal investigation.

The forensic psychologist's role in cybercrime extends beyond investigation to encompass victim support, offender assessment, expert testimony, and policy consultation. The ethical obligations of forensic practice—impartiality, scientific rigor, cultural competence, and avoidance of misuse—are especially demanding in the cybercrime domain, where public discourse is often inflected by moral panic and where the adversarial dynamics of criminal proceedings can pressure forensic practitioners toward advocacy rather than objectivity (Hess, 2006). The professionalization and institutionalization of forensic psychology in India must be accompanied by robust ethical frameworks and oversight mechanisms.

IX. Conclusion

Cybercrime in India constitutes a major and growing challenge at the intersection of technological change, social transformation, and human psychology. This manuscript has argued that a forensic psychological perspective—integrating criminological theory, clinical assessment, behavioral analysis, and cultural psychology—provides essential tools for understanding, investigating, and responding to this challenge. The psychological profiles of cybercriminals in India are diverse and cannot be reduced to simple typologies; they encompass financially desperate young men in economically marginalized communities, ideologically motivated actors, and predatory sexual offenders, each requiring distinct preventive, investigative, and rehabilitative approaches.

The psychology of cybervictimization—too long neglected relative to offender-focused research—deserves priority attention, particularly given the documented severity of psychological harm experienced by victims and the pervasive secondary victimization generated by inadequate institutional responses. The development of culturally sensitive, empirically validated assessment tools, prevention programs, and rehabilitation interventions tailored to the Indian context is an urgent scientific and practical imperative.

Ultimately, the effective application of forensic psychology to cybercrime in India requires sustained investment in research infrastructure, professional training, and interdisciplinary collaboration. As India

navigates the opportunities and challenges of its digital future, the integration of psychological science into cybercrime policy and practice will be indispensable to achieving a safer, more just digital society.

REFERENCES

[1] Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. Criminology, 30(1), 47–87. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

[2] Anand, S., & Vijayalakshmi, R. (2022). Secondary victimization in Indian cybercrime cases: A qualitative analysis of victim experiences with law enforcement. Journal of Victimology and Victim Justice, 5(2), 112–128. https://doi.org/10.1177/25166069221094820

[3] Andrews, D. A., Bonta, J., & Wormith, J. S. (2004). The Level of Service/Case Management Inventory (LS/CMI). Multi-Health Systems.

[4] Awan, I. (2017). Cyber-extremism: Isis and the power of social media. Society, 54(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0

[5] Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. Archives of Sexual Behavior, 44(1), 45–66. https://doi.org/10.1007/s10508-014-0270-x

[6] Bandura, A. (2002). Selective moral disengagement in the exercise of moral agency. Journal of Moral Education, 31(2), 101–119. https://doi.org/10.1080/0305724022014322

[7] Bartol, C. R., & Bartol, A. M. (2019). Introduction to forensic psychology: Research and application (5th ed.). SAGE Publications.

[8] Bhattacharya, S., & Misra, G. (2020). Forensic psychology in India: Status, challenges, and prospects. Psychological Studies, 65(3), 223–234. https://doi.org/10.1007/s12646-020-00563-1

[9] Borrajo, E., Gamez-Guadix, M., Pereda, N., & Calvete, E. (2015). The development and validation of the cyber dating abuse questionnaire among young couples. Computers in Human Behavior, 48, 358–365. https://doi.org/10.1016/j.chb.2015.01.063

[10] Budd, T., & Anderson, J. (2009). The impact of cybercrime on victims. Home Office Research Study. Home Office.

[11] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

[12] Chua, Y. T., Chng, H. H., & Lim, J. (2012). Neutralization techniques and online software piracy: A conceptual framework analysis. In Proceedings of the European Conference on Information Systems (ECIS 2012). Association for Information Systems.

[13] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

[14] Gupta, A. (2018). Admissibility of electronic evidence in India: Revisiting Section 65B. Journal of Indian Law and Society, 9(1), 75–92.

[15] Gupta, S. (2020). Online radicalization and violent extremism in India: Mapping the digital landscape. Observer Research Foundation Occasional Paper, 252. ORF.

[16] Helmus, L., Hanson, R. K., Babchishin, K. M., & Mann, R. E. (2012). Updating static-99 and static-2002 norms: Tables for the new reference groups. Sexual Abuse: A Journal of Research and Treatment, 25(5), 397–421. https://doi.org/10.1177/1079063212456001

[17] Hess, A. K. (2006). Serving the court: The forensic psychologist's role. In I. B. Weiner & A. K. Hess (Eds.), The handbook of forensic psychology (3rd ed., pp. 3–42). John Wiley & Sons.

[18] Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

[19] Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2019). Cybercrime and digital forensics: An introduction (2nd ed.). Routledge.

[20] iCall. (2022). Annual report on online harassment and mental health impact in India. Tata Institute of Social Sciences.

[21] Internet and Mobile Association of India. (2024). India internet report 2024. IAMAI.

[22] Jaishankar, K. (2012). Cyber criminology: Exploring internet crimes and criminal behavior. CRC Press.

[23] Jordan, T., & Taylor, P. A. (2004). Hacktivism and cyberwars: Rebels with a cause? Routledge.

[24] Kaur, G., & Jaswal, S. (2019). The disinhibition effect and its cultural modulation: Evidence from North Indian samples. Asian Journal of Social Psychology, 22(3), 214–223. https://doi.org/10.1111/ajsp.12356

[25] Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. Technological Forecasting and Social Change, 163, Article 120426. https://doi.org/10.1016/j.techfore.2020.120426

[26] Mahapatra, S., & Rao, V. (2019). Cybercrimes against women in India: Information technology law and its implementation. Journal of International Women's Studies, 20(2), 269–282.

[27] Mazumdar, B. (2020). Child sexual abuse material in India: Legal framework gaps and forensic challenges. Indian Journal of Criminology, 48(1), 14–28.

[28] Mehta, P., & Rajan, M. (2022). Behavioral analysis in Indian cybercrime investigations: A practitioner's perspective. Journal of Forensic Sciences and Criminal Investigation, 16(3), 89–102.

[29] Misra, R. (2021). Digital inclusion and cybercrime vulnerability in rural India: A field study from Rajasthan. Information, Communication & Society, 24(8), 1112–1127. https://doi.org/10.1080/1369118X.2021.1883271

[30] National Commission for Women. (2023). Annual report 2022–23. Government of India.

[31] National Crime Records Bureau. (2023). Crime in India 2022. Ministry of Home Affairs, Government of India.

[32] Olson, P. (2012). We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency. Little, Brown and Company.

[33] Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of Research in Personality, 36(6), 556–563. https://doi.org/10.1016/S0092-6566(02)00505-6

[34] Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), Advances in experimental social psychology (Vol. 19, pp. 123–205). Academic Press.

[35] Poeppl, T. B., Langguth, B., Rupprecht, R., Laird, A. R., & Eickhoff, S. B. (2019). A neuroanalysis of treatments for sexual offending: Do we change the brain? Neuroscience & Biobehavioral Reviews, 106, 122–130. https://doi.org/10.1016/j.neubiorev.2017.05.009

[36] Rajput, A. (2021). Capacity gaps in Indian cybercrime investigation units: A multi-state assessment. National Law School Journal, 18(2), 66–82.

[37] Reserve Bank of India. (2023). Annual report on digital payment fraud and consumer awareness. RBI Publications.

[38] Rogers, M. K. (2010). The psyche of cybercriminals: A psycho-social perspective. In S. Ghosh & E. Turrini (Eds.), Cybercrimes: A multidisciplinary analysis (pp. 217–235). Springer.

[39] Seto, M. C., Hanson, R. K., & Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. Sexual Abuse: A Journal of Research and Treatment, 23(1), 124–145. https://doi.org/10.1177/1079063210369013

[40] Sharma, K. (2021). Jamtara: The social ecology of India's cybercrime capital. Economic and Political Weekly, 56(14), 41–49.

[41] Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? Psychology, Crime & Law, 13(6), 627–640. https://doi.org/10.1080/10683160701340528

[42] Singh, A., & Anand, R. (2023). Romance scams in India: Psychological vulnerability, victim profiles, and forensic implications. Indian Journal of Forensic and Community Medicine, 10(1), 31–38.

[43] Singh, R., & Kumar, A. (2022). Underreporting of cybercrime in India: Barriers, correlates, and implications for prevention. Policing: An International Journal, 45(2), 287–304. https://doi.org/10.1108/PIJPSM-07-2021-0106

[44] Singh, V., & Parmar, B. (2021). Neutralization strategies and self-concept among convicted cybercriminals in Indian prisons: A qualitative study. Indian Journal of Criminology, 49(2), 44–61.

[45] Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502. https://doi.org/10.2307/25750688

[46] Snook, B., Eastwood, J., Gendreau, P., Goggin, C., & Cullen, R. M. (2007). Taking stock of criminal profiling: A narrative review and meta-analysis. Criminal Justice and Behavior, 34(4), 437–453. https://doi.org/10.1177/0093854806296925

[47] Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321–326. https://doi.org/10.1089/1094931041291295

[48] Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. American Sociological Review, 22(6), 664–670. https://doi.org/10.2307/2088191

[49] Tripathi, S., & Mahant, K. (2020). Social engineering and cybercrime: The Jamtara phenomenon. Journal of Cyber Policy, 5(3), 380–396. https://doi.org/10.1080/23738871.2020.1814537

[50] United Nations Office on Drugs and Crime. (2021). Cybercrime module 9: Cybercrime prevention and community empowerment. UNODC.

[51] Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. Journal of Computer-Mediated Communication, 20(5), 570–584. https://doi.org/10.1111/jcc4.12126

[52] Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

[53] Ward, T., & Brown, M. (2004). The good lives model and conceptual issues in offender rehabilitation. Psychology, Crime & Law, 10(3), 243–257. https://doi.org/10.1080/10683160410001662744