International Journal of English Literature and Social Sciences
Vol-11, Issue-4; Jul-Aug, 2026

Peer-Reviewed Journal
Journal Home Page Available: https://ijels.com/
Journal DOI: 10.22161/ijels

Mirroring the Offline World: An Integrated Conceptual Framework of Cybercrime Perpetration and Victimization in Online Media

Arun R. S.[1], Dr. Uthara Soman[2]

[1]Research Scholar, Loyola College of Social Sciences, Kerala, India
[2]Assistant Professor of Sociology and Research Officer, Kerala State Higher Education Council, Kerala, India

Received: 09 Jun 2026; Received in revised form: 27 Jul 2026; Accepted: 29 Jul 2026; Available online: 02 Aug 2026

Abstract— *Cybercrime does not emerge in isolation from society; rather, it reflects and replicates existing social, economic, and cultural conditions of the physical world within online environments (Wall, 2007). While cyberspace alters the scale, speed, and anonymity of offenses, the underlying human motivations—such as financial gain, power, revenge, and exploitation—remain largely unchanged (Grabosky, 2001). In India, this menace has escalated dramatically, transitioning from minor web defacements and identity thefts during the early e-commerce and UPI boom into a massive multi-billion-dollar threat dominated by complex cross-border financial frauds, aggressive "digital arrest" scams, and AI-driven extortion (NCRB, 2023). Despite diligent law enforcement interventions, the staggering financial toll and skyrocketing incident rates underscore the urgent need for a deeper, more structured understanding of digital offenses, particularly within highly vulnerable and gendered sectors of cyber abuse, such as cyberbullying, cyberstalking, and online harassment (Devika et al., 2019; IT for Change, 2019). Despite a growing body of literature, contemporary cybercrime research remains highly fragmented, frequently analyzing perpetrator motivations or victim vulnerabilities in isolation (Holt & Bossler, 2014). This academic separation obscures the dynamic, interactive process through which cybercrimes actually occur. Addressing this critical gap, this paper develops a comprehensive, integrated conceptual framework that synthesizes established criminological, sociological, and communication theories to explain cybercrime as a fluid interplay between offenders, targets, and technological contexts. Crucially, the framework positions the online media environment as a vital mediating and contextual variable. It explores how platform-specific structural features, such as user anonymity, rapid accessibility, algorithmic amplification, and weak architectural guardianship, facilitate harmful intersections between motivated offenders and suitable targets (Yar, 2005). By bridging these disparate dimensions, the proposed model maps the convergence of perpetrator traits and victim lifestyles into four distinct digital outcomes: financial loss, severe psychological harm, reputational damage, and systemic privacy violations. Ultimately, this paper provides a robust theoretical foundation to guide future empirical research, while offering actionable, evidence-based insights for policymakers, educational curricula, and platform providers to design user-centered safety features and proactive risk-reduction strategies.*

Keywords— ***Cybercrime, Integrated Theoretical Framework, Perpetrator Motivations, Victim Vulnerability, Routine Activity Theory, Online Media Platforms, Digital Literacy, Cyber Harassment, Financial Fraud, India.***

I. INTRODUCTION

It is often observed that patterns of crime present in the physical world are replicated within online environments (Wall, 2007). Cybercrime does not emerge in isolation from society; rather, it reflects existing social, economic, and cultural conditions. Countries with higher levels of fraud, corruption, harassment, organized crime, or financial offences frequently experience similar forms of misconduct in cyberspace (Grabosky, 2001). The internet provides new tools and opportunities for offenders, but the underlying motivations, such as financial gain, power, revenge, or exploitation remain largely unchanged. Consequently, online fraud mirrors traditional fraud, cyber stalking resembles offline harassment, and digital theft parallels conventional property crimes (Jaishankar, 2011). While cyberspace alters the scale, speed, and anonymity with which offences can be committed, it does not fundamentally transform the social factors that contribute to criminal behaviour. Therefore, online crime should be understood not merely as a technological problem but as an extension of broader societal patterns, inequalities, and criminal practices that already exist in the offline world.

India has also felt the brunt of this menace after a certain point of time. Cybercrime in India has surged dramatically and evolved in complexity, growing from a few lakh incidents a decade ago into a massive multi-billion-dollar threat today (NCRB, 2023). The landscape is currently dominated by online financial frauds, aggressive "digital arrest" scams, and AI-driven extortion, primarily operated by cross-border syndicates rather than isolated hackers (I4C, 2024). From basic defacements and identity thefts and ecommerce and upi boom to the dark web and cyber crime as a service, the current evolution has been equally staggering as the IT boom that started in India in 1990s. The current statistics suggest that India is facing severe financial losses amounting to over ₹22,000 crore despite diligent police interventions (MHA / I4C, 2024). This paper works into the gendered sector of cyber crimes and seeks to find a common theoretical framework for understanding the psyche of perpetrators and victims (Devika et al., 2019; Gurumurthy et al., 2019).

The most common methods of cyber abuse have been reported as cyber bullying, identity theft, phishing, online fraud, and harassment (Holt & Bossler, 2014). Understanding both cybercrime perpetrators and victims is essential for developing a comprehensive explanation of cybercrime in online environments. Much of the existing literature tends to focus either on offender motivations or victim vulnerabilities in isolation. However, cybercrime is a dynamic process that involves interactions between offenders, targets, and technological contexts (Yar, 2005). Examining perpetrators helps researchers identify the social, psychological, and economic factors that motivate cybercriminal behavior, including anonymity, financial incentives, and peer influence (Akers, 1998; Rogers, 2006). At the same time, studying victims provides insight into the characteristics, online behaviors, and situational factors that increase susceptibility to cyberattacks (Hindelang et al., 1978). Integrating both perspectives enables a more holistic understanding of how cybercrimes occur and persist across digital platforms. Such an approach also contributes to the development of more effective prevention strategies, cyber security policies, and educational interventions aimed at reducing both offending and victimization. Therefore, a theoretical framework that incorporates the experiences and behaviors of both perpetrators and victims offers a stronger foundation for cybercrime research and policy formulation.

Despite the growing body of cybercrime research, much of the existing literature examines either offender motivations or victim vulnerabilities in isolation. Consequently, there remains a limited understanding of how these dimensions interact within online media environments. The absence of an integrated theoretical framework restricts the ability to explain cybercrime as a dynamic process shaped by the interplay of perpetrator characteristics, victim behaviors, and platform-specific factors. Addressing this gap is essential for developing a more comprehensive understanding of cybercrime in digital spaces. The purpose of this paper is to develop an integrated conceptual framework for understanding cybercrime in online media by synthesizing theories related to offender behavior, victimization, and digital environments. Specifically, the paper seeks to examine how perpetrator motivations, victim vulnerabilities, and the structural characteristics of online platforms interact to create opportunities for cybercrime. By bridging fragmented theoretical perspectives, the proposed framework aims to provide a comprehensive foundation for future research, policy development, and cybercrime prevention strategies.

Research Questions

1. To examine the major theoretical perspectives that explain cybercrime perpetration in online media environments.
2. To analyze the key theories of cybercrime victimization and identify factors that increase vulnerability to online victimization.
3. To explore the relationship between offender motivations, victim characteristics, and the structural features of online media platforms.
4. To synthesize existing criminological, sociological, and communication theories into an

integrated conceptual framework for understanding cybercrime.

5. To propose a theoretical model that can guide future empirical research and inform cybercrime prevention strategies.

II. METHODOLOGY

This paper employs a qualitative conceptual synthesis (Jabareen, 2009) to develop an integrated theoretical framework for understanding cybercrime. Rather than gathering primary empirical data, the methodology involves systematically reviewing and intersecting fragmented criminological, sociological, and communication theories. It separates these theories into independent variables (perpetrator motivations like financial gain or revenge) and dependent variables (victim characteristics and outcomes). By utilizing Routine Activity Theory (Cohen & Felson, 1979) as an analytical bridge, the paper models how the structural features of online environments—such as anonymity, algorithmic amplification, and weak architectural guardianship—act as critical mediating factors (Yar, 2005). This synthesis results in a unified conceptual model designed to guide future empirical testing and evidence-based policymaking.

III. ANALYSIS

Perpetrators' POV (Independent Variables)

From the perpetrators' point of view, several theoretical perspectives have been employed to explain cybercrime perpetration in online media. **Routine Activity Theory** (Cohen & Felson, 1979) suggests that cybercrime occurs when motivated offenders encounter suitable targets in the absence of effective guardianship, such as cybersecurity measures or platform oversight. **Social Learning Theory** (Bandura, 1977; Akers, 1998) explains cybercriminal behavior as a learned process acquired through observation, interaction, and reinforcement within online communities and networks. **General Strain Theory** (Agnew, 1992) posits that experiences of stress, frustration, or perceived injustice may motivate individuals to engage in cyber offending as a coping mechanism. **Rational Choice Theory** (Cornish & Clarke, 1986) further emphasizes that offenders make calculated decisions by evaluating the potential rewards and risks associated with cybercrime. Collectively, these theories highlight the psychological, social, and situational factors that contribute to cybercriminal behavior and provide a foundation for an integrated theoretical framework.

The proposed framework identifies online platform characteristics, lack of guardianship/security, and digital literacy levels as key mediating factors that influence the relationship between cybercrime perpetrators and victims. Online platform characteristics, including anonymity, accessibility, algorithmic visibility, and communication features, can create opportunities that facilitate cybercriminal activities and increase victim exposure to risk (marwick & boyd, 2011). Similarly, the absence of effective guardianship mechanisms, such as cybersecurity safeguards, content moderation, privacy protections, and user monitoring, reduces barriers to offending and enhances the likelihood of victimization (Yar, 2005). Digital literacy levels further mediate cybercrime outcomes by shaping individuals' ability to recognize threats, adopt protective behaviors, and respond effectively to online risks (Hargittai, 2002). Consequently, these mediating factors determine how offender motivations and victim vulnerabilities interact within online media environments, ultimately influencing the occurrence and severity of cybercrime incidents.

Victim's Perspective

From the perspective of a victim, the literature suggests that several theoretical perspectives have been used to explain cybercrime victimization in online media environments. **Lifestyle Exposure Theory** (Hindelang et al., 1978) suggests that individuals who engage in high-risk online activities, such as extensive social media use or interactions with unknown users, face greater risks of victimization. **Victim Precipitation Theory** (Wolfgang, 1958; Amir, 1971) posits that certain behaviors, although often unintentional, may increase an individual's vulnerability to cybercrime. **Routine Activity Theory** (Cohen & Felson, 1979) explains victimization as a consequence of exposure to motivated offenders in the absence of effective guardianship, such as cybersecurity awareness or protective technologies. The **Online Disinhibition Effect** (Suler, 2004) further highlights how anonymity and reduced social constraints in digital environments can facilitate harmful interactions between offenders and victims. Collectively, these theories emphasize the role of individual behavior, online routines, and digital environments in shaping cybercrime victimization.

The online media environment constitutes a critical contextual factor within the proposed conceptual framework, shaping interactions between cybercrime perpetrators and victims:

- **Anonymity:** Enables users to conceal their identities, reducing accountability and increasing opportunities for cybercriminal activities (Suler, 2004).
- **Accessibility:** Refers to the ease with which individuals can connect, communicate, and access information across digital platforms, thereby

expanding both opportunities for offending and exposure to victimization (Wall, 2007).

- **Weak Guardianship:** Encompasses inadequate cybersecurity measures, limited platform monitoring, and insufficient regulatory oversight, which diminish barriers to cybercrime (Yar, 2005).
- **Platform Features:** Such as instant messaging, content sharing, recommendation algorithms, and large-scale networking capabilities, further influence user behavior and may facilitate harmful interactions (Marwick & boyd, 2011).

Collectively, these environmental factors create conditions that can either enable or constrain cybercrime, thereby affecting the likelihood and consequences of victimization in online media spaces.

Comparative Theoretical Synthesis

A comparative analysis of theories related to cybercrime perpetration and victimization reveals that cybercrime is best understood as the outcome of interactions between offender motivations, victim vulnerabilities, and digital environments. Perpetrator-oriented theories, such as Social Learning Theory (Akers, 1998), General Strain Theory (Agnew, 1992), and Rational Choice Theory (Cornish & Clarke, 1986), primarily explain why individuals engage in cybercrime by emphasizing learned behavior, social pressures, and cost-benefit calculations. In contrast, victim-oriented theories, including Lifestyle Exposure Theory (Hindelang et al., 1978) and Victim Precipitation Theory (Wolfgang, 1958), focus on the factors that increase an individual's susceptibility to victimization. Routine Activity Theory (Cohen & Felson, 1979) serves as a bridge between these perspectives by highlighting the convergence of motivated offenders, suitable targets, and inadequate guardianship. Similarly, the Online Disinhibition Effect (Suler, 2004) explains how the anonymity and reduced social constraints of online environments shape the behavior of both offenders and victims. Taken together, these theories suggest that cybercrime emerges from the dynamic interplay of individual motivations, victim characteristics, and the structural features of digital platforms, thereby supporting the need for an integrated theoretical framework.

Proposed Conceptual Model

The proposed conceptual model conceptualizes cybercrime in online media as the outcome of interactions among offender motivations, victim characteristics, and environmental factors. Offender motivations are shaped by factors such as financial gain, revenge, ideological beliefs, curiosity, social influence, and perceived anonymity (Rogers, 2006). Victim characteristics include digital literacy, online lifestyle, privacy practices, risk awareness, and the extent of online engagement (Hargittai, 2002; Holt & Bossler, 2014). These factors operate within online media environments characterized by anonymity, accessibility, weak guardianship, algorithmic amplification, and extensive opportunities for social interaction.

Drawing on Routine Activity Theory (Cohen & Felson, 1979), cybercrime is most likely to occur when a motivated offender encounters a suitable target in the absence of effective guardianship. Social Learning Theory, General Strain Theory, and Rational Choice Theory explain offender behavior, while Lifestyle Exposure Theory, Victim Precipitation Theory, and the Online Disinhibition Effect explain victim vulnerability. The model proposes that cybercrime emerges from the convergence of offender motivations and victim vulnerabilities within enabling online environments, resulting in outcomes such as financial loss, privacy breaches, reputational damage, and psychological harm.

Proposed Conceptual Framework Elements

Perpetrator-Related Independent Variables

The proposed framework identifies several perpetrator-related factors as independent variables influencing cybercrime behavior in online media environments:

- **Motivation:** Refers to the underlying psychological or social drivers that encourage individuals to engage in cybercrime, including revenge, curiosity, ideological beliefs, or personal gratification (Agnew, 1992).
- **Technical Skills:** Represent the knowledge and competencies required to exploit digital systems, conduct cyberattacks, or evade detection (Rogers, 2006).
- **Anonymity:** Reflects the perceived ability to conceal one's identity online, thereby reducing fear of punishment and increasing opportunities for offending (Suler, 2004).
- **Peer Influence:** Encompasses the impact of online communities, social networks, and deviant groups that may encourage or reinforce cybercriminal behavior (Akers, 1998).
- **Economic Incentives:** Refer to the anticipated financial rewards associated with cybercrime, such as fraud, extortion, identity theft, or data exploitation (Cornish & Clarke, 1986).

Collectively, these variables shape the likelihood and nature of cybercrime perpetration within online media environments.

Four Major Outcomes of Victimization

The proposed framework identifies four major outcomes of cybercrime victimization in online media:

1. **Financial Loss:** Refers to the monetary damages suffered by victims through online fraud, identity theft, phishing attacks, ransomware, or unauthorized financial transactions (NCRB, 2023).
2. **Psychological Harm:** Encompasses the emotional and mental consequences of cybercrime, including stress, anxiety, fear, humiliation, depression, and diminished trust in online interactions (Devika et al., 2019).
3. **Reputational Damage:** Occurs when false information, private content, or defamatory material is disseminated online, negatively affecting an individual's social standing, professional opportunities, or personal relationships (Citron, 2014).
4. **Privacy Violations:** Involve the unauthorized access, collection, disclosure, or misuse of personal information, resulting in a loss of control over sensitive data (Solove, 2006).

These outcomes represent the primary consequences of cybercrime and demonstrate the multifaceted impact of digital victimization on individuals in online media environments.

IV. CONCLUSION

In conclusion, studying cybercrime perpetrators and victims together provides a more comprehensive understanding of cybercrime in online media environments. While perpetrator-oriented theories explain the motivations, skills, and opportunities that facilitate offending (Akers, 1998; Cornish & Clarke, 1986), victim-oriented theories highlight the behaviors and vulnerabilities that increase the risk of victimization (Hindelang et al., 1978). Examining these dimensions in isolation offers only a partial explanation of cybercrime. An integrated perspective reveals how offender motivations, victim characteristics, and online media environments interact to shape cybercrime incidents and outcomes (Yar, 2005). Consequently, a combined theoretical approach strengthens both academic understanding and the development of effective prevention, intervention, and cybersecurity strategies.

Cybercrime is a multifaceted phenomenon shaped by the interaction of individual, social, and technological factors. At the individual level, motivations, technical skills, and personal circumstances influence the likelihood of engaging in or becoming vulnerable to cybercrime. Social factors, including peer influence, online communities, and patterns of digital interaction, contribute to the normalization and diffusion of cybercriminal behavior. Technological factors, such as platform design, anonymity, accessibility, and cybersecurity safeguards, create opportunities and constraints that affect both offending and victimization. Therefore, understanding cybercrime requires a holistic perspective that recognizes the complex interplay of human behavior, social dynamics, and digital environments.

Theories such as Routine Activity Theory (Cohen & Felson, 1979), Social Learning Theory (Akers, 1998), and Lifestyle Exposure Theory (Hindelang et al., 1978) complement one another by explaining different yet interconnected dimensions of cybercrime. Social Learning Theory focuses on how cybercriminal behaviors are acquired and reinforced through interactions within online communities and social networks. Lifestyle Exposure Theory explains how individuals' online activities and behavioral patterns may increase their susceptibility to victimization. Routine Activity Theory bridges these perspectives by emphasizing that cybercrime occurs when a motivated offender encounters a suitable target in the absence of effective guardianship. Together, these theories provide a comprehensive framework that accounts for offender motivations, victim vulnerabilities, and the environmental conditions that facilitate cybercrime in online media environments.

An integrated theoretical framework provides a more comprehensive understanding of cybercrime in online media by bringing together explanations of offender behavior, victim vulnerability, and the technological conditions that facilitate cybercrime. Rather than examining these dimensions in isolation, the framework recognizes cybercrime as a dynamic process arising from the interaction of individual motivations, social influences, online routines, and platform characteristics. This holistic perspective enhances the explanatory power of cybercrime research and offers a stronger foundation for developing prevention and intervention strategies. Future empirical studies should test and refine the proposed framework through quantitative surveys, qualitative interviews, and digital trace data analysis. Such research would enable scholars to evaluate the relationships among the framework's key variables and assess its applicability across diverse online media contexts.

The findings of this conceptual framework underscore the importance of translating theoretical insights into practical interventions. Policymakers should utilize these insights to develop evidence-based regulations and cybersecurity policies that address both offender behavior and victim protection. Educators can incorporate cybercrime awareness and digital literacy programs into educational

curricula to enhance users' ability to recognize and respond to online threats (Hargittai, 2002). Likewise, platform providers should strengthen security measures, improve content moderation, and implement user-centered safety features to reduce opportunities for cybercrime. By drawing upon established theories of perpetration and victimization, stakeholders can develop more effective prevention, awareness, and risk-reduction strategies that foster safer online media environments.

REFERENCES

[1] Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47–88.

[2] Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Northeastern University Press.

[3] Amir, M. (1971). *Patterns in Forcible Rape*. University of Chicago Press.

[4] Bandura, A. (1977). *Social Learning Theory*. Prentice-Hall.

[5] Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

[6] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.

[7] Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer-Verlag.

[8] Devika, J., Vijayakumar, C., Resmi, P. S., Mini, D. S., & Alexander, E. (2019). *Walking on Eggshells in Cyberspace: A Report on Gender Justice, Law Enforcement, and Women's Struggles and Negotiations in Malayali Cyberspace*. Centre for Development Studies (CDS) & IT for Change.

[9] Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243–249.

[10] Gurumurthy, A., Vasudevan, A., & Chami, N. (2019). *Born Digital, Born Free? A socio-legal study on young women's experiences of online violence in South India*. IT for Change.

[11] Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday*, 7(4).

[12] Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Ballinger.

[13] Holt, T. J., & Bossler, A. M. (2014). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

[14] Indian Cyber Crime Coordination Centre (I4C). (2024). *Annual Cyber Financial Fraud Assessment and Loss Estimates*. Ministry of Home Affairs, Government of India.

[15] IT for Change. (2019). *Gendering the Digital Public Sphere: Freedom of Expression and Violence Against Women in Cyberspace*.

[16] Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62.

[17] Jaishankar, K. (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. *CRC Press*.

[18] Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133.

[19] National Crime Records Bureau (NCRB). (2023). *Crime in India 2022: Statistics Volume II (Cyber Crimes)*. Ministry of Home Affairs, Government of India.

[20] Rogers, M. K. (2006). A two-tier model for cyberdeviancy. *International Journal of Cyber Criminology*, 1(1), 1–13.

[21] Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–560.

[22] Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321–326.

[23] Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

[24] Wolfgang, M. E. (1958). *Patterns in Criminal Homicide*. University of Pennsylvania Press.

[25] Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407–427.