GLOBUS

Globus Journal of Progressive Education
A Refereed Research Journal
Vol 15 / No 1 / Jan-Jun 2025 P - ISSN: 2231-1335, E- ISSN: 2582-7200

A STUDY ON SOCIAL AND PSYCHOLOGICAL DIMENSIONS OF CYBERCRIME BEHAVIOUR

*Km Shilpa
**Narendra Kumar Singh

Paper Received: 01.05.2025 / **Paper Accepted**: 22.05.2025 / **Paper Published**: 24.05.2025
Corresponding Author: Km Shilpa; doi: 10.46360/globus.edu.220251026

Abstract

The rise of cybercrime in the digital era cannot be understood solely through technological perspectives; it increasingly demands attention to the social and psychological forces shaping offender behaviour. This study explores the multifaceted behavioural dimensions that contribute to cyber offending, examining how motivation, identity, opportunity structures, online socialization, and cognitive biases interact within virtual environments. Drawing on criminological theories, behavioural psychology, and digital sociology, the paper analyzes factors such as anonymity, deindividuation, peer influence, and perceived risk reduction, which collectively enable individuals to engage in cybercrime with greater ease than traditional crimes. The study also highlights how socio-cultural contexts, including economic marginalization, online communities, and subcultural norms, influence both the initiation and escalation of cyber-offending pathways. The study discusses that effective cybercrime mitigation requires not only technological advancements but also deeper insight into the human factors driving deviant online behaviour.

Keywords: Cybercrime, Behavioural Psychology, Digital Sociology, Offender Motivation, Online Anonymity, Moral Disengagement, Social Influence, Cognitive Bias, Cyber Offending Patterns, Cyberpsychology.

Introduction

The rapid expansion of digital technologies has transformed not only how societies communicate, work, and transact, but also how criminal activities are conceived and executed. Cybercrime has emerged as one of the most pervasive global threats, exploiting the anonymity, speed, and borderless nature of digital environments. While much scholarly attention has focused on the technical mechanisms of cyberattacks, understanding the *human* element - specifically the social and psychological drivers behind cyber-offending - remains crucial for developing effective prevention and intervention strategies.

Cybercriminal behaviour cannot be explained merely through access to technological tools; it is deeply embedded in cognitive processes, emotional triggers, social influences, and environmental conditions.

The psychological dimensions of cybercrime encompass factors such as moral disengagement, rationalization, sensation-seeking, impulsivity, and cognitive distortions that enable individuals to justify or minimize the perceived harm of their actions. The online environment further amplifies these tendencies by providing anonymity, reduced accountability, and emotional detachment from victims. These conditions weaken traditional social inhibitors and create behavioural disinhibition, allowing offenders to act in ways they might avoid in face-to-face contexts.

Social factors also play a defining role in shaping cyber-offending pathways. Peer influence, online deviant communities, socio-economic pressures, and cultural norms significantly contribute to the normalization of cybercrime in digital subcultures. Platforms such as forums, dark web marketplaces, and encrypted communication networks create ecosystems where knowledge-sharing, identity formation, and group validation encourage sustained involvement in cybercrime. For some individuals, cyber-offending becomes not only a means of financial gain but also a source of status, belonging, and identity within these virtual networks.

**Research Scholar, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, Uttarakhand, India.*
***Research Supervisor, Maharaja Agrasen Himalayan Garhwal University, Shiv Nagar, Pokhra, Uttarakhand, India.*

Together, these social and psychological dimensions illustrate that cybercrime is a human behaviour shaped by complex interactions between individual traits and digital environments. Recognizing these dynamics is critical to formulating holistic responses that integrate technological safeguards with behavioural, educational, and socio-cultural interventions.

Review of Literature

Robles-Carrillo and García-Teodoro (2022) offer an interdisciplinary analysis of ransomware that directly links technical evolution of attacks with gaps in legal regulation. Their article in Security and Communication Networks shows how ransomware has become "almost pandemic" because of both advanced cryptographic techniques and the high impunity resulting from jurisdictional and regulatory weaknesses. The authors map the technical lifecycle of ransomware-from infection vectors and lateral movement to encryption and payment via cryptocurrencies-and then examine how existing criminal codes, computer-misuse laws and data-protection norms struggle to capture this complexity. They argue that many jurisdictions subsume ransomware under generic computer misuse, extortion or data-interference offences, which dilutes the specific harms and complicates sentencing. The paper proposes defining ransomware as an autonomous offence that explicitly reflects encryption-based coercion and large-scale economic disruption. It also stresses the need for harmonized rules on criminalizing ransom payment facilitation, regulating cryptocurrency exchanges that enable laundering of ransom proceeds, and strengthening obligations on organizations to implement preventive cybersecurity and incident reporting. By integrating technical and legal perspectives, the study demonstrates that effective ransomware control depends on joint development of security-by-design standards, forensic readiness, and specialized legal tools tailored to this attack model.

Focusing on the Internet of Things, Miniaoui et al. (2024) ask whether existing cybercrime laws meaningfully address emergent IoT security threats, using the UAE federal cybercrime law and RFID technology as a case study. Working within Security Journal, the authors combine doctrinal legal analysis with a technical mapping of RFID-based attack scenarios, such as cloning, skimming, denial-of-service and unauthorized tracking. They systematically compare concrete IoT attack vectors with the wording of cybercrime provisions and find partial but incomplete coverage: while broad clauses on "unauthorized access" and "interference with information systems" capture some behaviours, more subtle RFID abuses (e.g., covert tracking or data manipulation without system damage) fall into legal grey areas. The article argues that this mismatch creates enforcement uncertainty, weak deterrence and inconsistent application of sanctions. The authors recommend introducing technology-neutral but IoT-aware concepts-such as "unlawful manipulation of device identity," "unauthorized sensor data interception," and obligations for critical-infrastructure operators to harden RFID deployments-so that legislation keeps pace with ubiquitous computing. They also stress that IoT-specific cybercrime rules must be coordinated with data-protection, consumer-protection and telecommunications law to avoid regulatory overlap and loopholes. For regulators seeking to control cybercrime in smart-city and Industry 4.0 environments, this study illustrates how detailed threat modelling can be used to audit and update statutory frameworks.

At the level of regional regulation, Shaffique (2024) critically evaluates the European Union's proposed Cyber Resilience Act (CRA) as a response to systemic vulnerabilities in connected devices. Published in Computer Law & Security Review, the article argues that the CRA represents a major shift from post-incident liability towards ex-ante security obligations across the product lifecycle. By requiring manufacturers and developers of hardware, software and IoT products to implement secure-by-design measures, perform vulnerability assessments and maintain incident reporting, the regulation directly targets the technological roots of many cyber offences. However, through doctrinal and policy analysis, the author shows that the CRA's effectiveness will depend on how its broad security "essential requirements" are operationalized in harmonized technical standards and enforced by market-surveillance authorities. The paper warns that ambiguous terms, complex conformity-assessment procedures and uneven enforcement capacities across Member States may create compliance uncertainty and risk "checkbox" security. It also highlights tensions between strong security duties and innovation costs for SMEs, as well as possible overlaps with existing sectoral regimes like NIS2 and GDPR. Overall, Shaffique concludes that the CRA can significantly improve cybercrime prevention-especially for consumer IoT and industrial control systems-if accompanied by clear standards, realistic timelines and robust supervisory coordination. This analysis directly links regulatory design to the practical control of technologically mediated offences.

Analysis

Cybercrime is no longer a phenomenon driven solely by technological sophistication; it is increasingly shaped by human motivations, social structures, psychological mechanisms, and the behavioral affordances provided by digital environments. Understanding why individuals engage in cybercrime requires a nuanced analysis

that integrates insights from criminology, psychology, sociology, and cyber-behavioural science. This analysis examines the social and psychological factors influencing cyber-offending, emphasizing anonymity, moral disengagement, peer influence, cognitive biases, socio-economic pressures, and digital subcultures that facilitate deviant behaviour online.

1. Anonymity and Deindividuation in Cyberspace

One of the most powerful psychological drivers of cybercrime is the perception of anonymity. Digital spaces allow offenders to conceal their identity, evade real-world consequences, and dissociate their actions from their personal moral frameworks. This phenomenon, known as deindividuation, reduces self-awareness and weakens social restraints, making individuals more likely to violate norms.

The online environment fosters:

- reduced fear of punishment
- emotional distance from victims
- lower empathy due to lack of physical presence
- greater risk-taking behaviour

Anonymity thus transforms the cost–benefit calculation for offenders. What may seem morally unacceptable offline becomes psychologically permissible in cyberspace, where offenders perceive themselves as invisible actors operating beyond conventional societal boundaries.

2. Moral Disengagement and Cognitive Rationalization

Many cyber offenders rely on psychological mechanisms that allow them to justify or minimize the harm caused by their actions. According to Bandura's theory of moral disengagement, individuals reinterpret harmful behaviors in ways that align with their self-image.

Common rationalizations include:

- "There is no real victim" (especially in hacking, piracy, or financial fraud)
- "Everyone does it" (normalizing deviance)
- "Big companies can absorb the loss"
- "I am only testing their security" (self-justification)
- "It's harmless fun" (denial of consequences)

These rationalizations lower psychological barriers to deviant behaviour and create a cognitive environment in which cybercrime appears morally neutral or even justified.

3. Psychological Traits and Behavioural Predispositions

Cyber offenders often display certain psychological patterns that influence their decision-making:

a. Sensation-Seeking and Curiosity

Many novice hackers are driven by curiosity, thrill-seeking, or the desire for intellectual challenge. Cybercrime offers excitement and cognitive stimulation that some individuals struggle to find in everyday life.

b. Impulsivity and Low Self-Control

Routine Activity Theory and General Theory of Crime suggest that individuals with lower self-control are more likely to engage in digital deviance, especially crimes facilitated by instant access, such as phishing or online harassment.

c. Narcissism and Superiority Needs

Some offenders - particularly skilled hackers - engage in cybercrime to demonstrate dominance, technological mastery, or superiority over institutions and authorities.

d. Technological Self-Efficacy

Offenders with high confidence in their technical skills may feel empowered, perceiving cybercrime as low-risk and high-reward.

Together, these traits highlight the psychological diversity within cyber-offending populations, ranging from opportunistic amateur offenders to highly strategic, organized cybercriminals.

4. Peer Influence and Online Socialization

Cybercrime often develops within social contexts rather than in isolation. Online communities - forums, IRC channels, Telegram groups, dark web marketplaces - play a major role in reinforcing deviant behaviour.

These communities provide:

- technical knowledge-sharing
- moral support and normalization of offending
- status hierarchies based on skill and reputation
- collaboration opportunities for larger attacks
- access to illegal tools and services

Peer influence shapes offender identity, creating a subculture where illegal activities are celebrated, rewarded, and validated. Young offenders, in particular, are drawn into cybercriminal networks through social belonging, mentorship by senior hackers, and the promise of recognition.

5. Socio-Economic Pressures and Structural Motivations

Cybercrime is also influenced by broader socio-economic conditions. Individuals facing unemployment, poverty, limited opportunities, or social exclusion may turn to cybercrime as a means of economic survival. Key structural drivers include:

- global economic disparities
- youth unemployment in technologically skilled populations
- lack of legitimate opportunities in developing regions
- financial incentives and lucrative cybercrime markets

For many, cybercrime offers a level of financial return inaccessible through formal employment, especially in regions with significant digital skills but limited economic mobility.

6. The Role of Digital Subcultures and Identity Formation

Digital environments create unique cultural spaces that shape offender identity. These subcultures often possess:

- distinct norms and ethical codes
- collective identities ("hacktivists," "script kiddies," "carders," etc.)
- language, rituals, and hierarchies
- shared narratives against institutions or authority

Groups like Anonymous or various dark web collectives demonstrate how cybercrime can become intertwined with political expression, social protest, or ideological commitment. For such actors, cybercrime becomes not merely a deviant act but a symbolic performance of power, resistance, or belonging.

7. Reduced Perception of Harm and the Virtual Distance Effect

A critical psychological factor is the *virtual distance* between offender and victim. Unlike traditional crime, cybercrime often lacks:

- physical presence
- immediate emotional cues
- visible suffering
- direct confrontation

This distance weakens empathy and heightens the perception that cybercrime is victimless. Attackers may be unaware of the real human or economic consequences of data breaches, identity theft, or online harassment. The abstract nature of digital harm contributes to offenders underestimating the seriousness of their actions.

8. Online Disinhibition and Behavioural Amplification

John Suler's Online Disinhibition Effect explains why individuals behave differently (often more aggressively or impulsively) online. Key components include:

- dissociative anonymity
- invisibility
- asynchronicity
- solipsistic introjection (imagining others as fictional)
- minimized authority presence

These elements amplify deviant behaviour, encouraging individuals to engage in cyber stalking, trolling, hate speech, fraud, and other offences that they might avoid offline.

9. Cybercrime as a Learned Behaviour: Social Learning Theory

Cybercrime often spreads through mechanisms similar to traditional criminal learning:

- observational learning
- reward reinforcement
- imitation of peer models
- community validation

A novice cyber offender can rapidly progress into advanced roles by absorbing knowledge from experienced mentors in digital communities. Social Learning Theory thus explains the continuity and evolution of cyber-offending networks.

10. Implications for Cybercrime Prevention

Understanding the social and psychological roots of cybercrime suggests that technological solutions alone are insufficient. Effective prevention must integrate:

- behavioural profiling of offenders
- digital ethics education
- awareness campaigns targeting cognitive biases
- early intervention programs for youth
- strengthening digital communities that discourage deviance
- addressing socio-economic vulnerabilities

A holistic approach requires collaboration between psychologists, sociologists, criminologists, educators, and cybersecurity professionals.

Cybercrime is fundamentally a human behaviour shaped by psychological traits, social environments, structural pressures, and the affordances of digital technologies. Understanding these dimensions offers deeper insight into offender motivations and enables more sophisticated strategies for prevention, rehabilitation, and policy development. As technology continues to evolve, so too must our understanding of the human factors driving cyber-offending.

Conclusion

The evolution of cybercrime in the digital age highlights a fundamental truth: technological tools alone do not determine criminal behaviour; rather, cyber-offending is deeply rooted in complex social and psychological processes. This study underscores that understanding cybercrime requires moving

beyond a technical lens to analyze how individual traits, cognitive mechanisms, social interactions, and digital environments shape offender behaviour in meaningful and often predictable ways. The convergence of anonymity, reduced accountability, and the psychological distance afforded by cyberspace significantly alters how individuals perceive risk, responsibility, and harm. As a result, behaviours that would be restrained in physical contexts become easier to justify and execute in virtual environments.

Central to the psychological dimensions of cybercrime is the role of moral disengagement and cognitive rationalization. Offenders frequently downplay or deny the consequences of their actions, enabling them to commit harmful acts without compromising their moral self-image. Traits such as impulsivity, sensation-seeking, narcissism, and high technological self-efficacy further influence vulnerability to cyber-offending. These findings reveal that cybercrime is rarely the product of purely rational calculation; instead, it reflects cognitive distortions and emotional dynamics shaped by the unique affordances of digital spaces.

Social influences play an equally crucial role. Online communities, peer networks, and deviant subcultures serve as powerful enablers, providing not only technical knowledge but also moral validation and a sense of belonging. The normalization of cyber-offending within certain online ecosystems contributes to the escalation of harmful behaviours, particularly among youth who derive identity, status, or economic rewards from participation in such networks. Digital subcultures blur distinctions between play, exploration, and criminality, often leading individuals down pathways of deeper involvement in cybercrime.

Socio-economic pressures and structural inequalities further intensify cyber-offending motivations. For individuals facing unemployment, marginalization, or limited opportunities, cybercrime can appear as a viable - albeit illegal - alternative for economic survival. The global reach and scalability of cybercrime markets amplify these incentives, creating transnational networks that challenge conventional law enforcement approaches.

The analysis clearly indicates that effective cybercrime prevention cannot rely solely on technological defenses or punitive measures. Instead, it must incorporate behavioural science, social intervention, digital ethics education, and community-based strategies that address the root causes of cyber-offending. Early interventions targeting vulnerable youth, psychological support programs, socio-economic empowerment, and the promotion of prosocial online communities are essential components of a holistic response. Additionally, policies must recognize the role of empathy-building, moral reasoning, and digital literacy in reducing susceptibility to cybercrime involvement.

The social and psychological dimensions of cybercrime behaviour emphasize the need for an interdisciplinary approach to understanding and combating digital deviance. Recognizing cybercrime as a behavioural phenomenon shaped by human motivations and social contexts allows for more nuanced, sustainable, and ethical prevention frameworks. As technology continues to advance, addressing the human factors at the core of cybercrime will be critical for creating safer, more resilient digital societies.

Conflict of Interest

There is no conflict of interest by the authors in this manuscript.

References

1. Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. Mexican Law Review, 16(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892
2. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1), tyac014. https://doi.org/10.1093/cybsec/tyac014
3. Díaz-Pérez, L. C., Quintanar-Reséndiz, A. L., Vázquez-Álvarez, G., & Vázquez-Medina, R. (2022). A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology. Applied Computing and Informatics. Advance online publication. https://doi.org/10.1108/ACI-01-2022-0010
4. Miniaoui, S., Muammar, S., Muhammad, N., Al Muraqab, N., & Atalla, S. (2024). Do cybercrime laws address emergent IoT security threats? The case of UAE federal cybercrime law regarding RFID technology. Security Journal, 37(3), 1112–1122. https://doi.org/10.1057/s41284-023-00408-y
5. Robles-Carrillo, M., & García-Teodoro, P. (2022). Ransomware: An interdisciplinary technical and legal approach. Security and Communication Networks, 2022, Article 2806605. https://doi.org/10.1155/2022/2806605
6. Shaffique, M. R. (2024). Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? Computer Law & Security Review, 54, 106009. https://doi.org/10.1016/j.clsr.2024.106009

7. Ye, M., & Agarwal, N. (2024). Interplay of Family Dynamics and School Engagement in Self-Harm Adolescent: A Rapid Literature Review. The Family Journal.
8. Costa, F., & Ribeiro, A. (2021). Automated governance, digital policing and rights-based cyber law reform: A comparative legal study. European Journal of Digital Justice, 14(2), 143–170.
9. Delgado, M., & Torres, J. (2024). Why cybercrime convictions fail in the EU: Forensic traceability and evidentiary reform. Journal of Cyber Law & Governance, 6(1), 51–79.