The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 14, Issue 1, January- March, 2026
DIP: 18.01.227.20261401, DOI: 10.25215/1401.227
https://www.ijip.in

Research Paper

Cognitive-Behavioral Characteristics of Cyber Offenders: A Literature-Based Perspective

Penumarthi Gowtham Sai[1]*, Shaista Ahad[2]

ABSTRACT

Cyber offending has become a growing concern not only for cybersecurity professionals but also for researchers in forensic psychology. While a substantial body of work addresses the technological methods and legal implications of cybercrime, the psychological characteristics of cyber offenders themselves have received comparatively less detailed attention. This paper seeks to address that gap by reviewing recent research that examines the cognitive and behavioral features associated with cyber offending. which concentrates on key psychological elements commonly discussed in the literature, including cognitive distortions, moral disengagement, online disinhibition, decision-making biases, personality traits, and offender classifications. Studies were selected through a structured review of peer-reviewed publications, with emphasis placed on recent, relevant empirical and theoretical contributions. Across these studies, several consistent patterns emerge in how cyber offenders perceive their actions and make decisions. The findings point to recurring tendencies such as the use of rationalization and neutralization to justify behavior, reduced empathetic concern for victims, heightened sensation-seeking, excessive confidence in technical skills, and reliance on moral disengagement strategies. Offenders also frequently employ simplified decision-making processes that downplay potential harm and personal accountability. The discussion explores how these cognitive and behavioral tendencies interact rather than operate in isolation, and how they contribute to ongoing debates surrounding profiling, prevention, and offender management in cybercrime contexts. review concludes by outlining key implications and directions for future research. These include the need for longitudinal studies examining cognitive change over time, greater use of mixed-method designs that combine psychological assessment with digital behavior data, and more systematic evaluation of intervention strategies aimed at addressing distorted thinking patterns among cyber offenders. Overall, this review aims to deepen understanding of the psychological foundations of cyber offending and to support more informed approaches to law enforcement practice, threat assessment, and offender rehabilitation.

Keywords: *Cyber Offender Cognition, Moral Disengagement, Cognitive Distortions, Online Disinhibition, Offender Profiling*

[1]Research Scholar, Psychology, Shri Venkateshwara University.
[2]Assistant Professor, Psychology, Shri Venkateshwara University.
*Corresponding Author

Received: March 14, 2026; Revision Received: March 24, 2026; Accepted: March 28, 2026

Cybercrime includes phishing, hacking, identity theft, malware attacks, fraud, and online harassment. It continues to grow in size, complexity, and socio-economic impact. Despite improvements in cybersecurity and legal frameworks, many prevention methods fail because they overlook the psychological factors that drive offenders. Research on cybercrime has mainly focused on technical, legal, and organizational aspects. There has been less attention to the mental and behavioral factors behind those who commit cyber offenses. Understanding how offenders think is important not just for theory but also for practical uses like profiling, targeted deterrence, rehabilitation, and predicting risks.

Recent developments in criminology and forensic psychology show that cognitive distortions, moral disengagement, and decision-making biases are important in traditional crime. However, cyber offenses differ in their medium, anonymity, and the distance victims feel from the offenders. These factors introduce other psychological elements like online disinhibition and deindividuation. Yet, the current literature lacks a modern, comprehensive review of the cognitive-behavioral patterns linked to cyber offenders from the past 10 years.

This paper seeks to address that gap by reviewing empirical and theoretical studies published between 2015 to 2025. It will focus on offender thinking (e.g., rationalizations, distortions), behavioral traits (e.g., sensation-seeking, risk tolerance), moral disengagement processes, decision-making shortcuts in digital crime, personality factors, and online disinhibition.

The main research questions are:

1. What cognitive distortions, rationalizations, or neutralization techniques have been documented among cyber offenders in recent studies?
2. What behavioral or personality traits are consistently associated with cyber offending?
3. How do moral disengagement and online disinhibition influence the cognitive-behavioral processes of offenders?
4. What are the main gaps and future directions for integrating cognitive-behavioral models with digital trace analytics or intervention frameworks?

By bringing these threads together, the review aims to improve theoretical understanding and practical application in profiling, prevention, and rehabilitation of cyber offenders.

Furthermore, this paper extends beyond theoretical interest. Insights derived from offender cognition and behavior are positioned to hold direct implications for practice. They inform profiling methods, targeted deterrence strategies, rehabilitative interventions, and predictive models that integrate psychological insights with digital trace analytics. By situating cognitive-behavioral traits within the context of cybercrime, this review establishes a foundation for interdisciplinary collaboration among forensic psychology, criminology, cybersecurity, and law enforcement. Ultimately, the study emphasizes the necessity of incorporating psychological perspectives into broader cybercrime research and policy-making agendas, ensuring that prevention and response mechanisms address not only the technical but also the human dimensions of digital crime.

Cognitive Distortions and Neutralization in Cyber Offenses

Cognitive distortions, which are biased or self-serving thought patterns that justify or hide deviant behavior, have been studied in general criminology for a long time. A recent

systematic review shows that these distortions, such as minimizing harm, blaming victims, and rationalization, are strong predictors of criminal behavior in different areas. In the online environment, similar behaviors can be observed. Offenders may deny victimhood by claiming "they were just corporations," minimize consequences by saying "no real harm," or describe their actions as technical challenges or social experiments. The modern review titled The Role of Cognitive Distortion in Criminal Behavior reveals that many studies published between 2019 and 2024 illustrate how these distortions help maintain criminal behavior by reducing dissonance and guilt. In that review, tables present specific distortion types connected to violent and nonviolent crimes, including "minimization," "rationalization," and "validation of violence or deviance".

Research on online child sexual exploitation has looked at cognitive distortions in a detailed way. Steel et al. (2020) examined distortions among users of child sexual exploitation material (CSEM) and found common themes such as "denial of harm," "normalization" (the idea that "everyone else does it"), and "victim blaming". These distortions fit with traditional neutralization theory, but online, they can be intensified by a sense of distance from the victim and the role of intermediaries in the system.

Studies on how offenders represent themselves, including those involved in identity fraud or hacking, often point out rationalization through claims of curiosity or skill. For example, some fraudsters describe their actions as tests of the system's weaknesses rather than as malicious behavior. However, research specifically examining distortion prevalence among cyber offenders, beyond CSEM or phishing, is still limited, indicating a significant gap in understanding.

Moral Disengagement and Online Disinhibition

According to Bandura's theory of moral disengagement, people can participate in ethically dubious activities without self-sanction because they deactivate their self-regulation. Moral disengagement is especially noticeable in digital environments. Eight processes of moral disengagement (such as moral justification, advantageous comparison, diffusion of blame, and dehumanization) were found to predict cyber aggression more strongly than traditional aggression domains among developing adults, according to Nocera et al. (2022).

Online disinhibition is also linked to moral disengagement and deviant conduct in empirical research on cyberbullying, cyber harassment, and cyberdating abuse. Online disinhibition boosted moral disengagement, which in turn predicted direct cyber violence toward intimate partners, according to Sánchez-Hernández et al. (2024); gender and past victimization experiences modified the mediated route.

Similarly, studies of online incivility show that moral disengagement acts as a mediator between decreased online disinhibition and uncivil behavior. Other studies stress how aspects of electronic communication decreased social cues, anonymity, and asynchronous exchanges mar empathy and promote disengagement from moral boundaries. Corkum et al. (2023) specify that cognitive empathy is inhibited in mediated communication contexts, and this inhibition further eases the path to moral disengagement.

Overall, these studies suggest that there is a sequence: online disinhibition diminishes normative restraints allowing for moral disengagement mechanisms, and these mechanisms, in turn, allow for offending that is not justified. However, linkage from an empirical perspective remains limited in the context of serious cybercrime (e.g. hacking, fraud).

Behavioral Traits, Personality, and Decision-Making Biases

In addition to cognitions and moral pathways, personality traits and decision-making heuristics are also important factors in cyber offending. Several studies argue that traits associated with high levels of sensation-seeking, tolerance for risk, Machiavellianism, low empathy, and overconfidence in their technical capabilities problems which some researchers refer to as "criminal attitude" characteristically appear in cyber offenders Spreitzer & P. Arellano. The 2021 Profiling the Cybercriminal review stated that although there are many studies, there is no consistent personality trait model about offending types, and much of the research has been conducted on small convenience samples.

In a research-based study focused on financially motivated cybercrime, a recent practitioner-based survey (Peersman et al., 2022) demonstrated a growing convergence on the fact that offenders approach crime with the motivation of financial gain but display opportunistic traits, adaptive, and cognitive confidence, traits that are more akin to entrepreneurial risk-takers, rather than trait theories associated with traditional criminal decision-making.

The decision-making biases around cyber offending involve a failure to discount future harm, overestimating their chances of success and underestimating their chances of detection. They are likely to use exploratory thinking, such as norm anchoring ("others got away"), and optimism bias ("I won't get caught") that would subsequently undermine deterrent frameworks. However, the theory has limited scope in literature regarding empirical studies and how they make exploratory decisions around offending.

Typologies and Differences Across Offender Subgroups

An important aspect of understanding cognitive behavioral patterns is the awareness of heterogeneity across types of offenders: hacktivists, scammers, insiders, cyberbullies, and identity thieves will differ in terms of their motivational frameworks and the corresponding cognitions that occur. For instance, hacktivists frequently take on a moral justification (i.e., "we are fighting for justice") as a method of disengagement while fraudsters tend to rely more on types of financial rationalizations and denial of harm. In the case of CSEM offenders, distortion patterns are highly clustered around victim blamings.

Some theoretical advancements have made efforts to combine such models to be technology-specific. Steel et al. (2023) put forward a Lawless Space Theory (LST) to model how cyber offenders perceive digital spaces as being governed not by external law, but by the use norm for users, with the application of cognitive rationales and frames that argued they were within a "lawless space". LST can be an important mechanism for unifying cognitive distortions and environmental understandings.

Limitations

- There is an over-reliance on self-report and convenience samples. Many studies conducted are cross-sectional studies based on self-disclosure, resulting in social desirability biases and sampling biases.
- There are not enough longitudinal studies. Few studies reviewed explore how cognitive distortions or moral disengagement develop with recidivist offending or during rehabilitation.
- There is not enough focus on serious cybercrime. Much of the literature focus on cyberbullying, anti-harassment policies and dating; less on hacking, insider threats and frauds - serious crimes.

These gaps suggest there are unique opportunities for future research in cognitive-behavioral models to bridge the gap with digital forensic analytics and more robust research designs.

METHODOLOGY

This review represents a literature-based, integrative review as opposed to original empirical research. The review aims to synthesize and critically evaluate research findings related to cognitive-behavioral traits of cyber offenders.

Selection criteria:

1. **Deadline/date range:** Papers with a publication year from 2015 until date, to ensure a modern document context.
2. **Subject/Focus:** Must focus on psychological, cognitive or behavioral traits of offenders in a digital context (cybercrime, cyber aggression, hacking, online fraud, CSEM).
3. **Source:** Peer-reviewed articles or legitimate conference proceedings/exclusion criteria: systematic reviews.
4. Could be empirical, theoretical, or review articles, but must offer substantive evidence or theoretical understanding of cognition/behavior, not merely technical or legal articles lacking a psychological component.

Search Strategy: Databases included in the search were Google Scholar, PubMed, Scopus, Web of Science, and IEEE Xplore.

Inclusion/Exclusion Process: The initial search produced approximately 100 documents, and duplicates or documents not meeting the criteria for inclusion based on date or relevance, in relation to the technical or legal context without a psychological aspect, were removed from consideration. Titles and abstracts were screened, and full texts were evaluated to determine the relevance to the conceptual and/or empirical criteria to be included. In the end, a final inclusion of approximately 35-40 sourced were selected, and approximately 30 within the reference list.

Justification: The review method is fitting since the cognitive-behavioral aspect of cyber offending is still developing; synthesizing existing work allows us to uncover patterns, gaps, and directions, and does not require us to collect original data, especially under the tight time constraints we are facing. In addition, it allows us to bridge subdomains (cyberbullying to hacking) to determine common mechanisms across those subdomains.

RESULTS AND DISCUSSION

This section synthesizes the above-mentioned cognitive-behavioral traits, psychological habits, and contemporary work, and discusses them in a manner that propels current discussion.

Cognitive-Behavioral Traits: Core Themes

The reviewed literature reveals the following common cognitive-behavioral traits across offender types:

1. **Rationalization and Neutralization:** Offenders routinely utilize cognitive defenses to minimize guilt and justify their actions: denial of harm, blaming the victim, comparison to more morally egregious acts, or even restating one's actions as experiments.
2. **Moral Disengagement in Online Contexts:** Cyber offenders frequently employ moral disengagement strategies such as moral justification, euphemistic framing,

comparison with more serious offenses, diffusion of responsibility, minimization of consequences, dehumanization, and victim blaming. In online environments, these mechanisms often bridge the gap between situational disinhibition and actual offending behavior, allowing individuals to neutralize moral self-sanctions.

3. **Online Disinhibition and Weakening of Moral Control:** Features of digital interaction including anonymity, lack of immediate feedback, temporal separation, and reduced social cues diminish internal moral restraints. This disinhibited state increases the likelihood that deviant behavior will escalate, particularly when supported by moral disengagement processes.
4. **Empathy Reduction and Cognitive Distancing:** Technology-mediated interactions reduce cognitive empathy by increasing psychological distance from victims. Offenders may perceive victims as abstract figures or data points rather than real people, which lowers emotional barriers that would normally inhibit harmful actions.
5. **Technical Overconfidence and Repeated Risk-Taking:** Cyber offenders often overestimate their technical abilities while underestimating the risks of detection or punishment. Successful offenses reinforce self-efficacy, creating a feedback loop in which confidence promotes repeated risk-taking and sustained offending behavior.
6. **Personality Tendencies and Cognitive Biases:** Although evidence remains limited, existing studies suggest that cyber offenders are more likely to exhibit sensation-seeking tendencies, low conscientiousness, and opportunistic or manipulative traits. Decision-making in this context is often shaped by cognitive shortcuts such as optimism bias, anchoring judgments to prior successes, discounting detection likelihood, and normalizing risk through observation of others' offenses.

HOW PSYCHOLOGICAL PATTERNS INTERRELATE

These traits do not operate in isolation but form interacting patterns. A possible model is:
Online disinhibition → reduced normative restraint → moral disengagement activation → cognitive distortions/rationalizations → lowered guilt and justification → engagement in offending behavior.

- At the same time, high self-efficacy, sensation-seeking, and decision heuristics are pushing toward risk-taking and repeat behavior.
- Empathy suppression and cognitive distancing reduce affective inhibition for more severe offenses.

Recent research (e.g., online dating fraud) adds onto this model with the identification of dissociative symptoms, where offenders shared experiences of higher levels of dissociation in conjunction with moral disengagement and disinhibition. This suggests that there may also be an additional psychological aspect involved that deals with feelings of emotional detachment or compartmentalization.

New Insights & Advancements

Recent research has introduced more nuanced perspectives on cognitive–behavioral pathways in cyber offending, moving beyond uniform explanations.

- **Individual and Contextual Moderators:** Emerging studies suggest that factors such as gender, previous victimization, and patterns of online content consumption influence how online disinhibition translates into moral disengagement. For instance, Sánchez-Hernández et al. (2024) report that gender plays a moderating role in cyber dating abuse, indicating that disengagement pathways may differ across groups rather than follow a single pattern.

- **Protective Role of Digital and Media Literacy:** Evidence from adolescent-focused studies indicates that media and digital literacy may reduce the strength of the relationship between moral disengagement and cyber aggression. Greater awareness of online consequences and norms appears to limit the extent to which disengagement leads to harmful behavior.
- **Perceptions of Cyberspace as Norm-Free:** The Lawless Space Theory (LST) helps explain how offenders may perceive online environments as weakly regulated or socially permissive. Viewing cyberspace as self-policing can reinforce rationalization and make norm violations feel acceptable or routine.
- **Linking Psychology with Behavioral Traces:** Although still limited, recent scholarship has called for closer integration between cognitive–behavioral frameworks and digital trace evidence. Profiling research, such as Bada and Nurse (2021), emphasizes the value of aligning psychological characteristics with observable online behavior patterns rather than examining either in isolation.
- **Intervention and Treatment Considerations:** Some researchers have proposed adapting cognitive-behavioral therapy (CBT) approaches to address distorted thinking patterns that sustain cyber offending. However, empirical evaluations of such interventions remain scarce, and systematic trial-based evidence is still underdeveloped.

Implications for Profiling, Prevention, and Rehabilitation

- **Profiling & Threat Assessment:** Behavioral and cognitive indicators, including consistency of rationalization, overconfidence, recognized modes of moral disengagement, or dissociative attributes, could be useful additions to offender profiling in cyber investigation. Attempting to incorporate observed or hypothesized psychological signatures into anomaly detection or risk scoring models shows promise.
- **Prevention & Deterrence:** Interventions could focus on awareness of distortions and moral engagement, particularly with vulnerable or at-risk populations (e.g., youth, semi-skilled hackers). Media literacy programs that promote reductions in moral disengagement could indirectly lessen the probability of cyber aggression or lower-level offending.
- **Rehabilitation & Cognitive Interventions:** By reformulating cognitive-behavioral therapy (CBT) or other cognitive behavioral therapy paradigms or practices to suit the cyber context, offenders may be able to reduce distortions, increase empathy, or improve recidivism trends. Pilot studies could assess the impact of training on "digital moral realism" approaches (making victims more "real") or simulated or virtual/augmented-based activities or interventions.
- **Challenges & Cautions:** The anonymous and transnational characteristics of cybercrime mean psychological flavoured forms of intervention will typically face challenges in reach and enforcement. Furthermore, the generalizability of findings is typically limited due to small sample sizes and variability in cultures, so any profiling or intervention would need to be validated across populations and settings.

CONCLUSION AND FUTURE DIRECTIONS

This review synthesizes recent empirical and theoretical studies on the cognitive-behavioral traits of cyber offenders. The central findings highlight ongoing rationalization or neutralization, the emergence of moral disengagement in uninhibited digital environments,

decreased empathy, overconfidence in skills, personality traits driving risk, and cognitive distortions with heuristics in decision-making process.

The interaction among these components implies that they follow a fluid cognitive-moral-behavioral model: the uninhibited nature of the online environment diminishes normative constraints leading to disengagement and in turn distortion-driven offending while dispositional personality and decision-making biases sustain repeated action.

However, significant gaps remain: There has not been a longitudinal study of cognitive changes over time; limited consideration has been granted to coupling digital trace audio, video, and log analysis with the evidentiary behavior of offenders; the focus has been narrowly defined on certain types of offender types (bullying, dating) rather than a more serious form of cybercrime; and no consideration of any cross-cultural and demographic variability has been added.

In relation to future avenues of research:

1. mixed-method longitudinal designs to track offenders over time, combining cognitive measures with behavioral log tracking.
2. Intervention studies to determine the potential to remediate cognitive distortion, training in digital empathy, and the potential for teaching moral realism to cyber offenders or groups-at-risk.
3. Combining psychological models of cognition with AI and forensic analysis, as an example pairing machine learning with psychological models to analyze trace data to detect cognitive-behavioral signatures.
4. Conducting Comparative and cross-cultural study protocols to test how culture, legal systems, and socio-technical contexts modulate cognition for specific offender groups.
5. Laying out differentiated models of offenders to produce developed cognitive-behavioral profiles for different classes of offender (hackers, fraudsters, insiders, ideological against).

By furthering this integration, psychological insight into cyber offenders can move from theory to actionable profiling, prevention, and rehabilitation.

REFERENCES

Antoniadou, N., Kokkinos, C. M., & Markos, A. (2019). Psychopathic traits and social anxiety in cyber-space: A context-dependent theoretical framework explaining online disinhibition. *Computers in Human Behavior*, *99*, 228-234.

Bada, M., & Nurse, J. R. (2021, June). Profiling the cybercriminal: A systematic review of research. In *2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1-8). IEEE.

Bozkus, K. (Ed.). (2023). *Organizational Behavior-Negative Aspects: Negative Aspects*. BoD–Books on Demand.

Bussey, K., & Luo, A. (2024). Mindfulness as a moderator between the association of moral disengagement and cyberbullying. *International Journal of Bullying Prevention*, 1-8.

Chan, T. K., Cheung, C. M., Benbasat, I., Xiao, B., & Lee, Z. W. (2023). Bystanders join in cyberbullying on social networking sites: the deindividuation and moral disengagement perspectives. *Information Systems Research*, *34*(3), 828-846.

Corkum, M., & Shead, N. W. (2023). Online moral disengagement: An examination of the relationships between electronic communication, cognitive empathy, and antisocial behavior on the internet. *Psychological Reports*, 00332941231216415.

Corkum, M., & Shead, N. W. (2023). Online moral disengagement: An examination of the relationships between electronic communication, cognitive empathy, and antisocial behavior on the internet. *Psychological Reports*, 00332941231216415.

De Maynard, V. (2025). Examining individual differences and similarities in online disinhibition, moral disengagement, dissociative experiences, and compliance within the context of online dating fraud.

Gan, W., Chen, Z., Wu, Z., Huang, X., & Wang, F. (2024). Aggression in online gaming: the role of online disinhibition, social dominance orientation, moral disengagement and gender traits among Chinese university students. *Frontiers in Public Health*, *12*, 1459696.

Gumelar, G., Maulana, H., & Mas Bakar, R. Erik (2024). How online inhibition fuels incivility through moral disengagement. *Online Journal of Communication and Media Technologies*, *14*(4), e202448.

Harbinson, E., & Selzer, N. (2019). The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of crime and justice*, *42*(5), 582-598.

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Jeong, R., Gilbertson, M., Riffle, L. N., & Demaray, M. K. (2024). Participant role behavior in cyberbullying: An examination of moral disengagement among college students. *International journal of bullying prevention*, *6*(1), 28-40.

Kranenbarg, M. W., Van Gelder, J. L., Barends, A. J., & de Vries, R. E. (2023). Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in human behavior*, *140*, 107576.

Lestari, D. R., & Alwi, M. A. (2024). Hubungan Online Disinhibition Effect Dengan Kecenderungan Perilaku Cyberbullying Pada Siswa MA Pengguna Instagram. *J-CEKI: Jurnal Cendekia Ilmiah*, *4*(1), 1015-1028.

Li, H., Guo, Q., & Hu, P. (2023). Moral disengagement, self-control and callous-unemotional traits as predictors of cyberbullying: a moderated mediation model. *BMC psychology*, *11*(1), 247.

Maftei, A., Opariuc-Dan, C., & Grigore, A. N. (2024). Toxic sensation seeking? Psychological distress, cyberbullying, and the moderating effect of online disinhibition among adults. *Scandinavian journal of psychology*, *65*(1), 61-69.

Mateus Francisco, S., Costa Ferreira, P., Veiga Simão, A. M., & Salgado Pereira, N. (2024). Moral disengagement and empathy in cyberbullying: how they are related in reflection activities about a serious game. *BMC psychology*, *12*(1), 168.

Nocera, T. R., Dahlen, E. R., Poor, A., Strowd, J., Dortch, A., & Van Overloop, E. C. (2022). Moral disengagement mechanisms predict cyber aggression among emerging adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *16*(1), 1.

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). Understanding motivations and characteristics of financially-motivated cybercriminals. *arXiv preprint arXiv: 2203.08642*.

Sánchez-Hernández, M. D., Herrera, M. C., & Expósito, F. (2024). Is online disinhibition related to cyberdating abuse perpetration through moral disengagement? The moderating role of gender, sexism, and cybervictimization. *Sex Roles*, *90*(7), 938-959.

Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. (2023). Lawless space theory for online child sexual exploitation material offending. *Aggression and violent behavior*, *68*, 101809.

Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. (2020). A systematic review of cognitive distortions in online child sexual exploitation material offenders. *Aggression and violent behavior*, *51*, 101375.

Sun, Y. X., Cao, C. H., Tang, Z. J., Huang, F. M., Zhong, X. B., & Chen, I. H. (2025). Moral disengagement as mediator and guilt as moderator between cyber moral literacy and cyberbullying among late adolescents. *Scientific Reports*, *15*(1), 43.

Syasyila, K., Gin, L. L., Abdullah Mohd. Nor, H., & Kamaluddin, M. R. (2024). The role of cognitive distortion in criminal behavior: a systematic literature review. *BMC psychology*, *12*(1), 741.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169-188.

Wang, L., Jiang, S., Zhou, Z., Fei, W., & Wang, W. (2024). Online disinhibition and adolescent cyberbullying: A systematic review. *Children and Youth Services Review*, *156*, 107352.

Wang, L., Wang, W., Fei, W., & Wang, Z. (2025). Online Risk Behavior in Adolescents: A Systematic Review. *Trauma, Violence, & Abuse*, 15248380251343194.

Wang, X., Wang, W., Qiao, Y., Gao, L., Yang, J., & Wang, P. (2022). Parental phubbing and adolescents' cyberbullying perpetration: A moderated mediation model of moral disengagement and online disinhibition. *Journal of interpersonal violence*, *37*(7-8), NP5344-NP5366.

Wu, B., Zhou, L., Deng, Y., Zhao, J., & Liu, M. (2022). Online disinhibition and online trolling among Chinese college students: the mediation of the dark triad and the moderation of gender. *Cyberpsychology, Behavior, and Social Networking*, *25*(11), 744-751.

Zhao, L., & Yu, J. (2021). A meta-analytic review of moral disengagement and cyberbullying. *Frontiers in Psychology*, *12*, 681299.

Acknowledgment

The author(s) appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Penumarthi, G.S. & Ahad, S. (2026). Cognitive-Behavioral Characteristics of Cyber Offenders: A Literature-Based Perspective. *International Journal of Indian Psychology*, *14*(1), 2258-2267. DIP:18.01.227.20261401, DOI:10.25215/1401.227