ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

# The Role of Group Social Work in Preventing Adolescent Cybercrime--A Study Based on Peer Influence

**Bingxu Chen[a], Yiming Sun[b]**

*School of Law, Guangdong University of Technology, Guangzhou, China, 510520*
*[a]chenbingxu@mails.gdut.edu.cn, [b]211099683@mails.gdut.edu.cn*

***Abstract:*** *The purpose of this paper is to explore the necessity and application of group social work in preventing adolescents from engaging in cybercrime, focusing on the role of peer influence. By analyzing the current situation and causes of adolescent involvement in cybercrime, combining the core mechanisms of peer influence within groups, and examining the role of school and community social workers in addressing cybercrime among adolescents, a series of prevention and intervention strategies are proposed. This paper argues that creating a structured group environment can effectively alter adolescents' cognitive biases towards online risks, reshape their online behavior norms, and leverage the diffusion mechanism of "group influence-peer network fission" to radiate positive intervention effects from the core group to a broader group of adolescents. At the same time, it provides theoretical support and practical guidance for fostering a safer and more responsible online culture among adolescents.*

***Keywords:*** *cybercrime; group social work; adolescents; peer influence*

## 1. Introduction

With the rapid advancement of information technology, the internet has become deeply integrated into the daily lives of adolescents. However, the anonymity and openness of cyberspace have also provided new ground for juvenile delinquency. Cybercrime refers to illegal activities conducted using the internet and digital technologies. Adolescents, characterized by their still-developing psychological maturity, weak legal awareness, and strong curiosity, are particularly vulnerable to involvement in cybercrime under the influence of peers. In recent years, the number of adolescents cybercrime cases has shown an upward trend, and its social harm cannot be overlooked.

How to effectively prevent adolescents from engaging in cybercrime has become a critical issue of shared concern in the fields of education, law, and social work. Group social work, as a professional intervention method, emphasizes leveraging group dynamics and peer interactions to foster individual change and growth. The theory of peer influence posits that adolescents within groups are highly susceptible to the behaviors, attitudes, and values of their peers, often imitating or internalizing them as their own. Therefore, from the perspective of peer influence, employing group social work methods to intervene in the prevention of juvenile cybercrime holds significant theoretical and practical importance. This paper aims to explore the specific role and application pathways of group social work in preventing adolescents from engaging in cybercrime, with the goal of providing references for related practices.

## 2. Current situation and causes of adolescents cybercrime

### *2.1. Status*

Adolescents cybercrime refers to behaviors committed by adolescents using the Internet and digital technology that violate laws and regulations or seriously breach social ethics. This paper defines the hierarchical structure of adolescents cybercrime classification based on three categories: object, tool, and space.

ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

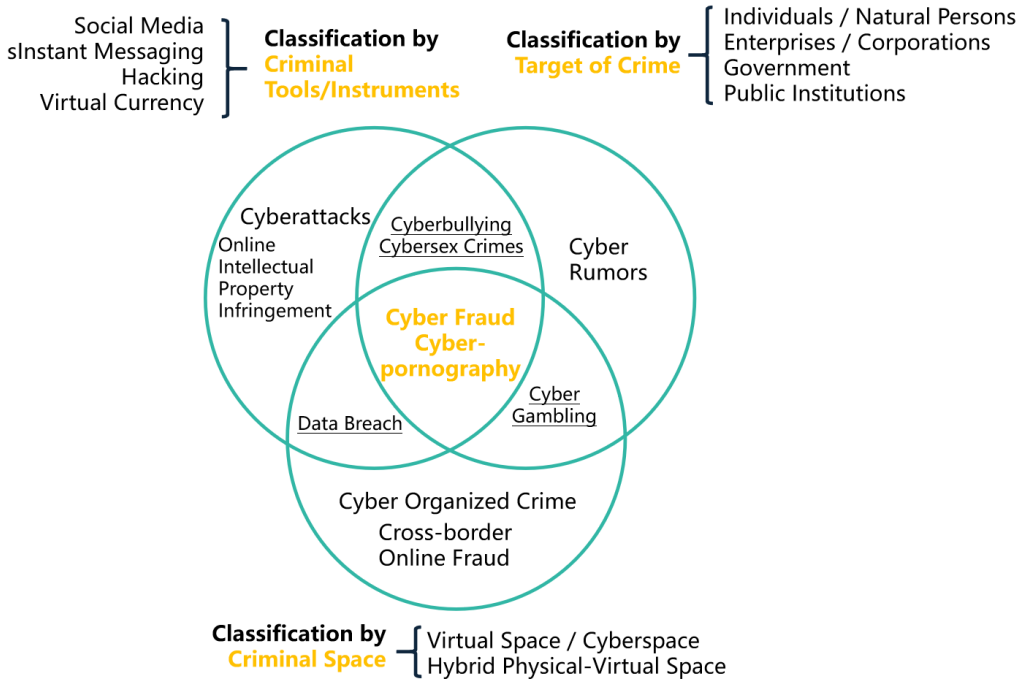


*Figure 1: Types of adolescents cybercrime.*

As shown in Figure 1, the Venn diagram illustrates a tripartite typology of cybercrime, categorized across three primary dimensions: criminal instruments (such as social media, hacking tools, and virtual currency), targets (ranging from individuals to government institutions), and the locus of the crime (virtual versus hybrid physical-virtual spaces). The intersecting regions highlight specific manifestations—such as cyberbullying and cyber fraud—that span multiple categories, underscoring the complex, multidimensional nature of cyber threats affecting adolescents.

### *2.2. Causes*

First, individual-level factors. Cognitive and emotional immaturity during adolescence serves as a fundamental internal driver influencing their potential involvement in cybercrime. Due to ongoing brain development, particularly in the prefrontal cortex responsible for judgment, impulse control, and risk assessment, adolescents are more prone to sensation-seeking, impulsivity, and misjudging the consequences of their actions. Their moral reasoning and legal awareness are often not fully developed, making it easier for them to rationalize unethical or illegal online behaviors as mere “pranks” or “jokes.” This cognitive and emotional immaturity lowers their internal barriers to committing adolescents cybercrime.

Second, peer group factors. The influence of peers is exceptionally powerful during adolescence. Within both online and offline social circles, group dynamics can significantly encourage cybercriminal behavior. This includes direct peer pressure to conform, the imitation of admired or high-status peers who engage in such acts, and the reinforcement provided by group approval. [1]The desire for belonging and social status within a group can override an individual's better judgment, leading them to participate in activities like software piracy, doxing, or coordinated online harassment to gain acceptance or acclaim.

Third, educational and familial factors. Deficiencies in school and family education systems play a critical role. Schools often lack comprehensive, age-appropriate curricula on digital citizenship, cyber ethics, and the legal ramifications of cybercrime. This educational gap leaves adolescents without a clear understanding of online boundaries and responsibilities. At home, factors such as insufficient parental supervision of online activities, a lack of open communication about internet use and risks, and the absence of positive role modeling for responsible digital behavior can create an environment where risky or illegal online activities go unnoticed, uncorrected, or even unintentionally encouraged. [2]

Fourth, societal and environmental factors. The broader socio-technological environment presents unique risks. The anonymity and perceived lack of traceability on many online platforms can reduce

ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

feelings of accountability and empathy. Furthermore, the rapid evolution of technology often outpaces the development and enforcement of relevant laws and regulations, creating grey areas that adolescents may exploit. A societal focus on technical prowess over ethical digital conduct can further skew adolescent perceptions, making cybercrime appear as a viable path to recognition or success.

## 3. Overview of relevant theories

Peer influence primarily operates through mechanisms articulated in social learning, normative social behavior, and differential association theories. We conceptualize peer influence as a dynamic process wherein adolescents' attitudes, beliefs, and behaviors are shaped by perceived norms and observed outcomes within their social networks.

According to Edwin Sutherland's Differential Association Theory, criminal behavior is learned through intimate personal groups, where definitions favorable to law violation outweigh definitions unfavorable to such acts. This learning includes not only techniques but also the motives, drives, and attitudes that accompany the behavior. In the context of online activities, this implies that adolescents may adopt cybercriminal behaviors if their peer interactions normalize or justify such actions while downplaying their consequences.

Albert Bandura's Social Learning Theory further elucidates this process through the concept of observational learning. Adolescents acquire behaviors by observing the actions and subsequent reinforcements received by peers within both real-world and digital environments. When peers are perceived to gain status, financial benefit, or social capital from engaging in cybercrime without facing significant negative repercussions, observers are more likely to model that behavior.

The Theory of Normative Social Behavior adds a critical layer by distinguishing between descriptive norms and injunctive norms. Adolescents may overestimate the prevalence and acceptability of cybercrime among their peers, creating a perceived social pressure to conform. This is particularly salient during adolescence, a developmental period marked by heightened sensitivity to peer approval and social identity formation. The desire for in-group affiliation can motivate adolescents to align their online behaviors with perceived group norms, even if those norms involve illicit activities.

Based on the above theories, this paper summarizes the Cognitive-Behavioral-Environmental Three-Dimensional Framework. As shown in Figure 2, this model posits that cybercriminal conduct emerges from the bidirectional interplay among cognitive-affective attributes, volitional acts, and environmental affordances. Specifically, personal factors shape behavior through expectations and values, while environmental stimuli activate and modulate behavioral intensity through individual psychological mediation, rejecting unidirectional causal explanations.

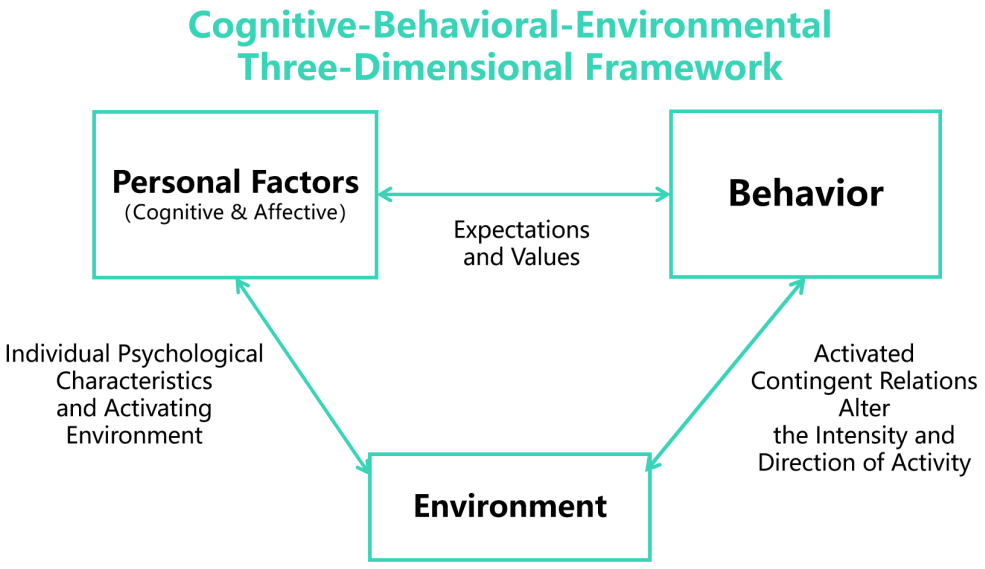


*Figure 2: Cognitive-Behavioral-Environmental Three-Dimensional Framework.*

This paper applies theories of peer influence to understand the social pathways that lead adolescents into cybercrime. In practical intervention design, these theories underscore that prevention must address

ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

the peer ecology. Merely educating adolescents about the abstract risks of cybercrime is insufficient if their immediate social environment continues to provide positive reinforcement for such acts. Specifically, through structured group work and organized activities, adolescents' perceptions and attitudes toward cybercrime can be systematically influenced. Within the group setting, after members acquire knowledge and skills to avoid cybercrime through interactive learning, they can further act as proactive "influence nodes," disseminating the acquired constructive attitudes and behavioral norms to their broader peer networks. This peer-based, fission-like diffusion of influence helps establish protective norms against cybercrime at the group level, thereby extending the reach of preventive effects and safeguarding more adolescents from such harm.

Peer influence processes may not only explain the rise in antisocial behavior in adolescence, but also offer an explanation for the development of more severe forms of antisocial behavior, including violence, gang involvement, and other more serious offenses. [3]

## 4. The Implementation Process of Group Social Work Interventions

The practical execution of the group intervention follows a structured, four-stage developmental model designed to transition adolescents from passive internet users to active proponents of digital legality.

Stage 1: Case Analysis and Awareness Raising. The process begins with the collaborative analysis of real-world cybercrime cases, specifically those involving youthful offenders. By dissecting "relatable" scenarios—such as unauthorized account access or the unintended consequences of online harassment—the social worker helps members transcend the "just a joke" rationalization. This stage focuses on heightening prevention awareness by illustrating the tangible harm caused to victims and the long-term legal repercussions for perpetrators. By grounding the discussion in actual cases, the group develops a foundational understanding that the virtual world has real-world consequences, effectively breaking down the cognitive biases that often lead to digital deviance.

Stage 2: Popularization of Legal Knowledge. Once awareness is established, the group moves into the systematic study of cyber-related laws. This stage involves simplifying complex legal codes into digestible, actionable knowledge. The social worker facilitates interactive workshops where members learn the legal boundaries of the internet, covering topics such as data privacy, intellectual property rights, and the specific statutes governing cyber-bullying and fraud. Rather than a dry lecture, this phase utilizes "legal role-playing," where members take on the roles of judges or defense attorneys. This helps internalize the law as a protective framework rather than a restrictive force, ensuring that legal literacy becomes a core component of the group's collective identity.

Stage 3: Communication Skills Training. With a legal foundation in place, the group focuses on interpersonal dynamics through communication skills training. This stage is vital for transforming group members into "influence nodes." Social workers train adolescents in assertive communication, conflict resolution, and peer mediation. The goal is to equip them with the verbal tools necessary to challenge illicit behavior in their own social circles without losing social status. By practicing how to say "no" to a peer-led cyber-attack or how to explain the risks of a "cracked" software link to a friend, members build the confidence required to maintain their ethical stance in high-pressure online environments.

Stage 4: Practical Exercises in Network Security Advocacy. The final stage shifts from internal learning to outward practice. Members engage in simulated and real-world exercises to popularize network security laws within their broader school or community. This might include creating digital safety posters, hosting short "peer-to-peer" webinars, or developing a social media campaign about responsible digital citizenship. By taking on the role of educators, adolescents reinforce their own learning and test their communication skills in real scenarios. This stage operationalizes the "fission" mechanism, as the group's influence begins to radiate outward, turning the intervention into a community-wide prevention movement.

## 5. The Role of Social Workers in Addressing Adolescent Cybercrime

Social workers are professionals who adhere to the core values of the field and employ specialized methods to provide social services. They are characterized by their commitment to the welfare of recipients, prioritizing service over personal gain, and utilizing professional approaches developed from both international standards and local practical experience. In the prevention of juvenile cybercrime, the

ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

role of social workers is pivotal. Through systematic intervention and the strategic management of peer dynamics, they catalyze the "fission" of positive influence throughout adolescent networks. [4] Specifically, social workers fulfill the following major roles and responsibilities:

First, the role of supporting and redirecting victims. Social workers provide psychological counseling and support to adolescents who have been harmed by or drawn into the periphery of cybercrime. By utilizing professional skills such as empathy and active listening, they create a safe environment for adolescents to share their digital experiences. Social workers employ therapeutic techniques to help these individuals recognize the emotional harm caused by digital deviance. Importantly, by helping victims regain self-confidence, social workers transform them into "resilience nodes" within their peer groups—individuals who can speak authentically to others about the risks of cyber-victimization, thereby initiating the first layer of positive peer influence.

Second, the role of educating and guiding the aggressors. Social workers establish professional relationships with adolescents who engage in cybercrime, using empathy training and legal education to foster recognition of their wrongfulness. They assess the underlying motivations, such as the desire for technical status, and redirect these impulses toward ethical digital conduct. By modifying the behavior of these "high-status" peers within the group, the social worker effectively shifts the group's descriptive norms. When these influential individuals adopt pro-social values, they act as the primary catalysts for "peer network fission," as their shift in attitude carries significant weight and imitation value among their broader social circles.

Third, management and coordination roles. Social workers assist in establishing and promoting prevention mechanisms within schools and communities. They collaborate with educational institutions to formulate digital safety policies and reporting systems. A key aspect of this role is coordinating the "peer ecology"; social workers organize training sessions for teaching staff and parents to help them support the positive peer leaders developed in group work. By integrating these at-risk youth into a comprehensive network of psychological and social support, the social worker ensures that the "influence nodes" created within the group have a stable environment to continue spreading legal and ethical knowledge to their peers. Peer pressure and socioeconomic status were found to have a relative influence on predicting cybercrime tendencies, whereas gender had no significant impact on these predictions. [5]

Fourth, the role of publicity and advocacy. Through the "home-school-society" linkage platform, social workers popularize knowledge regarding the dangers of cybercrime. They act as advocates for a healthy online culture, raising awareness among students and parents about the legal ramifications of digital actions. By participating in legislative proposals and engaging with civil organizations, social workers appeal to all sectors of society to support peer-led prevention models. Most importantly, they advocate for the recognition of "peer influence" as a formal tool in crime prevention, ensuring that the fission of positive behavioral norms is supported by broader social policies and community resources.

## 6. Conclusions

Based on the theories of peer influence and the Cognitive-Behavioral-Environmental (CBE) framework, this paper discusses in depth the necessity and application strategies of group social work in the prevention of adolescent cybercrime. Through a detailed analysis of the current situation and causes of juvenile digital delinquency, and combining the core mechanisms of group dynamics, this paper proposes a series of targeted preventive and intervention measures.

First of all, this paper clarifies the structural complexity of adolescent cybercrime, classifying it into a hierarchical framework based on object, tool, and space. These digital offenses not only violate laws and social ethics but also erode the moral foundation of the younger generation, potentially triggering long-term legal consequences and social harm. Therefore, the prevention and intervention of cybercrime is an urgent topic that requires immediate attention in the fields of law, education, and social work. In terms of causal analysis, this paper points out that individual cognitive immaturity, peer group dynamics, and deficiencies in family and school education are the main reasons for the occurrence of cybercrime. Adolescents' sensation-seeking tendencies and weak legal awareness make them vulnerable; peer pressure and the "contagion" of deviant behaviors in online groups exacerbate the risk; and the lack of digital citizenship education leaves a vacuum where negative norms can flourish. Moreover, social media acts as a vector for youth violence, and frequent exposure to violent activities and behaviors through these platforms has detrimental effects on adolescents, highlighting the importance of prevention strategies that address peer norms to mitigate cyber aggression. [6]

ISSN 2522-6398 Vol. 9, Issue 5: 13-18, DOI: 10.25236/FER.2026.090503

Based on the above analysis, this paper proposes the important role and application strategies of group social work in the prevention of cybercrime. First, through the guidance of the peer influence mechanism, group social workers can help adolescents correct their cognitive biases regarding online risks and reshape their behavioral norms. This includes the implementation of a "Digital Covenant" to establish shared group values; cognitive restructuring to break the "online disinhibition effect"; and the provision of legal literacy and digital resilience training to enhance adolescents' ability to resist negative peer pressure. Secondly, social workers utilize the "group influence-peer network fission" mechanism to extend the intervention's reach. By cultivating core group members into proactive "influence nodes," social workers enable these adolescents to disseminate positive legal norms and ethical behaviors to their broader social networks, effectively radiating the intervention effects from the micro-group to the macro-community. In addition, this paper emphasizes the multi-dimensional role of social workers as educators, supporters, and advocates. They must coordinate home-school-society resources to build a comprehensive support system that reinforces positive peer influence and ensures a consistent protective environment. Such strategies align with research indicating that family social work and community empowerment modules can be developed to address peer influence and pressure in juvenile delinquency, providing a framework for prevention efforts.[7]

In summary, this paper argues that adolescent cybercrime can be effectively prevented and reduced through the intervention of group social work and the strategic application of peer influence theory. This approach not only helps to protect adolescents from the legal and psychological pitfalls of the digital world but also fosters a safer, more responsible online culture. Furthermore, it provides valuable theoretical support and practical guidance for the cross-disciplinary integration of social work and juvenile justice. In the future, we expect more researchers and practitioners to pay attention to the dynamics of peer networks in cyberspace and work together to build a resilient and ethical digital environment for adolescents.

**Acknowledgements**

The paper is supported by "Guangdong Provincial Special Fund for Science and Technology Innovation Strategy."(Project No.pdjh2026bg084)

**References**

*[1] Khostarina, T., Nasution, N. A. R., Safitri, C. R. The Impact of Social Media Use and Peer Pressure on Adolescent Cybercrime Behavior: The Mediation Role of Emotional Intelligence and Parental Supervision Moderation[J]. Psikoborneo Jurnal Ilmiah Psikologi , 2025,13(4):747.*

*[2] Cioban,S., Lazăr, A. R., et al. Adolescent Deviance and Cyber-Deviance. A Systematic Literature Review[J]. Frontiers in Psychology, 2021,12, 748006.*

*[3] Dijkstra, J. K., & Gest, S. D. Peer influence in the development of adolescent antisocial behavior: Advances from dynamic social network studies[J]. Developmental Review,2018, 47, 1-20.*

*[4] Jugos, R. P., Nabe, N. Juvenile Delinquency from the Lens of Social Workers: A Descriptive Inquiry[J]. Psych Educ Multidisc J, 2025, 42 (9), 1283-1299, doi: 10.70838/pemj.420905, ISSN 2822-4353.*

*[5] Afolabi, O. O., & Afolabi, A. S. Peer pressure, socio-economic status and gender difference on cybercrime tendencies of undergraduates[J]. Journal of Pedagogical Sociology and Psychology,2024, 6(2), 111-122.*

*[6] Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. Social media as a vector for youth violence: A review of the literature[J]. Computers in Human Behavior, 2022,129, 107-115.*

*[7] Mohamad, M. M., & Zainuddin, N. A. A Case Study on Peer Influence and Peer Pressure in Juvenile Delinquency[J]. International Journal of Academic Research in Business and Social Sciences, 2023,13(5), 1744-1756.*