International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 20, No. 3, 2025

Combating Cyber Violence: A Multi-Level Approach for a Safer Digital Space

Riyang Dai, Jindian Lu, Yian Chen, Yige Wang, Xuanxuan Xie*

School of Digital Economy & Trade, Wenzhou Polytechnic, Wenzhou 325000, China

* **Corresponding Author:** Xuanxuan Xie

Abstract: In recent years, alongside the steady growth of China's internet user base, diverse forms of cyber violence-including doxxing, rumor-mongering, defamation, and the malicious spread of manipulated content-have emerged as frequent, widespread, and highly contentious issues. These phenomena pose significant potential harm to individuals and society. While the Chinese government and relevant authorities have prioritized this problem, enacting a series of policies and regulations, the inherent ambiguity and evolving nature of cyber violence present considerable challenges for both research and governance. This study, therefore, employs empirical investigation to further analyze the current state of cyber violence and its influencing factors. Based on the findings, the research proposes a multi-level strategy to combat cyber violence, aiming to contribute to building a safer digital space.

Keywords: Cyber Violence, Influencing Factors, Multi-Level Approach.

1. Introduction

According to the 56th Statistical Report released by the China Internet Network Information Center, as of June 2025, the number of internet users in China had reached 1.123 billion, with an internet penetration rate of 79.7%. As the barriers to internet access continue to lower, the highly widespread internet has reshaped the daily lives of the public. However, this proliferation has been accompanied by a surge in various online disorders, including doxxing, personal attacks, rumor mongering, defamation, and the malicious spread of manipulated content. Consequently, cyber violence has emerged as a critical societal issue of widespread concern [1]. High-profile cases of cyber violence have repeatedly sparked intense public debate, fueling growing demands for stronger regulatory measures against such behaviors.

The Chinese government and relevant authorities have placed significant emphasis on addressing cyber violence, identifying it as a priority for governance within the digital ecosystem. A series of policies and regulations have been enacted to safeguard the legitimate rights and interests of internet users and maintain a civilized and healthy online environment. Nonetheless, the distinct characteristics of cyber violence-which differ fundamentally from real-world violence-pose unique challenges for both its governance and academic research. On one hand, the legal statutes and institutional frameworks pertaining to cyber violence remain underdeveloped, resulting in regulatory grey areas that necessitate a collaborative, multi-stakeholder approach to establish an effective mitigation system [2]. On the other hand, within the context of a traffic-driven digital economy, internet users exhibit distinct psychological patterns, moral emotions, and behavioral tendencies in the context of cyber violence [3]. These considerations highlight the urgent need to conduct an in-depth analysis of the current state and influencing factors of cyber violence, in order to propose well-informed and actionable countermeasures.

2. Literature Review

The term "cyber violence" has long been discussed in academic circles, and scholars both domestically and internationally have conducted extensive research on the subject. Major research streams include the definition and impacts of cyber violence, foundational behavioral theories related to cyber violence, as well as its influencing factors and governance strategies. In studies concerning the theoretical foundations of cyber violence, mainstream perspectives include Albert Bandura's Triadic Reciprocal Determinism and Cognitive Behavioral Theory, which emphasizes the bidirectional interaction between internal cognition and external behavior. Within the context of cyber violence research, the three factors in Triadic Reciprocal Determinism correspond respectively to internet users, the behaviors exhibited in cyber violence incidents, and the actual social and online environments-all of which interact dynamically. Cognitive Behavioral Theory suggests that the study of cyber violence should integrate internal cognitive processes with external environmental factors to guide internet users toward rational thinking and behavior.

Deriu et al. and Jo (2025) employed mathematical statistical models to quantitatively analyze cyber violence behaviors and identify relevant influencing factors [4]. In a study on response strategies, Wang (2023) proposed the introduction of new legal provisions specifically targeting cyber violence, arguing that this would serve as an effective deterrent, foster healthier social norms, and provide timely and solid support for the construction of a digital legal order [5].

While existing research on the basic conceptualization and theoretical underpinnings of cyber violence has matured, providing a robust foundation for the field, studies on influencing factors, evolutionary mechanisms, and response strategies remain limited in scope and perspective. Therefore, there is a need to integrate existing theoretical frameworks with analyses of public opinion derived from recent cyber violence incidents, through comprehensive empirical

investigation, in order to propose multi-layered governance strategies [6]. Such efforts would offer valuable decision-making support for relevant authorities.

3. Research Methodology

This project was designed and implemented by integrating theoretical research with empirical analysis, policy development, and social education. A mixed-methods approach was adopted, which combined quantitative questionnaire surveys with qualitative in-depth interviews and case studies. This empirical investigation was informed by an extensive review of the existing literature. These methods were deployed within a coordinated research framework to ensure a comprehensive investigation into the current state of cyber violence and its influencing factors, thereby facilitating the proposal of multi-level preventive and responsive measures.

The survey was conducted in three sampled cities-Wenzhou, Taizhou, and Lishui-in Zhejiang Province, utilizing both questionnaire distribution and in-depth interviews to gain nuanced insights into the manifestations and determinants of cyber violence. Given that cyber violence behavior represents a comprehensive outcome influenced by both internal and external factors-including individual cognition, external stimuli, social environment, and online norms-this study builds upon existing research to examine five key independent variables: attitudes, subjective cognition, social environment, online norms, and propensity for cyber violence, analyzing their collective impact on actual cyber violence behavior.

The research team assigned clear and appropriate roles based on the nature of the tasks and individual members' expertise, ensuring division of labor and enhancing organizational and operational efficiency. Throughout the project, all team members engaged in mutual supervision, maintaining an orderly structure and efficient workflow to guarantee the smooth execution of the survey.

4. Findings and Analysis

(1) Analysis of Cyber Violence-Prone Populations

Differential analysis based on respondents' demographic characteristics revealed that gender, age, and education level exert varying degrees of significant influence across three dimensions: attitudes toward cyber violence, propensity for engagement, and actual abusive behaviors. Regarding attitudes, individuals under the age of 18 expressed stronger opinions compared to other age groups, while those with a bachelor's degree showed more pronounced views than those with other educational backgrounds. In terms of propensity for cyber violence, respondents aged 25–30 demonstrated a higher inclination toward engaging in such behaviors. When examining actual behavior, males were more likely than females to perpetrate cyber violence. Moreover, individuals aged 25–30 and those with vocational education were more prone to enact abusive behaviors under similar demographic conditions. Based on these findings, a preliminary profile of individuals more susceptible to involvement in cyber violence can be outlined: males, students, and young adults in the early stages of their careers. These groups are generally more willing to express opinions and attitudes online. Many are at critical life stages, potentially facing psychological pressures related to employment, relationships, and family responsibilities. Lacking adequate coping mechanisms and psychological support, they may be more vulnerable to becoming entangled in cyber violence, thereby exhibiting both the propensity for and actual engagement in such behaviors.

(2) Analysis of Cyber Violence Awareness

Regarding the recognition of cyber violence forms, most respondents accurately identified behaviors such as verbal intimidation, insults, rumor dissemination, and the malicious manipulation of images or videos. However, significant divergence existed as to whether doxxing and public exposure of private information constitute cyber violence. In judging verbally aggressive behaviors, participants generally recognized explicitly offensive language, yet showed considerable disagreement over whether indirect or implicit expressions-those not containing explicit profanity-should be classified as cyber violence. These findings indicate that while respondents possess basic legal awareness and discriminatory ability, the absence of clear and unified standards results in persistent ambiguity between cyber violence and other transgressions. During in-depth interviews, many participants expressed uncertainty in determining whether acts such as privacy invasion or indirect verbal attacks exceed acceptable boundaries. Beyond legal norms, social morality also influences public perception, contributing to cognitive biases.

(3) Analysis of Attitudes Toward Cyber Violence

Attitudinal analysis revealed a dualistic pattern in responses depending on whether individuals adopted the role of bystander or victim. As bystanders, netizens predominantly exhibited indifference, often choosing to ignore incidents or remain passive observers. In contrast, as victims, individuals showed a stronger tendency to actively respond through legal channels, official complaints, or reporting mechanisms to protect their rights. In-depth interviews further indicated that some bystanders considered reporting perpetrators to authorities or exposing them on social media but were hindered by a lack of clarity regarding accountability procedures, ultimately leading to inaction. This contrast in attitudes highlights how perceived personal interest and concerns for dignity shape responses, underscoring the importance of these differences in formulating effective prevention and intervention strategies.

(4) Analysis of Factors Influencing Cyber Violence Behavior

The survey demonstrated that subjective cognition, social environment, and online norms exert significant positive effects on engagement in cyber violence, with decreasing influence in that order. The propensity for cyber violence served a mediating role in these relationships. These results indicate that both internal and external factors collectively influence cyber violence behavior. Notably, internal subjective factors are equally critical as external social and normative conditions. Qualitative insights from interviews corroborated these findings: individuals who perceive themselves as powerful or influential online and believe anonymity protects them from punishment are more prone to aggressive and rights-infringing behaviors. Many respondents attributed cyber violence not only to personal factors such as emotional venting and ambiguous moral standards but also to societal influences including authoritarian and collectivist ideologies, which some perpetrators rationalize as a means to defend their rights and dignity. Additionally, imperfect legal regulations and governance gaps currently fail to effectively deter potential

offenders.

5. Conclusion and Recommendations: A Multi-Level Approach

Based on the findings of this study, effective prevention and mitigation of cyber violence require collaborative governance involving multiple stakeholders. Government agencies, platform operators, and internet users must each fulfill their responsibilities, cooperate closely, and establish a synergistic long-term mechanism. This entails building a closed-loop governance system covering pre-event monitoring and early warning, real-time intervention and handling, and post-event accountability and remedy. Accordingly, this study proposes the following multi-level recommendations (see Figure 1.) to facilitate coordinated action among all parties, ultimately constructing a comprehensive governance framework to combat cyber violence and foster a safer digital environment.

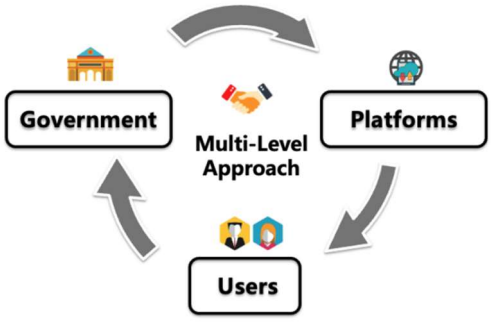

Figure 1. A Multi-Level Approach for a Safer Digital Space

(1) Government: Eliminate Regulatory Ambiguity and Ensure Effective Enforcement

The government and relevant authorities should implement comprehensive cyber violence policies and regulations, taking a leading role in establishing a multi-stakeholder collaborative governance system. It is essential to clarify the criteria for defining, identifying, and penalizing cyber violence to eliminate regulatory grey areas and provide a solid legal foundation. Additionally, mechanisms for reporting, handling, and tracking incidents must be optimized, with enhanced monitoring and analysis of abusive behaviors to promptly identify and counter emerging forms and trends. Oversight of online platforms should be strengthened through robust public opinion supervision mechanisms, obligating platform enterprises to fulfill social responsibilities by swiftly detecting and managing harmful information while intensifying efforts to combat cyber violence. Furthermore, initiatives promoting public adherence to online ethics-through humanistic education and guidance-should be advanced. Support must include necessary psychological assistance for victims, with particular attention to individuals across genders, ages, educational backgrounds, and professions. Strengthened cybersecurity education and awareness campaigns are also critical to disseminate knowledge about the harms of cyber violence and appropriate countermeasures, thereby elevating public awareness, self-protection capabilities, and fostering a civilized digital environment.

(2) Platforms: Deepen Self-Regulation and Leverage Technological Advantages

Platform enterprises should enhance internal management and establish robust content review and reporting mechanisms, enforcing suspension, restriction, or removal of accounts that publish illegal or non-compliant information. By harnessing technological advancements such as artificial intelligence and large-language models, information screening can be significantly improved to enable real-time monitoring, automatic classification, and accurate labelling of harmful online content. It is equally important to protect the privacy and rights of users affected by cyber violence and ensure effective post-incident accountability and support. Collaboration with government bodies and industry associations should be strengthened to actively participate in a multi-stakeholder governance system. Encouraging users to report abusive behaviors will foster broad public participation in cultivating a healthy and orderly online environment.

(3) Users: Enhance Awareness and Adopt Scientific Protection Strategies

As participants in the digital space, general users should strengthen their understanding of cyber violence-including its harms and consequences-and enhance self-protection awareness and capabilities. Active engagement in combating cyber violence is essential, through elevating digital civility and legal awareness, and upholding proper values and online ethics. Effective measures include resisting the spread of harmful content and implementing scientific protective strategies, such as using strong passwords, updating them regularly, and employing cybersecurity software to safeguard personal information and reduce targeting risks. In cases of victimization, individuals should remain calm, collect evidence, and seek support via official reporting channels or legal recourse, while attending to their psychological well-being. As publishers and disseminators of information, content creators and self-media users must consciously comply with laws and regulations, abstain from posting illegal content, and adhere to principles of truth, objectivity, and fairness. They should respect others' rights and privacy, respond rationally to trending online issues, and avoid sensationalist commentary for engagement.

6. Limitations and Future Research

This study has several limitations related to sampling, methodology, and data quality. The sample was primarily drawn from three cities in Zhejiang Province, which may affect the generalizability of the findings. Methodologically, the selection of data analysis approaches and measurement tools may have influenced the results due to the authors' limited expertise. Additionally, the reliance on self-reported data introduces potential biases, such as social desirability effects and cognitive limitations, which could affect accuracy. Future improvements should aim to expand the geographic and demographic scope of sampling, adopt more robust analytical techniques, and mitigate subjective biases through complementary data sources.

Future research should broaden the sampling framework to include more diverse regions and demographic groups to enhance representativeness. Theoretical expansion beyond planned behavior and social cognitive theories is also recommended to better capture the complexity of cyber violence. Further studies could also differentiate between types of cyber violence, analyze their distinct causes and impacts, and empirically evaluate the effectiveness and sustainability of intervention strategies proposed in this study.

Acknowledgments

The authors gratefully acknowledge the financial support from 2024 Zhejiang Provincial College Student Science and Technology Innovation Activity Plan (2024R470A004).

References

[1] Reneses M ,Gutiérrez R M ,Guerra B N .“It’s just a joke”: gender, sexuality and trivialisation in adolescent online violence such as cyberhate, cyberbullying, and online grooming[J].Humanities and Social Sciences Communications,2025,12(1):740-740.

[2] Yanjun L ,Wei W .Research on Chinese Legal Regulation of Internet Violence in the Internet Era[J].International Law Research,2024,13(1):19-19.

[3] Deriu F ,Villante C ,Muratore G M , et al.Challenging Big Data for studying gender-based violence: a methodological proposal[J].Quality & Quantity,2025,(prepublish):1-19.

[4] Jo H .Understanding Cyber Violence: Factors Influencing Cyberbullying among School-Aged Children[J].Child Indicators Research,2025,18(4):1-27.

[5] Wang C .Study on the Criminalisation of Cyber Violence[J].Journal of Social Science and Humanities,2023,5(12):

[6] Mujtaba M A ,Sabika S F .Influence of cyber violence and online victimization on cognitive development of female students from Pakistani higher education institutions[J].Journal of Aggression, Conflict and Peace Research,2024,16(4):330-347.