



Research on the Governance dilemma and Countermeasures of Cyber Violence

Yihan Pan¹, Guangxuan Chen^{2,*}, Qiang Liu², Ying Shi³

¹ Department of Computer and Information Security, Zhejiang Police College

² Institute of Bigdata and Network Security, Zhejiang Police College

³ Department of Public Order Policing Science, Zhejiang Police College

*Corresponding author. Email: chenguangxuan@zjjcxy.cn

Abstract. With the development of the Internet, cyber violence that violates citizens' private rights has intensified. Lack of a perfect system of laws and effective regulatory system, and insufficient technical countermeasures also contributed to a certain extent to the rampant cyber violence. The complete underground internet industry behind cyber violence has gradually formed, greatly affected the normal social order. To this end, this article discussed the current governance dilemma of cyber violence, and put forward suggestions for combating and governing cyber violence from the perspectives of establishing special regulations, improving judicial interpretations, increasing platform supervision, and strengthening technical countermeasures, so as to create a clear and clean network environment.

Keywords: cyber violence, governance dilemma, underground industry.

1 Introduction

With the development of Internet technology, China has entered the era of Self-Media. Compared with the previous development stage of the Internet, in addition to having stronger virtuality, anonymity, immediacy and other characteristics, self-media shows stronger interaction and subjectivity [1]. The "decentralized" characteristics of online speech make everyone have the right and channel to give their opinions, and the right to speak on the Internet is no longer only in the hands of a few well-known bloggers [2]. At the same time, due to the lack of network supervision and privacy protection in the early stage of the self-media era, the risk of network information dissemination has gradually increased. Every mobile user can become a publisher and disseminator of network information, and the interaction between netizens is more frequent and close [3]. Platforms such as Weibo, WeChat, and live video sharing are recognized and accepted by the general public, and are becoming part of people's daily entertainment. It makes it easier and faster for the public to receive social hotspots and participate in discussions on sensitive issues. With the help of netizens, small-scale events can quickly develop into hot online events through Weibo or Moments [4]. And with the in-depth discussion within the netizens, hot network events

gradually expand their influence, and then develop into public events that the whole people may pay attention to. The Internet provides people with a platform for free expression and equal communication, and the development of self-media provides people with a more convenient and efficient carrier ^[5]. However, due to the limitations of self-media and various contradictions in the process of social transformation, a lot of opinions expressed by netizens lack of rational thinking. Therefore, some people with bad intentions use the emotions of netizens to gain attention by expressing radical views and biased remarks. In the end, online public opinion turned to one side, triggering online violence ^[6]. As a new type of violence, cyber violence continues to generalize, and it has the indication of replacing judicial trials with online public opinion trials to some extent.

From a series of incidents like "Pornographic incident" that happened in recent years, it can be seen that exposing the privacy of others on the Internet has become a common practice, leading to fierce "verbal battle" and "doxing wars" ^[7]. The Internet is becoming an unrestricted means of expressing speech, and a series of harms caused by its blindness, extremeness, and irrationality have become increasingly obvious. The Internet's involvement and impact on the real society is increasingly greater, and the gangster-like violence has infiltrated the Internet and is showing an explosive trend.

This paper analyzes the current situation of cyber violence and the governance dilemma, and proposes a new mode of cyber violence governance and prevention, so as to ensure a harmonious and orderly network environment in the country ^[8].

2 Cyber Violence

2.1 The Concept of Cyber Violence

Cyber violence, as the name suggests, refers to violent behaviors in the Internet environment. Unlike traditional violence, this kind of violence is generally regarded as an extension of social violence on the Internet, and it is a hidden and nihilistic existence. Excessive remarks in online public opinion, publicly release of harmful pictures, videos, etc., intentionally exposing other people's privacy, or deliberately attacking other people's websites and stealing other people's private information through network hacking technology are all in the category of cyber violence ^[9]. Combining the manifestations in real life and the results of harm, cyber violence can be classified into four forms:

Firstly, the explosive growth of online rumors. In the network environment, massive amounts of information are generated all the time, and there is a lack of identification mechanisms and rumor-refuting mechanisms in the entire process from publication, dissemination to reception. In addition, the virtual nature of the network and the anonymity of users also provide a breeding ground for online rumors. The cost of making online rumors by netizens is low, while the cost of rights protection for victims is very high. Therefore, netizens who post bizarre, absurd and hurtful remarks are on the fringes of law and morality, and are basically not subject to substantial

legal punishment. High-profile speeches spread rapidly through the medium of the Internet, gaining network traffic and obtaining huge economic returns.

Secondly, the moral kidnapping of hypocrisy and coercion. Netizens usually use morality as a bargaining chip and coat to exert public opinion pressure on others on the Internet. Use an invisible soft binding force to coerce the parties involved, so that their behavior conforms to their own evaluation standards and expectations. These netizens, standing on the moral high ground, must be biased in their judgment of some behaviors on the Internet, which undoubtedly violates the spiritual realm of the individual, and the harm hidden in the screen is often invisible and will be ignored. Generally speaking, public figures are more likely to be the targets of moral kidnapping because of their high profile. Using moral kidnapping and herd mentality to incite more netizens's emotions and try to resonate with bystanders can get huge traffic, which contains unlimited business opportunities.

Thirdly, malicious online defamation. The public discourse rights possessed by the public benefit from the great openness of cyberspace. People can comment on things relatively unrestrictedly and express their emotional thoughts openly. However, it is precisely because of the freedom of new media, the low degree of regulation of the Internet, and the uneven moral literacy of netizens that freedom of speech has broken the moral bottom line. As a result, many netizens hold high the banner of "freedom of speech", and believe that slander and personal attacks against others are reasonable emotional venting. It is worth emphasizing that, along with the convenience and speed of the Internet, the dissemination of online speech has a large radius and a fast speed. Therefore, the negative impact of online slander on society and individuals is often more serious than slander in reality ^[10].

Fourthly, cyber manhunt. Cyber manhunt can effectively organize a large amount of information on the Internet, maximize the use of social resources, and help curb the breeding of cyber crimes and strengthen social supervision. On the other hand, cyber manhunt will lead to the participation of the whole people, exposing the personal information of the parties to the public view, often surpassing the incident itself, and even increasing the family members and interfering with the normal private life of others. Cyber manhunt has injected new vitality into the search mode. However, if the red line of supervision and privacy is exceeded, it will have a very bad social impact, cause serious physical and psychological trauma to the parties, and even threaten the safety of life.

To sum up, this paper regard the cyber as cyber torts in which netizens publish real or false information on the Internet to infringe citizens' right to reputation or privacy, or use morality to excessively accuse and restrain citizens, causing property damage and personal damage to citizens.

2.2 Related Research

Luo Xin believes that cyber violence is essentially a practice based on a power relationship that includes a micro-power structure, in which the power structure is formed by the self-empowerment of netizens and legalized by the production of moral discourse, making the perpetrators in constant moral criticism. included in this unequal

power structure. Psychologists Hou Yubo and Li Xinlin believe that in reality, new media can provide marginalized groups with an opportunity to express their opinions. Jiang Ning argued in "The Moral Examination of Cyber Violence" that cyber violence is a form of public opinion. This behavior uses moral evaluation as a sign of external moral behavior, but it violates the right to moral evaluation, that is, it imposes moral coercion on others through the pressure of public opinion. Du Tianyu pointed out that cyber violence is a negative influence generated by the network society, and is a negative reflection and expression of various fields such as economy, politics and culture in the network society in reality. The rule of law model is the only way to govern cyber violence. The legalization of cyber violence governance refers to the use of the rule of law thinking and the rule of law to reasonably regulate cyber violence on the track of the rule of law, so as to create a clean and upright cyber environment. Li Dongsheng believes that cyber violence is a relatively new social problem, and the existing laws and regulations are not enough to complete the governance task, and the legal and regulatory system still needs to be improved to deal with it systematically. Behind almost all cyber violence are intricate chains of interests, a "flow-only" online content creation orientation, and the spread of deformed values. All these constitute the soil for cyber violence to breed, and also "create" this world. the root cause of social governance problems. Therefore, he suggested that special legislation should be used to plug system omissions, improve the judicial system for combating cyber violence, reduce the cost of citizens' rights protection, and increase the punishment of those responsible for cyber violence.

The Internet first originated in the West, and there are many studies on the concept of cyber violence. For example, Peter Smith, Jess Mahdavi and Manuel Carvalho, three American scholars defined cyber violence in the article "Investigation Report on Forms, Perceptions, Effects and Age and Gender Factors of Cyber Violence in Relation to Cyber Violence", mainly mentioning the targets of cyber violence, the difficulty of victims' personal ability to face and resist cyber violence, and it predicts that with the popularity of smartphones, cyber violence may intensify. Keith R. Sunstein used the "group polarization theory" in "Republic of the Internet: Democracy in the Internet Society" for analysis, arguing that the radical and risk-taking views of netizens are the reasons for cyber violence. In the book "Iron Cage or Utopia: Law and Morality in Cyberspace", Richard Spinello pointed out that in the process of governance of cyberspace, the most important thing is the construction of relevant ethical and moral systems. Privacy law expert Daniel Shalef's "The Age of Unsecured Privacy" mainly expounds the relationship between freedom of speech and the right to privacy. As freedom of speech and protection of personal privacy are difficult to balance, it is urgent to find a balance between the two. Lawrence Lessig argues that cyberspace is not a entertainment place, but rather a symbol of domination. It is believed that the governance of the network society and the real society are consistent, and all rights in the network society must be implemented under the governance and control of the government, otherwise the network society may cause serious crisis due to excessive freedom. Professor Rolf Weber of the University of Zurich divides the governance model of the network society into four forms: government regulation, international cooperation, self-management and technical architecture model. Australia's

Fletcher believes there needs to be an appropriate balance of free speech for adults, and believes investigators can find the right balance between removing harmful content and free speech.

3 The Dilemma and Reasons of The Existing Governance of Cyber Violence

3.1 Legal Level

3.1.1. Unclear Legal Definition of Cyber Violence and Imperfect Relevant Judicial Interpretations.

At present, the laws in China have not yet stipulated the basic connotation of cyber violence. There is a lack of special laws against cyber violence, and there are quite a few laws involved. There is no clear definition of the level of cyber violence that constitutes illegality, resulting in inability to There are great obstacles in the implementation of laws and law enforcement, making cyber violence in a gray area for a long time. The most specific provision that can be found is the "Judicial Interpretation on Handling Criminal Cases of Defamation by Information Networks" promulgated by the Supreme People's Court and the Supreme People's Procuratorate on September 9, 2013. The judicial interpretation stipulates that the use of information networks to defame others, and the same defamatory information is actually clicked, viewed more than 5,000 times, or forwarded more than 500 times, it can constitute a crime of defamation. The judicial interpretation clearly stipulates the criteria for determining what constitutes defamation by an information network. Such regulations have a great deterrent effect, making netizens fearful before maliciously defaming others. However, cyber violence is not only limited to cyber defamation, but also various forms of illegal acts. None of these violations appear in the regulations, nor are there clearly defined standards. The current legislative work on cyber violence is slow and unable to keep pace with the intensifying cyber violence.

3.1.2. Difficulties in network supervision prevail.

Due to the strong randomness of cyber violence, the biggest difference between it and traditional violence is that ordinary violent acts are usually implemented after careful design, arrangement, and cyber violence does not need to go through these processes. This can be done by posting comments on social platforms from a personal account. In addition, due to the huge number of users of various social media, it is difficult to identify whether the remarks published by netizens are related to cyber violence in a short period of time. Therefore, the supervision of cyber violence can be considered as a dynamic process, requiring all aspects of supervision, and supervision before, during and after the event, which is a systematic process. This requires a lot of social resources. At present, China's work in this area is still insufficient, and the final result is not significant due to the low cost of regulation.

3.2 Social dimension

3.2.1. Intricate chain of interests.

With the rapid development of new media, the concept of "content is king" has been gradually defeated by "traffic-only theory". Network traffic and economic interests are inseparable. For example, with the change in the distribution mode of film and television dramas, the influence of online video websites is increasing, and the "traffic prosperity" created by rankings and clicks will be closely related to market share, advertising revenue and other bonus interests. Another example is some so-called "traffic stars" and "popular IPs". They hire navy soldiers, do hot searches, and stir up topics. The purpose is also to get high pay and earn hot money. At the moment of "traffic only", more and more media rely on shocking headlines, extreme views, and extreme emotions to attract the public's attention. In their writings, characters and events become cold data traffic and money-making machines. Due to the increasing market competition faced by news media, some news media lack fact-checking in their reports, blindly pursue fast traffic, and lack consideration of the consequences for the parties involved, resulting in more serious consequences of cyber violence. Compared with other instigators of cyber violence, the cyber violence created by the news media is more terrifying due to their own dissemination influence. The content released by these news media is due to the lack of objectivity of the content and the subjective assumptions of the publishers, thus consuming the emotions of netizens to obtain a huge amount of "data traffic", and then turning the "data traffic" into economic benefits.

3.2.2. Popular psychology.

Most cyberbullying begins with negative and malicious assumptions. Today's fast-paced life makes people accumulate negative emotions, lack of optimism, doubt society and others, and feel insecure. As a result, bystanders who do not know the truth mistakenly piece together the fragmented information with their own imaginations, and blame others from the perspective of God. The mass psychological mechanisms of this status quo include network disinhibition and collective unconscious release. In psychological research, "inhibition" refers to various phenomena such as individual behavior being constrained by self-consciousness, maintaining a certain level of anxiety in social situations, and caring about people's evaluations. In contrast, "disinhibition" refers to the reduction of an individual's self-consciousness. Because of the secrecy and openness of the Internet, people will take advantage of the freedom of the Internet to publish what they are afraid to say in real life on the Internet. Netizens who use the Internet as a decompression valve are more likely to have aggressive behaviors and it is easy to reveal one's own personality characteristics and even corresponding weaknesses. This is also a manifestation of the disinhibition of the Internet, where they can vent their emotions without any scruples. For example, many netizens subconsciously compare their frustrations in real life with the good lives of others, and the resulting gap is concentrated on the collective with the label of happiness through verbal attacks and abuse, and even goes beyond the moral boundaries, causing serious impacts on others.

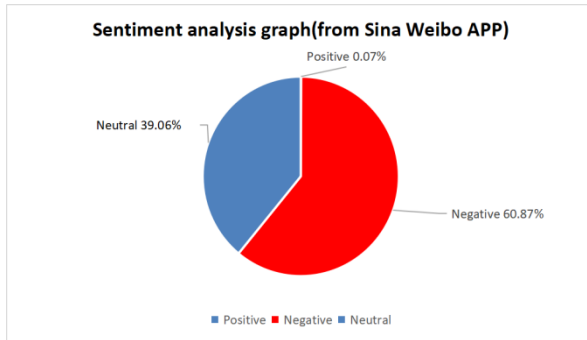


Fig. 1. Sentiment analysis graph (from Sina Weibo APP)

3.3 Technical level

According to the "Regulations on the Management of Internet User Account Names" issued by the Cyberspace Administration of the People's Republic of China, those who currently speak through public platforms such as Internet social networking require network users to register with their real names in advance. However, the crux of the problem is that the information registered by network users on the platform is not all real personal information. Under the premise of not stipulating that the platform has a high censorship obligation and cannot break technical barriers, when cyber violence occurs and the rights of the parties are infringed, the party whose rights are damaged cannot obtain the real information of the perpetrator. It is difficult to preserve relevant evidence, and it is unfair to the injured party in terms of rights relief. Moreover, in the process of determining the infringer, the perpetrator may also modify or delete the previously forwarded information in order to avoid responsibility. As a result, the original evidence is often destroyed. It is usually difficult to fix the evidence for rights protection by the parties alone, and the use of data recovery and other technologies will be time-consuming and labor-intensive, resulting in high costs. In this way, the issue of forensics will become the unavoidable focus of cyber violence incidents. The lack of technology in investigation and evidence collection has also indulged the breeding of cyber violence from the side.

More and more platforms adopt a combination of AI technology and manual review to filter information, guide users to reflect and revoke their comments, and thus resist the occurrence of cyber violence. It is true that AI technology has provided great help from the source for creating a clear network environment, and it is extremely efficient. However, there will still be many netizens expressing bad speech through homophony and separators to avoid technical monitoring, and most platforms only stay in the rapid processing of text, and cannot quickly deal with expression media such as pictures and videos. It can be seen that the technology still has much room for improvement and development.

4 Countermeasures and Suggestions for Cyber Violence Governance

4.1 Construction of laws and regulations

In order to govern the cyber violence, governments of various countries have formulated corresponding laws and regulations, and their legislation mainly regulates cyber violence and the underground industry that may exist behind it in terms of protecting citizens' rights and obligations, protecting citizens' information security, computer network crimes, children's Internet protection, and cyber bullying.

Since 1997, a series of related laws and regulations have also been established in China, including the governance of cybercrime, internet underground industry, and unfair cyber competition, as shown in Table 2.

For small tables, please place it within a column and bigger table be placed in a text frame spanning to both columns. Use the Table facility available within the MSWord. The font in the row header should be bold and you can use the style available from the style palette.

Table 1. Existing Legal Regulations for Governing Cyber Violence

Legal documents	Time	Legal documents	Time
Decision of the Standing Committee of the National People's Congress on Safeguarding the Security of the Internet		2000	
Regulations on the Administration of Internet Electronic Announcement Services		2000	
Self-discipline Convention on Civilized Internet Access		2006	
Judicial Interpretation on Handling Criminal Cases of Defamation by Using Information Network		2013	
Opinions on Several Issues Concerning the Application of Criminal Procedures in Handling Cybercrime Cases		2014	
Law of the People's Republic of China on Network Security		2016	
Measures for the Administration of Internet Group Information Services		2017	
Law of the People's Republic of China on Anti-Unfair Competition		2019	
Provisions on the Ecological Governance of Network Information Content		2019	
Law on Data Security		2021	
Opinions on Strengthening the Construction of Network Civilization		2021	

In the context of the current vacancy in China's anti-cyber violence special law, China can learn from the basic principles of foreign Internet legislation, such as the principle of free entry. The "freedom" of this principle is not unprincipled freedom, but through real-name authentication, netizens information registration and other forms to register the personal information of netizens in a register to prevent and control the online violence of netizens; For example, the United States has formulated the principles of responsibility for the classification of information dissemination content and the protection of citizens' personal data. These principles strengthen the civic responsibility system, strengthen accountability and governance, strengthen the pro-

tection of citizens' personal information and prevent the leakage of netizens' information, and prevent the wanton dissemination of false information on the Internet. Different from the earlier development history of the Internet in some foreign countries, in China, the definition and legal regulation of some network chaos is still relatively lacking. Therefore, the legislation of relevant foreign network regulations has a great impact on regulating the network environment. For reference, the author thinks that our country can start from the following points: realize the real-name system on the Internet as soon as possible, which will help netizens to consciously regulate their own behavior, and also help to hold accountable afterwards; to a certain extent, to supervise network behavior, this does not mean to prohibit freedom of speech, but to put an end to the possible problems of cyber violence and criminals who may use the internet to disturb the social stability of our country. It is necessary to focus on the online behavior of children and adolescents. Children and adolescents, as the mainstay of the country's future development and the hope of national rejuvenation, are the most creative and energetic, but at the same time, due to their immature mental development, they are likely to be deceived or fall into cybercrime, the abyss of cyber violence.

To sum up, this paper hopes to build and improve China's anti-cyber violence legal system by learning from foreign laws and regulations on cyber violence. At the same time, we should also realize that we still have a long way to go on the road of cyber violence and even cyber behavior norms.

4.2 Vigorously promote the online real-name system

The online real-name system refers to a system in which netizens must use their real names and ID numbers to register on the website before they can express their opinions on the Internet. In foreign countries, many countries have already started to study how to create a healthy network dynamic environment through the network real-name system. The European Union began to study network identity management in 1998. In 2006, it proposed to use biometric technology to verify the identity of eID holders. Since then, the European Union began to implement eID in its member states to solve identity authentication, authentication and electronic signatures in network applications, privacy protection and other issues. In 2006, Japan implemented the hidden real-name system through the binding of mobile phone-SIM card-ID card/driver's license-e-mail. The Obama administration of the United States promulgated the National Strategy for Trusted Identity in Cyberspace (NSTIC Strategy) in 2011, which is led by private enterprises to establish a user-centered identity ecosystem, and strive to realize the dynamic whole-process management of network real identity. In order to solve the problems of identity theft, privacy leakage, network fraud and other illegal and criminal problems in cyberspace.

The author believes that the introduction of the real-name system is still the general trend. The overall advantages of this move outweigh the disadvantages, and it is more conducive to purifying the country's Internet ecological environment. In fact, the real-name system does not restrict all the freedoms of netizens. It does not directly require users to use their real names to walk on the Internet, but records the user's real-name

information in the network background and saves it in the background. Therefore, netizens can still use "vest" and "nickname" as their codenames to express their opinions as before, so this is no different from the previous anonymous way. There will be no question of restricting freedom of speech. Only when netizens publish infringing or illegal information, the platform will take the initiative to check your real information and deal with it according to the severity of the speech. Under this system, both network operators and state authorities can directly track down and verify the true identities of netizens, and force the background to delete their bad remarks, and hold netizens accountable depending on the severity of the incident. The implementation of the real-name system will truly allow netizens to respect laws and regulations again, regulate their behaviors in accordance with Internet standards, and truly purify the Internet environment.

4.3 Innovative technical means to filter out bad information

At present, the means of Internet governance in developed countries can be roughly divided into three categories: one is the classification and filtering of Internet content. For example, the United States adopts the PICS (Platform for Internet Content Selection) technical standard protocol to scientifically search and design web content according to the classification method; Australia has passed the content classification, and has restricted the age of some netizens who watch over-grade Internet content through the identity verification system. The second is to invest a lot of money in the research and development of Internet information security technology. The third is to actively develop and promote relevant software for monitoring online public opinion. For example, public departments such as schools in the United States use network filtering software; Singapore's "Family Access Network" aims to filter pornographic information, protect minors, and enable minors to form a correct online environment in a healthy network environment. values.

In view of the current situation of the country's reputation for cyber violence and insufficient technical governance, we can strengthen technical means to prevent cyber violence from the following aspects.

4.3.1. Establish a new cyber violence monitoring system.

We should focus on the monitoring of various social software on the mobile side. The life cycle of online public opinion crisis from occurrence to demise is regular. Only by grasping each development stage of public opinion crisis can effective management be implemented. First, in the germination period of online violence, we need to establish a network early warning and monitoring system. The system should focus on accurate identification and treatment. By analyzing abnormal behaviors in user comments, bullet screens and other links, comprehensively reporting the number and frequency, monitoring, judging, and early warning of the incentives that cause cyber violence or other crises, discovering problems in time, controlling the source of transmission, and stifling cyber violence in its germination in the cradle. Second, when cyber violence has spread to a certain stage, causing a public opinion crisis in a

certain range, it is also necessary to timely and accurately reflect the current public opinion development status through the network monitoring system, and analyze the current mood of netizens through algorithms to prevent the crisis from further expansion and avoid "The Broken Window Effect" occurs. Third, when the cyber violence has reached the late stage and the situation has stabilized, we need to sort out the context of the entire incident in time through detection records, and sum up experience and lessons. And it is necessary to improve monitoring and identification, traceability and accountability, so that netizens who hide in the dark and make hurtful words have nowhere to hide, receive corresponding punishments, and play a warning role. And it is necessary to pay attention to whether there is any residual negative information that may be copied and forwarded continuously, causing subsequent impacts.

4.3.2. Establish strict, clear and practical Internet grading standards.

At present, the technical means we can currently achieve is to use the monitoring, filtering, tracking, blocking, processing and other functions of network intelligence software technology to control and guide the trend of network public opinion, and to eliminate the impact of negative information in a timely manner. However, this "one-size-fits-all" approach of keyword filtering and content blocking is not only inefficient but also very passive. We can learn from the experience of the United States and other countries, and combined with the current situation in my country, establish a scientific and complete grading system according to the content of network communication, and then combine with today's powerful monitoring and filtering technology to achieve better results.

4.3.3. Increase investment in research and development of network security technologies.

For the governance of online violence on the mobile side, we need to cultivate a team of network technology professionals, including professional mobile network public opinion analysts, who can provide professional mobile network public opinion analysis, predict the trend of public opinion, and provide opinions on handling network public opinion. Provide support for emergency handling, tracking and resolution of terminal network public opinion. With the help of technical research and development and capital investment of management and control methods, efforts should be made to improve the technical means, level and coverage of network management, and fully apply the technical means to public opinion analysis, netizen control and management, and IP address query of the network, especially the mobile Internet.

5 Conclusions

Cyber-violence is seriously poisoning the people, damaging the atmosphere of the Internet, and endangering the public order of the Internet. At present, there are problems such as insufficient legal regulation of cyber violence in my country, lack of awareness of infringement among netizens, and imperfect technology, which has led

to many lawbreakers exploiting loopholes and acting recklessly for the sake of attracting attention. By analyzing the current situation of cyber violence in China and drawing on foreign experience, this article believes that at the level of legal regulation, it is necessary to clearly regulate cyber violence through special legislation and clarify the legal responsibility of the subject; at the level of law enforcement and justice, it is necessary to further improve judicial interpretations, and strictly implement the network real-name system, strengthen the supervision of network platforms; at the technical level, we should establish a new network violence monitoring system, a strict, clear and feasible Internet classification standards, and increase the research and development of network security technology.

Acknowledgments

This work was supported by the National Social Science Foundation of China under Grant No. 21BSH051.

References

1. Hua, Zhenzhen. (2017) The governance dilemma and legal regulation of cyber violence. *Journal of Hubei University of Economics*, 14: 84-86.
2. Wang, Yang. (2018) Concept Definition of Cyber Violence from the Perspective of Public Domain. *News Research Guide*, 9: 92-93.
3. Yang, Yancheng. (2016) Discussion on the Definition and Classification of the Language of Cyber Violence. *Journal of Hunan University of Science and Engineering*, 37: 170-173.
4. Li, Huajun. (2017) Research on the Development of Network Violence: Intension and Type, Status Characteristics and Governance Measures. *Journal of Intelligence*, 36: 139-145.
5. He, Jiaqi. (2016) Taking Weibo as an Example to Analyze the Current Situation and Standardization of Internet Violence. *Theory Research*, 24: 5-6.
6. Tian, Shengbin. (2020) Identification and regulation of cyber violence from the perspective of social governance. *Journal of South-Central University for Nationalities*, 40: 168-173.
7. Wang, Tiannan. (2019) Analysis of the Development Trend of Cyber Violence and the Way of Governance. *Journal of CAEIT*, 40: 917-923.
8. Li, Xiaolin. (2021) Research on the causes and prevention measures of cyber violence from the perspective of new media. *Psychological Monthly*, 16: 213-215.
9. Xiang, Yushan. (2020) Analysis of coping strategies from the causes of social network violence—Taking Weibo hot events as an example. *Crisis Management and Communication Strategies*, 1: 159-161.
10. Wang, Manrong. (2009) Research on the formation mechanism and governance counter-measures of cyber violence. *Lanzhou Academic Journal*, 194: 148-151.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

