# Exploring the Causes and Countermeasures of Cyber Violence in the Internet Era

# Xiaoyu Cao<sup>1,a,\*</sup>

<sup>1</sup>Faculty of Arts and Social Sciences, University of Malaya, Kuala Lumpur, 50603, Malaysia a. s2039174@siswa.um.edu.my \*corresponding author

Abstract: In this current Internet era, the Internet is very popular and almost everyone is using it. However, some problems have arisen from this, and cyber violence is one of them. Today, cyber violence is happening more and more. Therefore, this article will study the causes of cyber violence and the countermeasures for cyber violence. This study provides an insightful and comprehensive study of cyber violence and broadens the research on cyber violence. Finally, it is found that the causes of cyber violence are: First of all, The virtuality and anonymity of the Internet. Secondly, some information media and netizens disseminate information irrationally. Thirdly, the relevant laws and regulations are not perfect. Fourthly, the supervision of Internet platforms is not in place. Fifthly, Internet users are getting younger. The countermeasures for cyber violence are: Firstly, improve the regulatory policies and laws for cyber violence. Secondly, the Internet platform should improve the regulatory strategy. Thirdly, improve the network public opinion supervision and platform reporting system. Fourthly, strengthen the early warning of public opinion and the guiding role of mainstream media. Fifthly, improve the rule of law and moral cultivation of Internet users.

**Keywords:** cyber violence, causes and countermeasures, internet era

#### 1. Introduction

The Internet is an interactive platform that enables mutual communication and participation. The Internet is the most efficient, inexpensive, intuitive, and quick way to convey an idea or information. Today is the Internet era, the Internet is very popular, the Internet has penetrated more cheaply to everyone, almost everyone can enjoy this high-speed information transmission method at an extremely low cost, and the use of the Internet has become a universal way of life. Because of the development of the economy, technology, etc., the Internet is very popular. Taking China as an example, according to "The 50th Statistical Report on China's Internet Development", as of June 2022, China had 1.051 billion internet users and a penetration rate of 74.4% (as shown in Figure 1). At the same time, the Internet can exchange information without space restrictions, and people and information can interact and communicate with each other, with fast updating speed and satisfying personalization, which is deeply loved by people. However, in the Internet era where the Internet is very popular, many social problems have also arisen, such as cyber violence, which is one of the most serious social problems. Cyber violence is the abuse, defamation, bashing, and insulting of the victim via the Internet while posing a threat to or otherwise negatively affecting their right to privacy, personal safety, and their ability to go about their daily lives. Cyber violence is often committed

© 2023 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

through the use of e-mail, online games, instant messaging, and community sites to annoy and taunt others. For example, in the name of "funny", some people create videos, pictures, and emoticons that vilify others and spread them widely, causing great distress to the people concerned; some people use social hotspots to turn normal differences of opinion into geographical discrimination and gender confrontation and to attack people with different views. The participants of cyber violence include unknown groups or individuals. Victims of cyber violence usually do not tell their family and friends that they have suffered from cyber violence. Studies have shown that most cyber violence, such as malicious video clips, can cause both physical and psychological damage to the victims [1]. As the Internet is very popular, almost everyone uses the Internet, so cyber violence is even more prevalent. Therefore, it is necessary to study the causes of cyber violence in the Internet era as well as the countermeasures.

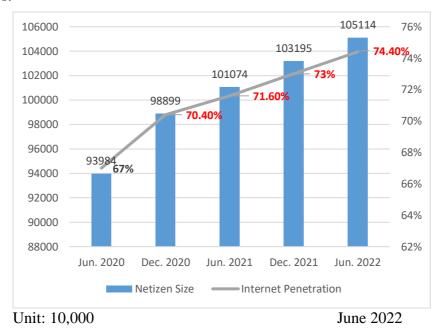


Figure 1: China's Netizen Size and Internet Penetration [2].

# 2. Literature Review

In the 1990s, computers began to spread significantly, and the Internet came into millions of homes. Due to the proliferation of Internet users, behaviors that violate ethical norms on the Internet often occur, and cyber violence gradually emerges. Researchers have focused on two aspects of cyber violence: on the one hand, they have focused on the problem of cyber violence among two vulnerable groups, namely, teenagers and women. On the other hand, research on the governance of cyber violence has mostly used legal methods to safeguard the reputational and privacy rights of Internet users and control their conduct through legal regulation. For example, South Korea has implemented the "Real Name Internet System" and Japan has enacted the "Anti-Hacking Law" and the "Youth Internet Environment Improvement Law".

French social psychologist Gustave Le Bon's book "The Crowd: A Study of the Popular Mind" has enlightening significance for the study of cyber violence." This book introduces the emergence of popular psychology in detail: "The characteristics of group and group psychology point out that when a person appears as an individual, he has a distinct personality, and when he blends into a group, all of that person's personality will be absorbed by that group, and his thinking will be replaced by the thoughts of the group, even if this thought is extremely absurd, and when a group exists, he will have the traits of emotionality, dissimilarity, and low IQ and will appear "impulsive", "blind",

"fanatic" and other characteristics, which is also the most concentrated expression of cyber violence [3]. "The self-serving bias theory proposed by Thomas Gilovich, on the other hand, rationalizes the reality of cyber violence in which some Internet users who have a hatred of the rich would blame everything on social injustice [4]. Byung-Chul Han pointed out in the book "Im Schwarm: Ansichten des Digitalen" that digital communication stimulates instantaneous impulsive responses, while the virtuality of the Internet makes people lose their authenticity [5]. The German sociologist Ulrich Beck wrote in "Risk Society: Towards a New Modernity" that "the individual practical activities of human beings affect the security of society as a whole, and the more frequent human activities are, the greater the risks they pose, and the more dangerous the risk structure becomes from normal and manageable, and the more sensitive and vulnerable society becomes with this signal of danger [6]." This explains very well why the Internet becomes unsafe and why cyber violence is frequent: the high frequency of human use of the Internet is a major objective factor in the creation of cyber violence, and the variability of human minds leads to different attitudes in the face of the same events, behavior becomes unpredictable as more and more people are exposed to the same events.

In today's Internet Era, cyber violence is becoming more and more prevalent, so scholars from various countries are seeking to explore solutions to cyber violence. Canadian Information Processing Society has established ethical guidelines: "to improve the knowledge of the general public, to publish relevant opinions in relevant fields, not to withhold information, not to publish false information, not to publish misleading information, not to use other people's information freely, to follow the appropriate regulations, and to govern cyber violence with the same connection between cyber ethics and social ethics [7]." In his book "The Future of Reputation: Gossip, Rumor, and Privacy on the Internet," American jurist Daniel J. Solove seeks to strike a balance between the rights to privacy and the freedom of speech, contending that "the law should play an important role in governance in the face of online rumors, human flesh search, and other serious violations of people's rights and freedoms [8]." In "Cyberethics: Morality and Law in Cyberspace," American scholar Richard A. Spinello proposes that three major principles should be followed when confronting cyber problems: "harmlessness (not to use information technology to violate the legitimate rights and interests of others), autonomy (respecting the legal rights and interests of cyber participants), and informed consent (clear consent of rights holders before using their information) principle, which is the fundamental principle to address cyber violence [9]."

#### 3. Causes

The causes of cyber violence include the followings:

# 3.1. The Virtuality and Anonymity of the Internet

The frequent occurrence of cyber violence is inseparable from the characteristic of the Internet, the most prominent characteristic of the Internet is its virtual and anonymous nature. On the Internet, people are in a virtual communication scenario, and Internet users speak anonymously. The norms and constraints that should be followed in real life are lost in network communication, and Internet users do not have to take responsibility for their behavior, and the risk tends to be zero. Therefore, the sense of responsibility and legal awareness of Internet users is greatly reduced, and they can easily break through the moral bottom line and express their opinions emotionally. When stimulated by a certain event, many Internet users are in an irrational state, and they can't wait to attack the person concerned, showing their discontent and anger.

# 3.2. Some Media and Netizens Disseminate Information Irrationally

In recent years, with the continuous progress of network technology, the types of new media have become increasingly diverse, and all kinds of public numbers and so on have emerged. Among them, there is no lack of adding subjective opinions in front of objective facts, leading viewers astray, deliberately amplifying and highlighting the contradictions in events to gain attention and increase the number of readers and click-through rates. After the dissemination and superposition of multiple parties, what viewers see is often different from the facts, or even contrary to the line, which makes some radical netizens launch online denunciations and ferment into cyber violence. Why are some netizens so radical? Cass R. Sunstein first introduced the concept of "information cocoons" in 2006 in his book "Infotopia: How Many Minds Produce Knowledge". He pointed out that because the public only pays attention to its own needs and interests, it can, over time, confine itself to a "cocoon" of self-imposed isolation. When different voices challenge the three views, some people will be eager to prove it and become radicalized, a phenomenon that is very common on the Internet [10]. The irrational venting of negative emotions by netizens is also the cause of cyber violence. People sometimes accumulate negative emotions in life and work, and because they have no way to vent in real life, they will vent irrationally to the parties involved in cyber violence. Cyber violence caters very well to the inner activities of such emotional catharsis.

#### 3.3. The Relevant Laws and Regulations Are Not Perfect

The network society is an extension of the real society through network technology and is a projection of the real society on the network. The Internet era has formed a situation where everything is connected and should be managed under the law. However, in the process of building and improving the legal system, there will be certain loopholes in the law, this is because in the process of the rise and development of the Internet due to the rapid changes in network technology, the improvement of the law cannot keep up with the development of the network, so the legal loopholes arise, and these loopholes allow many unscrupulous elements to exploit the loopholes. "Cyber violence is usually a mass event, and the participants often include thousands of Internet users, which makes it difficult to legislate [11]. Moreover, the participants of cyber violence are very abstract and non-specific, so even if there are relevant laws, it is difficult to implement them procedurally.

# 3.4. The Lack of Supervision of Internet Platforms

In today's Internet era, people of all kinds can voice their opinions online, and there is no threshold for publishing information on various online platforms, which allows many people to publish subjective and one-sided content and even induce misunderstanding of information. In today's very popular self-publishing industry, for example, to ensure their operations, many self-publishing platforms are very "simple and brutal" in their requirements for contracted subjects, regardless of quality, as long as they can attract attention. To enhance the commercial value, the operating platforms rack their brains to enhance the click rate and reading volume through various "odd" information and eye-catching titles and use capital means to make malicious hype. Some contracted Internet celebrities brainwash netizens to manipulate the public's perception of public opinion, continue to stir up incidents, and guide violent public opinion. Due to the inadequate supervision of the Internet platform, these violent public opinions cannot be resolved promptly, which eventually leads to the emergence of cyber violence.

# 3.5. Internet Users Are Getting Younger

The popularity of the Internet has allowed more minors to have access to outside information. However, due to the immature mental development of minors, their views on certain issues are too immature and they are easy to blindly follow suit and be used by others. At the same time, due to Internet users getting younger, there will inevitably be problems with low education levels. Some minors do not fully understand legal knowledge and have a shallow understanding of legal concepts, so they carry out cyber violence at will, which is also a reason for cyber violence.

# 4. Policy Implications

The author of this paper believes that several countermeasures should be taken to governance cyber violence as follows.

# 4.1. Improve the Regulatory Policies and Laws for Cyber Violence

For example, laws should be introduced specifically to control cyber violence, which can allow cyber violence to be addressed in a more targeted manner. Or introduce relevant laws and policies to govern the problem of cyber violence. Take China as an example, China has formulated and introduced the Data Security Law and the Personal Information Protection Law, thus providing legal protection for data security and personal privacy protection at the legal level. The data property rights protection system is further improved in the operation mechanism to provide institutional guarantees for the data security of users and the protection of personal privacy and personal information. This effectively protects the data security of Internet users and can effectively prevent the occurrence of cyber violence.

# 4.2. The Internet Platform Should Improve the Regulatory Strategy

Let cyber violence happen nowhere under the perfect supervision of the Internet platform. For example, the Internet platform can require users to have real-name authentication, and only users who carry out real-name authentication can use it. After Internet users perform real-name authentication, they will be responsible for their remarks. Because of the real-name authentication, when they publish defamatory or insulting remarks, the Internet platform can directly find out their personal real information based on their account information and then punish them.

# 4.3. Improve the Network Public Opinion Supervision and Platform Reporting System

Internet users should be encouraged to exercise their right to monitor public opinion and encourage real-time supervision of the Internet environment. At the same time, the reporting system of the network platform should be improved, once the occurrence of cyber violence should be reported in time, which can quickly curb cyber violence.

# **4.4.** Strengthen the Early Warning of Public Opinion and the Guiding Role of Mainstream Media

In the Internet era, strengthening the early warning mechanism of public opinion and the guiding role of mainstream media is an effective measure to prevent and control online rumors and stifle all kinds of cyber violence. Early warning and effective monitoring and channeling of public opinion can make mainstream public opinion and positive energy occupy the mainstream of public opinion [12]. Sudden cyber violence is a long-term accumulation of social conflicts, which to a certain extent reflects people's needs and voices at a certain stage of society. If government departments establish a long-

term mechanism for monitoring and analyzing online public opinion, they can regulate prominent social contradictions by proactively identifying problems, thus easing the tension of social opinion and avoiding the development of online public opinion in the wrong direction. There should be full cooperation between governmental network supervisory departments and network opinion monitoring departments to strengthen contact and communication. Based on fully understanding and effectively analyzing public sentiment, the development trend of online public opinion should be predicted. Through analyzing the collected information, the government should predict the development trend of public opinion and deal with various online emergencies and keep good data on this basis to provide a reference for the next governance.

# 4.5. Improve the Rule of Law and Moral Cultivation of Internet Users

In real life, Internet users are the main pushers of cyber violence. Therefore, on the Internet, Internet users should view social phenomena from a rational perspective, be restrained and keep the bottom line when making comments on the Internet, and also improve their ability to distinguish right from wrong and their immunity to vulgar culture. Internet users should also pay attention to avoid exposing private information on the Internet and strengthen the protection of personal information.

#### 5. Conclusion

In today's Internet era, cyber violence is happening more and more. The reasons for the occurrence of cyber violence are: First, the virtuality and anonymity of the Internet. The second reason is that Information media dissemination distorts the truth and irrational venting of negative emotions by netizens. The third reason is the relevant laws and regulations are not perfect. The fourth cause of cyber violence is the lack of supervision of Internet platforms. The fifth cause of cyber violence is that Internet users are getting younger. In the face of the problem of cyber violence, the following countermeasures should be taken: First, Improve the regulatory policies and laws for cyber violence. Second, The Internet platform should improve the regulatory strategy. Third, Improve the network public opinion supervision and platform reporting system. Fourth, Strengthen the early warning of public opinion and the guiding role of mainstream media. Fifth, Improve the rule of law and moral cultivation of Internet users.

This study studies the causes of cyber violence and puts forward some suggestions for the governance of cyber violence. Therefore, this study deeply and comprehensively studies cyber violence, which will help more people understand cyber violence in-depth and allow more people to have a more comprehensive understanding of the causes and countermeasures of cyber violence, so this research has profound significance.

#### References

- [1] Kalesan, B., Weinberg, J., & Galea, S.: Gun violence in Americans' social network during their lifetime. Preventive Medicine, 93, 53–56 (2016).
- [2] The 50th Statistical Report on China's Internet Development. China Internet Network Information Center (CNNI C), (2022). Retrieved 7 April 2023, from https://www.cnnic.com.cn/IDR/ReportDownloads/202212/P02022120934 4717199824.pdf
- [3] Gustave Le Bon.: The crowd: a study of the popular mind. New York City, N.Y. Wallachia (2015).
- [4] Pronin, E., Gilovich, T., & Ross, L.: Objectivity in the Eye of the Beholder: Divergent Perceptions of Bias in Self Versus Others. Psychological Review, 111(3), 781–799 (2004).
- [5] Han, B.C. Im Schwarm. Berlin. Matthes & Seitz Berlin Verlag (2015).
- [6] Beck, U.: Risk society: towards a new modernity. London. Sage Publications (1992).
- [7] Canadian Information Processing Society. Internet Code of Conduct. 20-22 (1994).
- [8] Solove, D. J.: The future of reputation: gossip, rumor, and privacy on the Internet. New Haven, Conn.; London. Yale University Press (2008).

# Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries DOI: 10.54254/2753-7048/16/20231102

- [9] Spinello, R. CYBERETHICS: morality and law in cyberspace. S.L. Jones & Bartlett Learning (2020).
- [10] Sunstein, C. R.: Infotopia: how many minds produce knowledge. New York; Oxford. Oxford University Press (2008).
- [11] Song, M.: On the Causes and Legal Regulations of Cyber Violence. HEILONGJIANG UNIVERSITY OF TECHNOLOGY. 23(2), (2023).
- [12] Li, G.: The Current Situation, Causes and Governance of Cyber Violence in the New Media Era. Media Forum, 106(10), (2022).