Available Online: 27 January 2026 DOI: 10.54254/2753-7102/2026.31497

Analysis of criminal law regulation on defamation by cyber water army

Jiaqian He

Law School, East China University of Politics and Law, Shanghai, China

23010101158@ecupl.edu

Abstract. With the development of information network technology, crimes in cyberspace are also increasing. In view of the defamation behavior of using the cyber water army, it is found that it has the development trend of industrialization and concealment, and its serious harm to social order and individual rights and interests. By analyzing the characteristics of defamation in the cyber water army, which are different from traditional defamation in behavior mode and communication mechanism, this paper points out the difficulties faced by the current criminal law in subject identification, plot standard and prosecution procedure. Therefore, it is proposed that people should clearly crack down on the main sponsors and active participants, set quantifiable standards of seriousness of the circumstances, and promote the lowering of the threshold of public prosecution and the improvement of related crimes, so as to build a governance path that takes into account both the cracking effect and the modesty of criminal law.

Keywords: cyber water army, defamation, cyber bully

1. Introduction

With the deep embedding of information network technology and the digital transformation of social communication mode, crimes in cyberspace are becoming increasingly rampant, especially the crimes of cyber water army, which are developing in industrialization and concealment. Using it to spread false information to damage the reputation of specific objects has become a social public hazard that needs urgent attention, and its harm is far from being covered by traditional defamation crimes. From commercial defamation to personal attacks, such behaviors seriously erode network order and market fairness. For example, the "Xiao Huijun case" and a series of false accusations that have spread all over the network before, although the judicial judgment has cleared the parties, the life and career of the slanderers harassed by the cyber water army in recent years have suffered a great blow, whether it is economic loss or reputation infringement. Another example is the "NIO-Tesla Cyber Water Army" incident, which is a typical unfair commercial competition by discrediting rival products. Many cases have shown that the defamation of the cyber water army is not a simple dispute of reputation or interests but has been transformed into a precise attack on isolated individuals by systematic forces such as capital and flow, and has become an organized social infringement. Faced with this new threat, the traditional defamation crime is faced with severe application difficulties in the identification of the subject of the crime, the assessment of the harmful consequences and the prosecution

procedure, which leads to the inefficiency of the current criminal law regulation system with the traditional defamation crime as the core. The purpose of this paper is to focus on the special subject of "cyber water army", to explore the evolution and application dilemma of traditional defamation crime in the network environment, and to try to build a regulatory system that can not only crack down effectively, but also abide by the principle of modesty of criminal law, in order to provide useful intellectual reference for criminal trial practice to effectively punish the organizers and core participants of the cyber water army in dealing with increasingly complex network violent crimes, and to explore a systematic regulatory path.

This paper adopts the methods of comprehensive analysis and comparative analysis, from the phenomenon to the essence. Firstly, it defines the core concept of "cyber-water-army defamation", clarifies its function principle, and distinguishes the difference between cyberspace communication and traditional information communication, as well as the result of this difference on "crime of defamation". Combined with the summary, the existing experience and shortcomings are discussed, and finally the further improvement path is put forward.

2. The basic theory of defamation by using the cyber water army

Since scholars want to link the behavior of the cyber water army to the crime of defamation, it is natural to make clear the constitutive elements of crime of defamation first. First of all, the object of defamation crime is the personal dignity and reputation right of others (it must be a specific natural person). Secondly, the objective aspect of the crime is to fabricate (fabricate out of thin air) and spread (face the majority and not limit the way) some fictional facts, which is enough to damage the personality or reputation of others (who are required to be able to obviously infer the person referred to), and the circumstances are serious (specific to social networks, there are special provisions); Then, the subject is the general subject; Finally, the subjective requirement of this crime must be intentional (including having clear knowledge that the act is sufficient to and recklessly allowing such consequences to occur). It should be noted that the specific motive does not affect the establishment of the crime but is considered as a sentencing circumstance.

2.1. The behavior pattern of defamation by using the cyber water army

The cyber water army exists on the basis of the Internet. The virtuality, pluralism, immediacy and interactivity of the Internet provide the environment and foundation for the deformation of Internet language symbols, so taking this as the origin, the network interaction gradually slides to network violence, and this violence is further strengthened by the immediacy and pluralism of the Internet [1]. The cyber water army takes advantage of this. Usually, false or hard-to-distinguish contents will be collected or manufactured to attract public attention, during which these contents will be spontaneously deconstructed by Internet users and form groups with different views; Then, hot topics will be created by making use of the public's psychology of pursuing sensational and juicy gossip and the "contradictions" among the pre-existing groups. At this time, a group of "opinion leaders" will emerge to guide the direction of public opinion, put a label on someone, and create confusion. In more cases, it may affect the actual interests of the victims, especially in situations related to strong reputation, such as commercial wars and other market competition links, and sometimes it will become props for public figures to establish a specific image to compete for a certain resource [2]. This also shows that it has moved away from simply damaging its reputation, but towards some means of unfair competition.

2.2. The characteristics of this model

Because of the special carrier based on the Internet, the cyber-water-army defamation shows the double extensibility in time and space and the coincidence of organized and unorganized. The scale and rapidity of network information dissemination led to the double extension of time and space of cyber water army defamation. As a kind of cyber violence, cyber-water-army defamation, with the help of internet social media, can easily become powerful in a short time, leading to the exponential spread of a certain information in a very short time; This also means that the scope of communication is uncontrollable and unpredictable, which further strengthens its special field effect of public opinion and brings spatial extensibility different from the traditional defamation model [3]. In addition, the Internet space, in which words, pictures and videos are the main media of information dissemination, also makes it difficult for information to be completely deleted once it is disseminated, leaving almost permanent traces. Although this trace may not be easily touched by the public, this feature means that the network-based defamation can transcend the time limit, and a topic that has not been "detonated" before will be turned out several years later and "cooperated" with new information content to become another "explosion point". This double extension makes traditional remedies such as "eliminating the influence" ineffective, thus strengthening the importance of pre-risk prevention.

The anonymity of cyberspace brings about the combination of organized and unorganized network water forces. Due to the imperfection of the real-name mechanism and the decentralized nature of cyberspace, the cyber water army is in a special field characterized by anonymity, which determines that in this violent mode, the perpetrators and victims are alienated, which is further manifested in the verbal attacks or encirclement of individuals by netizens, and is covered with some kind of "spontaneity" fog [4]. However, in fact, Internet users often fall into a state of being an unorganized mob. Compared with the real space with distinct identity, the individual's speech is more trapped by the group and tends to follow suit. This will eventually lead to the discussion of a topic, although a specific viewpoint community can be deliberately created, but the process that really leads to its growth and alienation is often uncontrolled.

3. The criminal law regulation dilemma of using the cyber water army to defamation

3.1. Disagreement of the target

There is no doubt that the defamation of the cyber water army type belongs to joint crime, but the "common intention" required by the traditional joint crime theory will encounter obvious proof problems when dealing with the water army model. It is extremely difficult to prove whether many unknown members of the water army can be called criminal contact with the initiators. Cyber-water-army defamation usually involves many subjects, such as initiators (employers), organizers (leaders of water-army), concrete implementers (members of water-army), and netizens who account for a large proportion in number and are trapped or deceived. This has also led to a serious limitation of the scope of criminal attacks against them, and often only the initial initiator can be investigated, but it is difficult to punish the organizers and active participants who play a key role in amplification. In addition, the rampant misconception that "the law does not blame the public" leads to the dilution of the responsibility of the violent actors in the cyber water army, which ultimately further leads to the difficulty of the victims in defending their rights because of the dispersion of legal responsibility [5].

In addition, the evasion and ambiguity of platform responsibilities cannot be ignored. There is an endogenous contradiction between the platform's traffic pursuit and the maintenance of network order, and its motivation to fulfill the "gatekeeper" obligation is insufficient [6]. As the field where cyber-water-army

defamation directly occurs, the platform may even let the water army do whatever it wants in pursuit of "heat". This is why some scholars support the platform's inaction to help the crime become a principal offender.

3.2. The standard of "serious circumstances" is unknown

In the face of the "false flow" of the water army's brush, the traditional standard of incrimination of defamation seems to be inadequate, and it is unscientific to judge the seriousness of the case only by digital standards [7]. At the same time, defamation information flows across platforms under the impetus of the water army and algorithm, and its harm scope and degree far exceed the legislative preset, resulting in insufficient penalty deterrence of imprisonment of less than three years. Compared with the crime of helping information network criminal activities, there has been a clear explanation, and the terms and requirements of serious circumstances have been clarified. However, because of the "previous crime" and the "new model", the cyber water army defamation is rarely really applicable, let alone a mature system. In addition, the diversity of harmful consequences of online defamation and the difficulty in determining repeated defamation also make it more difficult to determine the seriousness of the circumstances [8].

3.3. Obstacles to criminal prosecution

Now that it has been made clear that the defamation of the cyber water army is a precise blow to individuals by social systematic forces, it is inevitable that the practice of applying the private rights model to cyber violence crimes will be criticized. Due to practical obstacles such as difficulty in proof, high cost of private prosecution, and difficulty in locking the subject, there are many cases in which criminal law can hardly provide effective relief for victims in the regulation practice of cyber violence crimes. According to statistics, in 2022, the people's court received number of 618 criminal cases in the first instance, of which only 29 cases were prosecuted. In that year, a total of 587 cases were concluded, of which 271 cases were rejected, 110 cases were dismissed and number of 97 cases were allowed to be withdrawn, while only 79 cases were judged, accounting for one fifth. What's more, only 43 people were convicted [9]. The threshold of public prosecution is too high in view of the widespread concern about the defamation of the cyber water army, and because the standard of "seriously endangering social order" is also vague, it is often possible to be initiated only after the victim has suffered extreme personal or mental damage. This dilemma further makes the organizers and main participants who use the cyber water army to defame without fear.

4. Improvement of the criminal law regulation path of cyber water army defamation

4.1. Clear definition of the crackdown targets: initiators, active participants and omission-based accessory offenders

The criminal chain of defamation in the cyber water army is extremely long. By analyzing the degree of subjective malignancy, people should focus on the initiators and active participants, as well as the omission-aiding criminals to strengthen "pre-risk prevention". For initiators and active participants, a two-level governance logic is applied. Its specific contents mainly include: for the "single behavior is serious" network defamation, people should expand the explanation of the existing charges in the principle of legality through the path of interpretation; As for the cumulative defamation behavior of the water army, which is "the single act is not serious but the comprehensive consequences are serious", people should resort to the path of legislation and plug the punishment loophole by adding special charges [10]. Here, it is necessary to

distinguish between active participation and passive participation. The way to distinguish is whether to subjectively participate in the cyber water army with the purpose of harming others. This is mainly due to the modesty principle of criminal law. It is not appropriate to use criminal law for netizens with entertainment purposes and "sharing sensational gossip" mentality.

In addition, considering the governance potential of the platform for cyber-naval defamation, it is also necessary to improve the process supervision of the platform. As a participant and main beneficiary of risk manufacturing, the platform has the obligation of risk prevention that must match its social power. Similar reference models include helping the offender to become a principal offender or establishing and actively applying the crime of failing to fulfill the obligation of information network security management.

4.2. Setting quantifiable criteria for the severity of the plot

Take "causing serious consequences" as an objective constituent element, and make good use of the purpose explanation to take into account such behaviors as organization, using algorithms and cross-platform communication, and take the organizer's realistic purpose and the actual loss suffered by the victim as sentencing or aggravating circumstances, instead of just rigidly applying the number of clicks and forwards as the criteria for determining the seriousness of the circumstances. In this process, people can consider formulating the classification standard of cyber violence information, establishing a typical case base, and clearly defining the identification standard of cyber water army defamation, in order to attack the content and object more accurately [10].

4.3. Strengthening the allocation of punishment and lowering the threshold of public prosecution

In criminal law, special crimes related to cyber violence and defamation of cyber water army are added. This is because cyberspace has become an important part of daily life and will affect normal production activities and social order. This legal interest protection is important enough to require criminal law to establish new crimes, and this does not conflict with the promulgation of special departmental laws or field laws. In addition, at the judicial level, people should adopt a functionalist position, allocate the public prosecution procedure, expand the scope of public prosecution, or adjust the understanding of "handling only after telling" so that the victim can choose between private prosecution and public prosecution, so as to reduce the burden of proof for the victim. In addition, there are ways such as adding property punishment to compensate the victims directly with more direct and "visible" practical benefits.

5. Conclusion

At present, people live in a deeply networked society, and this is also the period when China society is transforming from tradition to modernity. Because of its openness, anonymity and decentralization, the Internet has become a place for the public to pursue entertainment and vent their emotions. In today's Chinese Internet, people's creativity in culture and entertainment has been deeply engraved in the hearts of every witness. However, the forms of violence brought about by cyberspace can never be ignored. As a malignant variant of cyber violence, the characteristics of organization, industrialization and technicalization of cyber-navy defamation pose a severe challenge to the regulation system of defamation in traditional criminal law. The core problems analyzed in this paper, such as the dilemma of subject identification, the lag of conviction standard and the difficulty of starting public prosecution, jointly reveal a fundamental problem, that is, the legal framework born in the offline acquaintance society has shown obvious inadaptability in dealing with

anonymous and large-scale malicious attacks online, and the mentality of "the law does not blame the public" has prevailed in it.

In view of this background, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued "Guiding Opinions on Punishing Cyber Violence and Crimes according to Law" in September 2023, and soon afterwards, the National Internet Information Office also issued "Regulations on Cyberviolence Information Governance", all of which aim at comprehensively controlling cyber violence and crimes and creating a clean and upright cyber spiritual home. However, the related problems have not been fundamentally solved. Judging from the seven typical cases released by the Supreme People's Court, the scheme it follows is still mainly to investigate the responsibility of illegal information publishers, and rarely involves the responsibility of those who forward, comment and like.

The core idea of the solution proposed in this paper is to promote the modern transformation of the criminal law regulation concept from "passive response and case handling" to "active intervention and systematic governance", whether it is to accurately crack down on the behind-the-scenes criminals through "accomplice behavior becoming a crime", to build a comprehensive evaluation system to restore the actual harm of the crime, or to activate the public prosecution procedure to relieve the victims. People can no longer regard the cyber water army as a scattered individual anomie, but must take it as a complete black ash production chain to carry out a legal "surgical" blow. In the final analysis, the governance of cyber-water army defamation is not only to protect every specific individual from the fall of reputation and spiritual suffering, but also to protect the integrity of the public cyberspace.

References

[1] Qin, B. (2025) Words, communities and regulations: multidimensional thinking on the generation of cyber violence. *Modern Communication, 47*(1), 44-53.

[2] Xu, J. (2021). Analysis on the influence of water army on public opinion on the internet. In *Proceedings of the 2021 3rd International Conference on Literature, Art and Human Development* (pp. 718–722). Atlantis Press.

[3] Lao, D. (2024). The basic position of the criminal law governance of cyber violence. *Forum on Political Science and Law, 42*(3), 39–54.

[4] Chen, M., Wang, Z., & Wu, H. (2024). Practical dilemmas facing criminal legislation on network violence and ideas for responding to them. *Journal of Politics and Law, 17*(4), 43–56.

[5] Li, X., & Zhai, Y. (2024). Cyber violence on digital platform: Evolution mechanism, governance dilemma and breakthrough path. *New Media and Society, 26*(4), 76–89.

[6] Wang, Y. (2023). The research on criminal legislation of cyber violence. *Lecture Notes in Education Psychology and Public Media, 15*(1), 173–178.

[7] Song, W. (2022). Judicial cognizance of other serious cases of defamation crime in cybercrime. In *Proceedings of the 2022 6th International Seminar on Education, Management and Social Sciences* (pp. 2883–2891). Atlantis Press.

[8] Zhou, J., Yu, H., & Li, Z. (2023). Understanding and application of guiding opinions on punishing cyber violence and crimes according to law. *China Applied Law, 43*(5), 53–62.

[9] Cai, Y. (2025). The logic of criminal governance of cyber violence and its path. *Research on the Rule of Law, 22*(5), 135–146.

[10] Luo, Y., & Cai, Y. (2023). Research on the current situation and prevention countermeasures of the crime of network insult and defamation. *Science of Law Journal, 2*(8), 45–58.