Journal of Politics and Law; Vol. 17, No. 3; 2024
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Criminalization Challenge and Analysis of Network Crime Assistance Behaviors

Hong Huang[1]

[1] The Institute of Portuguese-Speaking Countries, Macao Research Center for the Belt and Road Initiative, City University of Macau, Macau, China

Correspondence: Hong Huang, Studies of Portuguese-Speaking Countries, Institute of Portuguese-Speaking Countries, City University of Macau, Macau Special Administrative Region of China, 999078, China. E-mail: A23091100490@cityu.edu.mo

Received: March 11, 2024 Accepted: May 23, 2024 Online Published: May 29, 2024

doi:10.5539/jpl.v17n2p59 URL: https://doi.org/10.5539/jpl.v17n2p59

Abstract

The rapid development of the network society is in sync with the current era's pace. In comparison to traditional criminal methods, the utilization of the internet for criminal activities has progressively emerged and become increasingly prevalent. Nonetheless, this also poses a challenge in characterizing the offender's behavior. The objective of the study is to reveal the inadequacies in existing laws, policies and practices, and clarifying the harm of assisting in cybercrime and the plight of victims will help develop more effective support services and coping strategies, thereby improving the efficiency and quality of assistance to victims. This study focuses on the identification disputes that arise during the adjudication process of practical cases, combined with the existing legal provisions of the data for qualitative and quantitative analysis, and carries out a type study on the identification of helping behavior of cybercrime. Although China has specified the crime of assisting information network criminal activities in Article 287 bis of the Criminal Law, it remains controversial in distinguishing this offense from other crimes in actual cases. The study found that the techniques and means of cybercrime continue to evolve, from simple scams to sophisticated cyberattacks and data breaches, indicating that perpetrators are adapting to technological developments and changes in security measures. Consequently, it is crucial to clearly elucidate the connection between various recognition schemes from the theoretical perspective of norm violation and legal interest infringement, in order to provide an effective solution for the resolution of identification disputes in actual cases.

Keywords: network crime, criminal concurrence, behavioral aid, conviction and sentencing

1. Introduction

In today's society, cybercrime has gradually become systematic and complete, and based on the criminal motive, criminal means and criminal purpose, the characterization of network help behavior has also emerged. In this kind of crime, the criminal planning for the crime covers the provision of Internet access, server hosting, network storage, communication transmission and other technical support, as well as advertising promotion, payment settlement and other assistance behavior, which has attracted wide attention in the field of theory and practice. In the process of conviction of cybercrime, due to the differences in means and the interweaving of behavioral processes, the assisting behavior of cybercrime presents diversified characteristics and has a clear trend of classification analysis and research.

1.1 Research Background

The rapid development of information technology and the wide application of the Internet have become the main means and media of cybercrime, and cybercrime has gradually become a serious problem in the world. This not only harms the interests of individuals and organizations, but also poses a serious threat to national security, social stability and economic development. Cybercrime not only poses a threat to personal privacy and property security, but also has a serious impact on the entire social order. Its complexity and particularity make it a challenge to identify it accurately. In many cases, the methods of cybercrime are difficult to define and can easily lead to innocent people being implicated. The study of the controversy on the criminalization of cybercrime aiding behavior is helpful to clarify the legal definition of related behavior and ensure the fair and equitable handling of such cases in judicial practice. Therefore, the research on cyber crime has been paid more and more attention by

academia, government and society.

1.2 Research Purpose

Compared with the original traditional form of upstream crime, when the network help behavior becomes a specific crime, it may be the strictness of the law, or the variability of practice. The establishment of the crime of "assisting information network criminal activities" provides a legislative reference for other network assisting behaviors, but it also causes differences in the identification of actual operation. At present, the process of criminalization of network help behavior is advancing, but the specific classification of help behavior is still being improved. The criminal law research of cybercrime assisting behavior is based on the classification of charges of information cybercrime activities, guided by actual cybercrime cases, divided into three major topics: upstream crime, downstream crime and crime of assisting information cybercrime activities, and in-depth discussion of the form of Internet assisting behavior in the conviction process.

1.3 Research Significance

Helping behavior is an important part of cybercrime. Through in-depth study of helping behavior, we can understand the operation mechanism of cybercrime more comprehensively. This helps to reveal the root causes of cybercrime, so as to prevent and combat cybercrime more effectively. However, the help of cybercrime is often covert and transnational, making it more difficult to combat cybercrime. By studying help behavior, we can more accurately locate the source of crime, effectively combat all aspects of cybercrime, and improve the efficiency and success rate of combating cybercrime. In the process of committing a crime, the act of helping can provide resources for a wide range of potential criminals to commit a crime, and the harm caused by this wide range and the danger to legal interests are incalculable. By studying the help behavior, we can find and prevent the potential network crime in time, and reduce the occurrence and harm of network crime. Not only that, through the study of cybercrime helping behavior, it can provide strong support for improving relevant laws, regulations and supervision mechanisms, protect the legitimate rights and interests of individuals and organizations, and maintain national security and social stability.

2. Analysis of Upstream Crimes of Network Criminals

According to the Opinions of the Supreme People's Court on the Criminal Procedure of Cyber Crimes and related judicial interpretations, we can roughly summarize cyber crimes into three categories. The first is computer information system damage crime, which is also known as the common sense of hacker crime. This kind of crime mainly targets computer networks and carries out destructive activities, including the contents stipulated in Articles 285 and 286 of the Criminal Law: First, illegally intruding into computer information systems, illegally obtaining computer information system data and illegally controlling computer information systems; The second is to provide programs and tools for invading and illegally controlling computer information systems, as well as criminal acts such as damaging computer information systems. In the second part, the behavior of providing the programs and tools needed for crime, that is, the help behavior of cyber crime, it focuses more on the attachment to upstream crime, that is, the intrusion into the computer information system and the illegal acquisition of computer information system data crime in the front part.

The second is cybercrime, which is mainly carried out in cyberspace and the confirmation of criminal facts depends on electronic data transmitted and stored on the Internet. For example, Dissemination of obscene information through computer networks (dissemination of obscene electronic information on the Internet), online betting as a means of gambling (implementation of betting on the Internet), the spread of infringing data such as pirated software on the Internet (dissemination of infringing electronic information on the Internet), the establishment of illegal online game services on the Internet (operation of infringing services in cyberspace), and the online pyramid selling of virtual goods (pyramid selling) On the Internet), the online sale of citizens' personal information (citizens' personal information is transmitted through the Internet), etc.

The third is net-related crime, that is, the use of computer networks to organize connections but the main criminal acts are carried out offline crime cases. For example, the use of computer networks to connect the implementation of pyramid selling, robbery, theft, gun sales, sales of contraband and other criminal activities. In such cases, the crime cannot be committed directly on a computer network, which is merely a platform for communication. This kind of crime can be divided into two categories: one is through the establishment of websites, communication groups, mass release of information and other ways to organize or commit crimes against unspecified people. For example, through the establishment of fake e-commerce websites to implement shopping fraud, the establishment of pyramid marketing websites to organize pyramid marketing, a large number of sales of counterfeit money, fake invoices and other contraband information to implement the crime of selling contraband. The other type is the traditional crime that a certain person uses the Internet to organize and commit, or the crime that is committed

against a certain person, such as the crime that criminals commit murder, robbery and other criminal activities through the Internet. Unlike the previous type of crime, in this type of criminal activity, the perpetrator usually does not set up a website or communication group on the Internet.

After reading through the Supreme People's Court's classification of the upstream crimes of cyber crimes, the author has a preliminary understanding of criminal behavior and criminal means. Based on the perpetrator's use and motivation of the Internet. In the first type of network crime, the perpetrator's criminal behavior is inseparable from the network, which belongs to the parallel relationship between the crime and the network. Without the network environment, the first type of perpetrator will lose the continuation of the crime. The second type of cyber crime takes the network as the communication medium for the behavior. Due to the development of network modernization, the second type of criminal has formed a new crime mode, which belongs to the use of the boundary between the network and the real crime. However, the subject of the third type of cybercrime is more inclined to the traditional entity crime, and the use of network media only accelerates the criminal efficiency of the perpetrator. Even without the help of the network, the third type of crime can still be committed within the scope of traditional crime.

3. Conduct identification Disputes in Practical Cases

In the adjudication process of actual cases, the help behavior of cybercrime in the conviction and sentencing, the main crime mode is divided into three categories, one is the upstream crime accomplice punishment; The second is to help information network crime conviction punishment; The third category is based on the rest of the downstream aiding crime into the criminal judgment. The author briefly analyzes and discusses the actual judgment results and disputes of the three types of crimes, in order to understand the confusion and development of the existing conviction and sentencing system of cybercrime helping behavior.

3.1 The Focus of the Crime of Upstream Crime and Helping the Crime of Information Network Crime

After the implementation of the Criminal Law Amendment (IX), the charge of assisting the crime of information network crime has led to a series of debates on the source of network crime and the interweaving of accomplices in judicial cases. According to the provisions of Article 287 bis of the Criminal Law of the People's Republic of China, if a person knows that others use information networks to engage in criminal activities, but still provides them with Internet access, server hosting, network storage, communication transmission and other technical support, or advertising promotion, payment and settlement assistance, and the circumstances are egregious, he will be sentenced to three years in prison or criminal detention. And could be fined.

In 2019, a fraud ring conspired to commit Internet fraud. They planned the operation, and one of the actors paid for the purchase of A fake lottery website. For their benefit, A agreed to produce the website for them and provide the necessary technical support. With a website in hand, the scam gang began to implement their plan. Using the technology provided by A, they cleverly set up the prize pool, adjusted the odds, and used publicity stunts with a high probability of winning to attract victims to participate on the network. However, the law has a long way to go. With the confessions of the victims, the perpetrators were finally brought to justice. In the court's trial of this cyber crime case, for the members of the fraud gang, the first and second instance courts had no objection, unanimously found them guilty of fraud, and sentenced them accordingly. However, the opinions of the two courts were divided on the issue of A, which provided the lottery website. The lower court pointed out that although A knew that others used lottery websites to commit fraud, he still provided them with technical assistance and a criminal platform, which not only exposed his attempt at illegal possession, but also involved a coordinated crime. Therefore, A should be regarded as an accomplice to the crime of fraud and accept corresponding legal sanctions. However, in the second instance, the court's opinion on the conviction of A was different. They believe that A, knowing that others use the information network to commit crimes, still provide them with a false lottery website, and the circumstances are serious. According to this view, A's behavior should constitute the crime of assisting information network criminal activities.

3.2 The Dispute of Criminalization between Upstream Accomplices and Downstream Crimes

The controversy of the identification of network crime is not only limited to the crime of helping the letter, but also exists between the accomplice of upstream crime and the downstream crime of helping the crime. In a large number of practical cases, in many actual cases, the core dispute is mainly reflected in the upstream network crime complicity and downstream assistance crime involved in money laundering crimes. In these cases, the number of cases of complicity in upstream cyber crimes and crimes of concealing and concealing the proceeds of crime is significant. Let's take a case from 2018 to 2019 as an example. In the case, defendant A, for the purpose of seeking illegal benefits, although it was clear that Lin was implementing telecom fraud, it still provided wechat two-dimensional code for him to collect fraud proceeds. In addition to the above acts, defendant A also used wechat,

Alipay and other platforms to transfer the proceeds of fraud, involving a total amount of 2 million yuan, from which he sought profits of 200,000 yuan. It is worth noting that defendant C assisted defendant A in the transfer and storage of stolen money several times during this period, involving an amount of 180,000 yuan. Regarding defendant C's crime, the prosecution and the court are in full agreement that he is suspected of the crime of concealing and concealing the proceeds of crime. However, there is disagreement about the conduct of defendants A and B. The primary court decided that they were suspected of covering up the proceeds of the crime, but the procuratorate appealed, claiming that their behavior was in line with the characteristics of the crime of fraud, had sufficient legal basis, and should be regarded as the co-criminals of the crime of fraud. In fact, the core of the criminal dispute between the prosecutors and the law lies in the fact that the court maintains that defendants A and B, in the process of pursuing illegal proceeds, knew that the transferred funds were derived from fraud by others, but still covered up the behavior, which is in line with Article 312 of the Criminal Law on the constitutive elements of the offense of concealing and concealing the crime, and should be judged on the charge. However, the procuratorate pointed out that defendants A and B took the initiative to provide QR code payment services while knowing that the upstream cyber criminals were committing fraud. Such assistance is actually carried out before the fraud is carried out, rather than as a remedial measure afterwards. This indicates that the perpetrator has the intention to join the joint crime, and has carried out the relevant acts and shared the stolen money after the fact. Therefore, A and B should be punished as accomplices to the crime of fraud.

3.3 The Confluence of the Crime of Assisting Information Network Crime and Downstream Crime

Similar to the pre-determined disputes, in the actual judicial process, the dispute on criminal responsibility for assisting information network crimes focuses on the distinction between the charges of covering up, concealing the proceeds of crime and the proceeds of crime. In 2020, Liu, Wang and Yin followed the instructions of Tang and others in Fuzhou City, Jiangxi Province, and assisted Tang and others in transferring fraud proceeds by providing bank accounts, ID cards, mobile phones and on-site authentication in order to achieve illegal gains. Among them, Liu and Wang jointly participated in the transfer of up to 225,587 yuan; The transfer amount involved in Yin reached 214,527 yuan. The primary court decided that the three people were suspected of covering up and concealing the proceeds of crime, however, at the stage of appeal, the higher procuratorate countered that the three people clearly knew that others committed crimes in the information network environment, but still provided payment channels for settlement assistance, the situation is serious, and should be punished as the crime of assisting information network crime.

4. Analyze the Identification of Helping Behavior of Network Crime

In the context of cybercrime, the accomplice behavior of upstream crime often involves the help behavior of downstream. Downstream acts of assistance are regarded as collaborative acts of upstream crime because they provide crucial support for the upstream crime. In fact, the downstream criminal helper is the partner of the upstream criminal, whose core responsibility is to provide others with the necessary help to make it easier for the upstream criminal to achieve their criminal goals. Although they did not actually participate in the execution of the upstream crime, their help played a key role in the overall criminal activity. Therefore, these downstream criminal helpers should be regarded as accomplices of upstream crimes and investigated for criminal responsibility according to law. It is clear that downstream enablers, such as those who provide technical support or other assistance, are essentially helping upstream offenders to complete their crimes. These downstream assisting actors should be regarded as accomplices of upstream crimes and should be treated as accomplices of upstream crimes. In order to further deepen the understanding of this view, we can obtain an authoritative explanation from the judicial authorities. For example, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued the "Guidance on Several Issues concerning the Application of Law in Handling Online Gambling Crime Cases", which clearly states that anyone who knowingly provides services to gambling websites may be regarded as an accomplice in the crime of opening casinos. In detail, whether providing Internet access, server hosting, network storage space, communication transmission channels and other businesses, or advertising on the Internet, developing new members, or developing software or providing technical support, as long as the total service fee charged exceeds 20,000 yuan, it may be regarded as an accomplice to the crime of opening a casino. In addition, providing fund settlement services for gambling platforms, the income of more than 10,000 yuan, or assisting gambling websites to collect gambling funds of more than 200,000 yuan, will be regarded as a criminal act to participate in the establishment of casinos. For example, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued the Opinions on Several Issues Concerning the Application of Law to Criminal Cases such as Telecommunications and Internet Fraud. The opinions clearly put forward that any act of knowing that others are engaged in telecom network fraud criminal activities, but still providing them with Internet access, server hosting, network storage, communication

transmission and other technical support or payment and settlement assistance will be regarded as a joint crime. For downstream helpers to be considered as assisting the offender, their assistance must be closely related to the actual conduct of the principal offender. This criterion is based on the accessory principle of accomplice. In the cyber crime, the principal plays the core role, they are the key link to promote the criminal behavior to meet the legal requirements. Simply put, downstream helpers are identified as accomplices because their actions are closely linked to those of upstream cybercriminals. The existence of accomplice is based on the existence of intentional principal. Only after an upstream cybercriminal actually commits a crime, are those who assist the crime downstream punished. If there are no special provisions, the abettor and the aiding offender can be established only after the principal act has been committed. Therefore, it has certain advantages to identify the downstream helper in the network crime as an accomplice. However, there are inherent limitations to such strategies: First, if the downstream facilitator has provided corresponding support before the upstream cybercriminal actually committed the crime, such as the downstream facilitator provided network access or advertising services before the telecom network fraudster committed the fraud, then this method will not be effective in identifying such behavior. Secondly, if the upstream cybercrime has been completed, the downstream assistance behavior will be launched, such as transferring the stolen money to others and assisting in money laundering, and the crime of accomplice identity fraud can not be established. Therefore, there are still some shortcomings in this method to curb the coordinated operation of cybercrime.

Amendment (IX) to the Criminal Law has added provisions on the crime of assisting information network criminal activities, which makes the auxiliary behavior of combating various kinds of network crimes more accurate and efficient, so as to maintain the healthy development of information networks. However, in terms of the definition of this crime, there are three different theoretical opinions: the first opinion maintains that the crime is a sentencing guideline for assisting the crime, that is, the offender is not promoted to the main offender, and is still regarded as assisting the offender, but because the provisions of the sub-provisions provide for independent statutory penalties, so the punishment provisions on assisting the offender in the general provisions of the Criminal Law are no longer followed. Another view suggests that the offence is regarded as criminalization of assisting the commission, or assisting the act. That is to say, in the provisions of the criminal law, it is directly stipulated as a criminal act, and equipped with a separate statutory penalty. The other view is that the crime is independent, indicating that the crime of assisting cyber criminal activities has a unique position in terms of both actual objective and criminal law formulation. Therefore, we should abandon the recognition of its accessory role and regard it as an independent crime. There are three different views and arguments on the charge of aiding information network crime. The author makes the following observations: First, from a number of perspectives, these views together reveal the nature of the crime. Although this helps to identify assisting behavior in cybercrime to a certain extent, there are still certain drawbacks. With regard to the first view, the criminal is still considered an accessory offender because of the principle of treating assisting cybercrime as a penal act. The strength of this view is that it emphasizes the interdependence between downstream coordinated behavior and upstream cybercrime, arguing that the composition of the crime should be based on the actual actions of upstream cybercriminals. It emphasizes the inherent auxiliary nature of cybercrime assistance, and pays attention to the restraint effect of accomplice's accessory attribute on the scope of the establishment of accomplice. However, the weakness of this view is that downstream actors who assist upstream cybercriminals before they commit the actual act or after the principal result is known cannot be found guilty of the crime. For the second view, the advantage is that it also reveals a link between downstream assisted behavior and upstream cybercrime. Regrettably, however, in the absence of a determination of criminal assistance, downstream assisting actors cannot be convicted if they do not care what crimes are committed by others using the information network, but are concerned only with providing undifferentiated assistance services. For the third view, it is worthy of affirmation that it emphasizes the crucial position of downstream collaborative behavior in the black and grey industrial chain of cyber crime, and specifically points out the nature of such behavior's infringement on legal rights and interests in cyber crime.

For the assistance determination of downstream crime, the main purpose is to evaluate the relevant behavior by determining whether there is a crime with the nature of assistance. These charges are called assisting because key elements of upstream cybercrime have been incorporated into the constitutive elements of downstream crime. Although these charges can be used to make a reasonable assessment of assisting in cybercrime, their scope of application is limited. The constituent elements of downstream crime have formed constraints on the relevant scope of upstream cyber crime. For example, money laundering, which is often involved in downstream crimes in practical cases, as well as the act of concealing and concealing the proceeds of crime and its proceeds, can be regarded as the scope of implicated criminals in theory. In other words, in cybercrime, those who know the circumstances of the crime after the crime has been committed may help through various means. This is called "complicity". The existence of such complicit crimes must be based on the premise that others have already

committed the relevant criminal acts. When someone provides payment settlement support in a cybercrime, those funds are usually the proceeds of the crime and the proceeds it generates. This raises the complex issue of how to trace and verify the sources of these funds. However, according to the actual situation, such payment settlement assistance does not only target funds obtained from crimes, but also includes funds used by criminals. In online fundraising fraud cases, criminals may invest their own funds in advance in order to gain the trust of the victim and successfully obtain funds. Although these funds are owned by criminals and used for criminal acts, they are not the same as the proceeds of crime involved in the crime of money laundering and the proceeds generated. Therefore, it cannot be determined only by the money laundering charges involved in downstream crimes.

5. This Paper Probes into the Problem of Existing Identification Relationship from Two Perspectives

In the examination of cyber crime, from the Angle of damage of legal interests, there is a certain degree of correlation between assisting behavior and carrying out behavior. In the actual operation process, the confirmation of assisting behavior of cybercrime usually depends on the substantive assessment of legal interest infringement. The determination of the accomplice of upstream cybercrime is based on the dependence assessment of downstream auxiliary behavior based on the charges involved. In response to this requirement, upstream cybercriminals and downstream assistance behavior need to be interrelated, and at the same time, downstream assistance behavior should have an effect on the legal rights and interests violated by upstream cybercrimes. Choosing independent evaluation of downstream helping behavior is to evaluate its behavior according to the charges involved in downstream helping crime. This evaluation method weakens the function of meaning connection, and the core of evaluation is to judge whether the downstream helping behavior infringes on the legal interests protected by the downstream helping crime. On the other hand, if we choose to help the crime of information network crime, we will go beyond the scope of assisting accomplices. This identification method requires a separate assessment of downstream assistance, while focusing on upstream cybercrime enforcement. The existence of the meaning of the connection is not the key to the identification, because the charge has the characteristics of double legal interests, so it is easy to compete with the identification of the accomplice of the upstream network crime. In this case, according to the principle of imaginary concurrence, choose the crime with heavier punishment to deal with. In addition, we should also comprehensively examine many relevant factors, such as the definition of laws and regulations, the subjective intention of the actor, the nature and severity of the behavior. Together, these factors determine whether aiding constitutes an accomplice to cybercrime or an independent crime.

In addition, the identification of cybercrime assistance behavior usually requires in-depth analysis from the perspective of violating laws and regulations. As a new form of crime, cybercrime is different from traditional crime in identifying its helping behavior. Therefore, the existence of meaning connection is not the key to judgment. It is important to take a comprehensive look at the behavior itself and the extent of the violation of laws and regulations. From an in-depth perspective, the help behavior of cybercrime can be divided into two categories: first, the downstream criminal communicates and cooperates with the upstream criminal before or during the implementation of the cybercrime, providing technical assistance or other support. If the circumstances are serious, it can be regarded as a coordinated crime; The second is the criminals downstream of the network, aiming at illegal profit and providing indiscriminate assistance in the online world. As long as they are aware of upstream criminals using information networks to engage in illegal activities, and provide them with technical assistance or other support, and the crime is serious, they can also be considered accomplices. In the second case, downstream criminals do not actually need to know what crimes are committed by upstream criminals, and the meaning of their connections is not the key factor. In the traditional theory of accomplice, the connection between the aided offender and the aided offender is usually strong, but this rule seems to be no longer applicable in the cyber crime. When evaluating the identification of help behavior of cybercrime, from the perspective of violation of regulations, it is necessary to comprehensively consider the definition of laws and regulations, the existence of causality, the subjective mentality of the perpetrator and other factors. However, in cyberspace, there are many helpful behaviors whose meaningful connections gradually weaken or even disappear, and such behaviors are increasingly becoming a key link in the realization of cybercrimes.

6. Conclusion

This paper makes a preliminary understanding of the current phenomenon of cyber crime, and the purpose of the research is to analyze the harm and scale of the helping behavior in the process of cyber crime. After analyzing the existing laws and actual cases, the author argues that broad and precise criminal liability standards should be established to ensure comprehensive coverage and clear targets for cybercrime assists.

Through the research of existing literature and the further analysis of practice, the author finds that the rapid

progress of information technology has led to the gradual renovation of the means of assisting cyber crimes. The traditional means of crime can achieve the crime phenomenon of "visible but invisible" through the information network. With the support of scientific and technological means, the efficiency and concealability of crime have been further improved. This undoubtedly poses a severe test for legislation and enforcement. However, the output of this paper is that in the future research process, we should pay attention to the identification and prevention of new cybercrime helping behavior, as well as the improvement of relevant laws and regulations. For crimes of different degrees, we should also use specific charges to regulate. The criminalization of network crime helping behavior is also the penalty trend of network crime helping behavior. In addition, issues such as the age of criminal responsibility and the determination of criminal intent for cybercrime assistance also need to be further explored. Moreover, strengthening international cooperation is the key to combating cybercrime. Countries should establish effective cross-sectoral and cross-regional cooperation mechanisms, enhance intelligence sharing, technology exchange and law enforcement cooperation, and jointly address the threat of cyber crimes. At the same time, increase the punishment of cybercrime assistance, destroy the criminal industry chain, cut off the source of criminal proceeds, and fundamentally curb the occurrence of cybercrime. However, to prevent the occurrence of cybercrime help behavior, we still need to start from the source. We will strengthen cyber security education, raise the general public's awareness of the rule of law and prevention capabilities, and form a cyber crime prevention and control system with the participation of all people.

However, in the research process, due to the singularity of disciplines and the diversity of research topics, the author has failed to conduct a deeper discussion on cyber crime at the level of network technology in terms of the principle of criminal means and the behavior mode of information crime, which is also the current research direction of conviction and sentencing of cyber crime in combination with disciplines.

The interdisciplinary cooperation and communication should be strengthened in the future study of helping behavior of cybercrime. For example, experts in law, computer science, psychology, sociology and other fields participated in the research, in order to deeply explore the causes, characteristics and prevention strategies of cybercrime help behavior from different angles. In addition, it is necessary to strengthen the empirical research on cybercrime helping behavior, and reveal the development trend and law of cybercrime helping behavior by collecting and analyzing a large number of case data. This helps to provide more targeted guidance for legislation and enforcement. Most importantly, always pay attention to the application of emerging technologies in the field of cybersecurity, such as artificial intelligence, big data, blockchain, etc. Technology has great potential in preventing and combating cybercrime, and future research should actively explore ways to apply these technologies to cybercrime prevention and governance.

References

Chen, X. B., & Huang, H. (2023). Judicial determination of meaning contact in network joint crimes. *Journal of Beijing University of Posts and Telecommunications,* (3), 66-67.

Chen, X. B., & Wang, X. C. (2023). The dilemma of complicity attribution and theoretical reconstruction in network technology service crime participation. *Journal of Chongqing University,* (1), 67-79.

Chen, X. L. (2022). The criminalization of complicity in aiding information network criminal activities: Perspectives on the crime of aiding information network criminal activities. *Comparative Law Research,* (2).

Liu, R. W., & Wang, G. Z. (2023). Criminal determination of aiding behavior in network crimes. *Rule of Law Research,* (2), 130-131.

Pi, Y., & Du, J. W. (2021). Theoretical exploration and legislative study on the criminalization of aiding behavior. *Qilu Journal,* (1).

Ren, Y. J., & Nie, R. (2023). Understanding and application of the crime of aiding information network criminal activities. *Journal of Wuhan Police Cadet Academy,* (4), 37-38.

Wang, R. Y. (2022). The boundary of criminalization of network crime aiding behavior: Perspectives on narrowing the application of Article 287(2) of the Criminal Law. *Heilongjiang Human Resources and Social Security,* (14), 100-103.

Zhang, M. K. (2016). On the crime of aiding information network criminal activities. *Politics and Law,* (2).

Zhao, G. R. (2023). The construction of legal doctrine of aiding behavior in network crimes from the perspective of complicity. *Rule of Law Review,* (7), 97-99.

Acknowledgments

I am very grateful to Weiyuanhu Academy for its support of my research, to the relevant academic staff for their contributions, and to the professors of Renmin University of China for their theoretical help.

Authors contributions

Master Huang Hong is fully responsible for the research and data collection of this paper, as well as the revision of the article.

Funding

Not applicable.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.