Qualitative Analysis of Criminal Characterization on Assisting in Crimes and Gaining Profits Therefrom

Jiahui Ding *

College of Foreign Languages, North China University of Science and Technology, Tangshan,063210, China

* Corresponding Author Email: BaiQuan985@outlook.com

Abstract. To effectively regulate, accurately penalize and systematically prevent assist cybercrimes, Article 287-2 of the Criminal Law of the People's Republic of China, which defines the offense of aiding cybercriminal activities, has been specifically established in China's Criminal Code. This paper aims to conduct a systematic comparative analysis and jurisprudential discussion on the offense of aiding cybercriminal activities in China's legal system, and the equivalent aiding cybercrime offenses established in major extraterritorial jurisdictions, including the United States, Germany and Japan. This study combines a series of typical specific cases in China's judicial practice in recent years, and carries out in-depth classification and empirical research on this category of crime with "provision of technical support, payment and settlement assistance" and "acquisition of illegal proceeds" as its core characteristics. Through the aforementioned multi-dimensional comparative analysis and case dissection, this study attempts to draw conclusions with both theoretical and practical value on the delimitation of boundaries between the offense of aiding cybercriminal activities and other equivalent aiding offenses involving illegal proceeds, in terms of constitutive elements, incrimination standards and judicial identification. Ultimately, the "aiding act + illicit gain" offenses are classified into three categories: "instrumental" aiding, cooperative aiding and post-offense aiding, and the proposed perspective is substantiated with specific case examples.

Keywords: Offense of aiding information network criminal activities, accomplices in cybercrime, helping behavior.

1. Introduction

The 55th Statistical Report on the Development of China's Internet released in January 2025 shows that 2024 marked the 30th anniversary of China's full access to the Internet. The number of Internet users in China reached 1.108 billion, with an Internet penetration rate of 78.6%, and the added value of core industries of the digital economy accounted for 10.5% of the GDP [1]. While the rapid development of the Internet has driven social transformation, it has also given rise to a large number of cybercrimes, with telecommunications and online fraud being particularly prominent. In 2025, courts across the country concluded 41,000 cases related to such crimes, involving 85,000 people, an increase of 1.2% year-on-year [2]. Against this backdrop, the number of cases of the crime of helping information network criminal activities has risen sharply and has become one of the most prosecuted crimes in recent years, especially after the "card-cutting" campaign, it has continued to grow at a high speed, attracting significant attention from both the academic and practical communities.

Against the backdrop of the central government’s intensified efforts to combat telecommunications fraud—and amid rapid advancements in big data and artificial intelligence technologies—the offense of “assisting information network criminal activities” is increasingly emerging as a paradigmatic catch-all charge under China’s Criminal Law. The subjective awareness of knowing in the crime of aiding information network criminal activities is ambiguous, the definition of objective assisting behavior is unclear, and the threshold for conviction is relatively low. These factors make the crime of aiding information network criminal activities inherently prone to being overly broad. Therefore, it is necessary to conduct a substantive restrictive interpretation of this crime before applying it [3]. Otherwise, it may lead to some judicial misjudgments.

This study will focus on the ambiguous boundary between the crime of helping information network criminals and the co-conspirators of upstream crimes and conduct research and analysis. The

aim is to further enrich the theoretical framework of the criminal composition of the crime of helping information network criminals and provide clear and feasible theoretical basis and reference solutions for judicial practice.

2. Research Status on the Offense of Providing Assistance for Profit

2.1. Current Situation of Research in China

In Chinese academic circles, there are three primary perspectives on the characterization of the offense of assisting information network criminal activities: The first is the theory of independent offense, which holds that this crime is the principalization of neutral aiding acts, constitutes an independent offense, and can be handled in accordance with the principle of concurrence of offenses [4]. Second is the accomplice exception theory, which regards it as a special accessory offender and stipulates that it shall apply only when the accomplice cannot be established; third is the substantive limitation theory, which advocates that the identification shall be narrowed based on a comprehensive consideration of both subjective and objective factors [5].

Most existing studies have been conducted from the perspectives of "knowledge with certainty", "serious circumstances" and constitutive elements. The limitation of current research lies in the insufficient typification of the typical "assistance for profit" model, and the failure to establish a unified distinguishing rule by incorporating charging methods, participation levels and behavior stages.

2.2. Current Status of International Research

Against the background of the globalization of cybercrime, the regulation of cyber aiding behaviors varies significantly across jurisdictions. As an independent offense formulated to address China’s domestic criminal ecology, China’s offense of aiding information network criminal activities has no direct counterpart in foreign legislation. Nevertheless, the academic debates on "neutral aiding acts" in extraterritorial research provide theoretical references for the improvement of domestic legislation [6].

Germany has been chosen as the typical representative of civil law countries, while Japan is included as a supplementary representative of Asian civil law countries. In the modern legal system of Germany, there is no such term as "aiding information crime", but Germany regulates similar behaviors through a three-level system of complicity theory + special chapter on computer crime + administrative supervision, adhering to the principle of "no principal offender, no accomplice". The core logic is "no principal offender, no accessory". If someone only provides neutral technical services and cannot prove that they have criminal intent for the upstream crime, they usually only face administrative penalties. Therefore, in the German legal system, those who knowingly provide assistance and profit from it are punished as accomplices to fraud or computer crime. The eclectic theory represented by Professor Claus Roxin in Germany holds that when imposing restrictive penalties on neutral assistance behaviors, both the objective and subjective aspects should be considered simultaneously. Professor Roxin proposed the "intention dichotomy", dividing the subjective intent of neutral assistance offenders into "definite intent" and "accidental intent" [7].

In Japanese criminal law theory, the Japanese Criminal Code stipulates "joint principal offender", "abettor", "accessory", mitigation of accessory, restrictions on the punishment of abetting and assisting, and complicity in status crimes in Chapter 11 "Complicity" of the first part "General Provisions", and also provides for each article in the second part "Crimes".Accordingly, all constituent elements of a crime stipulated in each provision correspond to "perpetrators", which means that the restrictive concept of perpetrator is adopted [8]. For the aforementioned reasons, although the Japanese legal system also does not contain the offense of "aiding information network crime", a large number of offenses related to aiding acts are classified as perpetrator offenses.

There are significant differences in the regulatory approaches between common law systems of the United Kingdom and the United States. The United Kingdom adopts a pluralistic evaluation

framework based on the Computer Misuse Act 1990, as well as offences including fraud, money laundering and conspiracy, and makes a conviction selection based on the infringement of legal interests, subjective viciousness and the degree of harm, with emphasis placed on the hierarchy of subjective intent and behavioral danger [9].

Compared with the other countries mentioned above,American law distinguishes between first-degree principal offenders, second-degree principal offenders and accessories before the fact.It went without saying that principals in the first degree included those who use another person to commit the offence. Accessories before the fact came in two vari-eties—solicitors and facilitators [10].This means that the conviction of the helper is usually based on the upstream crime. Once convicted, they are typically treated as an accomplice to the upstream serious crime and face even more severe criminal penalties.

Overall, the civil law system focuses on the principle of complicity and the restriction on neutral assisting acts, while the common law system emphasizes the imposition of liability for multiple offenses and accomplice liability for felony offenses. Both systems provide important references for China to reasonably define the crime of assisting information network criminal activities and prevent it from becoming an all-encompassing offense.

3. Typological Analysis and Case Study of the "Assistance-Profit" Behavior

According to research and analysis, scholars have classified the behavior of providing online assistance and profiting from it into three typical patterns.

3.1. Tool-Based Support: Dual-Card Provision with a Fixed Pricing Model.

The first category is "tool-oriented" assistance, which provides the "two certificates" or technical interfaces and charges a fixed fee.This type of offense is relatively less harmful, and its judgment is fairly straightforward; it is a typical peripheral crime.This behavioral pattern is characterized by a hierarchical outward radiation centered on network service providers, which provides assistance for multiple criminal acts and presents a "one-to-many" or "many-to-many" behavioral pattern [11]. For instance, in the case of Li selling his bank card, Li merely provided his own bank card and received a fixed monthly rent of 3,000 yuan. He did not participate in the planning of the fraud, did not share in the spoils, and did not handle the flow of funds. Subjectively, he only had a general awareness, and objectively, he only provided peripheral tool support, without exerting control or a key driving force on the fraud. This behavior meets the constitutive elements of the crime of assisting information network criminal activities and should be recognized as such, rather than as an accomplice to fraud. However, if the case involves the perpetrator's continued participation in the criminal process or if there is a situation of "premeditated collusion" before the criminal act occurs, the nature of the behavior may escalate, constituting a more serious crime of fraud.

3.2. Cooperative Assistance: Deep Involvement and Proportional Sharing

The second type is the "cooperative" assistance where one deeply participates in the criminal process and shares the illegal gains in proportion.The "deep involvement" herein is a crucial boundary distinguishing the crime of aiding and abetting information network criminal activities from the upstream fraud offense or other crimes. Such depth is not only reflected in the explicit cognition of the criminal purpose, but more importantly embodied in the whole-process nature of the perpetrator's conduct and its functional indispensability.For instance, defendant Zhao, fully aware that others were carrying out telecommunications fraud, voluntarily provided his bank card to the criminal gang in order to obtain a 5% commission for each successful transaction. This was not merely a simple act of providing a tool, but the beginning of a deep collaboration. During the subsequent fraud operations, when the fraudsters lured the victims into transferring money to Zhao's bank account through deceptive phone calls, Zhao was present throughout the process and actively followed up. As soon as the funds arrived, he immediately complied with the request to perform facial recognition verification

or enter the dynamic password received on his mobile phone to ensure that the fraud proceeds could be promptly and smoothly transferred to the next-level accounts controlled by the criminal gang. It is evident that what Zhao provided was not a static, "dead" payment tool, but rather, by leveraging his real-time control over his personal bank account, he offered dynamic, proactive, and synchronized assistance at the core stage of the fraud chain - the transfer and transformation of funds.Each of his identity verification operations directly facilitated the completion and consummation of the fraud crime. This kind of "real-time cooperative operation" has been deeply integrated with the act of committing fraud, essentially becoming an inseparable continuation of the fraud behavior, making him no longer an external helper. Therefore, the nature of his actions has transcended the scope of the crime of aiding information network crimes, and thus should be recognized as an accomplice to the crime of fraud.

3.3. Post-Event Assistance:Transfer of Funds after the Completion of a Crime

Thirdly, it refers to the "ex post-facto" assistance involving intervention in capital transfer after the completion of the antecedent offense. Such conduct occurs after the perpetration of the crime is completed and the harmful consequences have already emerged, and is mainly manifested in the transfer, concealment and conversion of criminal proceeds and their gains, which satisfies the constitutive elements of the crime of covering up and concealing criminal proceeds and the proceeds from criminal proceeds as stipulated in Article 312 of the Criminal Law.For example, in the case of Yu, despite knowing that the funds involved were proceeds from fraud, Yu still provided his bank card and relevant information to assist in transferring the funds for illicit profits. However, Yu's involvement occurred after the fraud was completed and the victim had already suffered losses, which constitutes post-offense assistance and should be convicted as the crime of covering up and concealing criminal proceeds.

In summary, even for the same conduct of "providing assistance for profit", significant differences exist in conviction determination based on the degree of participation and the stage of the conduct: where the actor only provides tools without deep participation, the offense of aiding information network criminal activities may be established; where the actor participates deeply and is highly integrated with the perpetrating act, the actor constitutes a co-offender of the crime of fraud; where the actor intervenes to transfer funds after the offense is completed, the actor shall be convicted and punished for the crime of covering up or concealing criminal proceeds.The three types of punishment vary in severity, and judicial identification must accurately distinguish them based on the depth of participation, the timing of intervention, subjective cognition and the role of conduct, so as to avoid improper expansion of the crime of aiding information network criminal activities.

3.4. Differentiation Rules between the Crime of Aiding Information Network Criminal Activities and Other Offenses

Subjective-level differentiation rules. If the perpetrator only has general knowledge and is unaware of the specific type of the upstream crime and does not participate in the conspiracy, they are generally convicted of the crime of helping information network crimes; if the perpetrator has definite knowledge, has a connection of intent with the upstream party and conspires in advance, they are convicted as an accomplice of the upstream crime; if the perpetrator only becomes aware after the fact that the proceeds are from a crime and transfers them, they are convicted of the crime of concealing or disguising criminal proceeds.

Objective criteria for differentiation. If the perpetrator merely provides peripheral assistance such as tools or accounts without getting involved in the core process, they should be convicted of the crime of aiding information network criminal activities. If the perpetrator participates in the division of labor, cooperation, and operation, and plays a crucial role in the completion of the crime, they should be convicted as an accomplice. If the perpetrator gets involved after the upstream crime has been completed, they should be convicted of the crime of concealing or disguising criminal proceeds.

The rules for distinguishing the profit-making aspect. If the actor receives a fixed rent or fixed remuneration, which is unrelated to the proceeds of the crime, it is generally recognized as the crime of aiding and abetting information network crimes; if the actor shares the proceeds in proportion to the amount of the crime and is directly linked to the illegal gains, it is generally recognized as an accomplice; if the profit is obtained after the completion of the upstream crime, it is generally recognized as the crime of concealing or disguising the proceeds of crime.

4. Conclusion

This article takes the offense of aiding information network criminal activities as the research basis, and conducts an analysis centering on the divergences in criminal law evaluation regarding the behavioral mode of "providing assistance for profit".Through analysis of actual cases, this paper concludes that conduct that only provides payment and settlement instruments or technical interfaces, charges fixed consideration, and does not intervene in the core link of the antecedent offense should in principle be convicted and punished as the crime of aiding information network criminal activities. Where the perpetrator not only provides assistance, but also is deeply embedded in the criminal process through real-time coordinated operation, profit sharing in proportion to illegal income and other means, such conduct has formed functional integration with the perpetrating act. In this case, it is inappropriate to adjudge it as the crime of aiding information network criminal activities; instead, the adjudication shall follow the principle of accomplice attribution, and the conduct shall be identified as an accomplice of the antecedent offense such as fraud. As for conduct that intervenes after the completion of the antecedent offense and assists in transferring funds to conceal the whereabouts of illicit money, the legal interest infringed by such conduct has shifted to the order of judicial prosecution, which is more consistent with the normative protection purpose of the crime of concealing or covering up the proceeds of crime.

References

[1] The 55th Statistical Report on the Development of China's Internet was released. Media Forum, 2025, 8(2): F0003.

[2] Zhang Jun. Work Report of the Supreme People's Court. People's Court Daily, 2026-03-10: 004.

[3] Liu Yanhong. The Judicial Expansion Trend and Substantive Restriction of the Crime of Assisting Information Network Criminal Activities. China Legal Review, 2023, (03): 58-72.

[4] Dong Xu, Xie Xinnan. Criminal Characterization of Payment and Settlement Assistance Behaviors: An Empirical Analysis Based on 237 Cases. Law Review of University of International Business and Economics, 2024, 8(01): 303-314.

[5] Mao Bin. The Predicament and Reflection on the Recognition of Knowledge in the Crime of Assisting Information Network Criminal Activities. Evidence Science, 2022, 30(06): 730-742.

[6] Chen Ying. Research on the Judicial Determination of the Crime of Assisting Information Network Criminal Activities. Sichuan Provincial Party School of the Communist Party of China, 2025.

[7] Roxin. Strafrecht Allgemeiner Teil, Band II. München: C. H. Beck, 2003: 26. 241.

[8] Nage Madoka. The Basic Theory of Japanese Negligence Offender and Accomplice. Chuo University, 2016.

[9] Ye Liangfang, Ma Luyao. The Development of Criminal Legislation on Cybercrime in the UK and Its Implications. Social Sciences Abroad, 2020, (05): 40-51.

[10] Dubber M. D. Criminalizing complicity: a comparative analysis. Journal of International Criminal Justice, 2007, 5(4): 977-1001.

[11] Shi Xiongwen. Typological Analysis and Judicial Application of the Crime of Assisting Information Network Criminal Activities: Based on "Technical Support Type" and "Commercial Assistance Type" Behaviors. Journal of Huaqiao University (Philosophy and Social Sciences Edition), 2025, (01): 103-115, 127.