Proceeding of ICSPHS 2026 Symposium:Ethics, Law, and Psychology: Interdisciplinary Reconstruction of Humanities in Medicine
DOI: 10.54254/2753-7048/2026.ZJU31409

The Chinese Approach to Combating Cybercrime: Achievements, Challenges, and Measures

Yuerong Li

Law School, Central South University, Changsha, China
8106220512@csu.edu.cn

Abstract. The popularization of the Internet and the development of technology have given rise to industrialized cybercrime, especially the rise of a large number of assistance behaviors. To prevent cybercrime from causing actual harm as soon as possible, it is necessary to promptly crack down on such assistance behaviors. This article takes the "Crimes of Helping Information Network Criminal Activities" (CHINCA) as the core object. Through the integration and analysis of existing literature and empirical research, it reveals the increasingly prominent "pocket crime" tendency in judicial practice due to the generalization of the "knowing" determination, the ambiguity of the behavioral boundary, and the mechanization of the circumstances standard. On this basis, the study further proposes systematic correction paths from the dimensions of theoretical reconstruction and judicial restraint, such as clarifying the normative attribute of this crime as a "substantive preparatory crime" and implementing the concept of "incrimination in form, but acquittal in essence". This paper not only responds to the practical difficulties in China but also provides references for countries to balance crime governance and rights protection in the digital age.

Keywords: Crimes of helping information network criminal activities, "pocket crime", criminalization of assistance behavior, knowing, serious circumstances

1. Introduction

Cybercrime often exhibits distinct transnational characteristics and causes far-reaching harm. For instance, the criminal platform case of "16Shop" cracked by Interpol in 2023 affected 43 countries and victimized over 70,000 people, vividly demonstrating the scale and destructive power of its cross-border spread [1]. With the surging of cybercrime, the provision of technical support, payment settlement, advertising promotion, and other assistance has also become increasingly large-scale and chain-like, forming a “chain of gray industry”, further complicating governance. Against this background, merely relying on traditional “accomplice theory” to punish the perpetrators is no longer sufficient for effective governance. To address this challenge, the international community, on the basis of updating domestic legislation in various countries, has actively promoted collaborative governance. For example, the signing of the Convention on Cybercrime (Budapest Convention) and the adoption of the United Nations Convention against Cybercrime in 2024 both reflect the strengthening of global consensus.

DOI: 10.54254/2753-7048/2026.ZJU31409

In China, due to the large scale and complexity of types of cybercrimes, the previous "punishing as accomplices" model has encountered practical choke points, such as difficulty in proving the case and a narrow scope of crackdown. Therefore, in 2015, China passed the "Amendment to the Criminal Law (IX)" to establish the CHINCA, which independently criminalizes the assisting behavior, with the intention of building a "full chain" governance system. However, this legislative tool has gradually shown its duality in judicial practice. On the one hand, its deterrent effect has been confirmed by case data; on the other hand, the continuous expansion of its application scope has also raised widespread concerns among the academic community about "pocketization". Specifically, the subjective aspect shows a tendency of "knowing" being undervalued and generalized, and relevant studies indicate that there are problems of "knowing" requirements being undervalued and content being ambiguous in practice, further leading to the risk of "presumption expansion" [2,3]. Objectively, some scholars point out that the "serious circumstances" standard is prone to being mechanically applied, and the boundary of the assisting behavior in practice has become increasingly blurred [4,5]. This article will first elaborate on the problems that the aiding in crime aims to solve and the current situation of its solution, then deeply analyze the causes of its application alienation, and finally systematically explore feasible solutions, to provide profound insights from China's practice for global cybercrime governance.

2. The current situation and the effectiveness of governance in combating CHINCA

2.1. The failure of regulation by the traditional accomplice theory

The current cyber joint crimes exhibit a completely different structural pattern from traditional crimes. Their organizational structure tends to be "loosely structured", characterized by a "low degree of organization and loose division of labor system"; the core entities show a "hidden" trend, with "the concealment of the principal offender's identity, cross-border hiding or the breakdown of the evidence chain" becoming a structural norm; the "intentional coordination among the participating entities" is scarce, and the behavioral connections are fragmented; the illegal content of individual acts is significantly minor, and the independent criminal liability is significantly insufficient [6].

This kind of structural alienation has placed the traditional accomplice theory in a double predicament. On the one hand, the problem of "absence of the principal offender" is prominent: due to the difficulty in identifying the principal offender or the insufficient criminality of their actions, the "principal offender" is essentially lacking in criminal evaluation or is not punishable. On the other hand, the phenomenon of "failure of the aider's liability attribution" is widespread: although online assistance behavior plays a crucial role in the criminal process, according to the subordinate nature theory of accomplices, due to the lack of an attachable principal offender's behavior, it is difficult to attribute liability. This leads to a structural loophole in criminal regulation [7].

2.2. Legislative oversight leads to the difficulties of accountability

In high-incidence and highly costly cybercrime activities, cybercrime helping behavior plays an indispensable and crucial role. These acts serve as the fundamental support for the operation of the criminal chain, transforming mere criminal intentions into executable criminal behaviors. Given the foundational position of helping behavior within the entire criminal ecosystem, establishing an effective legal regulatory system for them becomes particularly urgent. From a comparative law perspective, the legislation of major legal systems has limitations in regulation. In the Anglo-

DOI: 10.54254/2753-7048/2026.ZJU31409

American legal system, for instance, the "Password trafficking with intent to defraud" stipulated in Section 1030(a)(6) of the United States' Federal Code, although treating helping behaviors as an independent crime, only regulates specific behaviors such as "providing passwords", and is unable to cover diverse forms of cybercrime assistance behaviors. In the civil law system, Germany adopts the protective approach of "Criminalization of preparation act" through Article 202c of the Criminal Code, reflecting the idea of prioritizing the protection of legal interests, but does not adopt the legislative technique of criminalizing helping acts. All this reveals that current legislative systems have not yet expanded the scope of helping objects to "pan-network crimes", and the regulatory scope is clearly limited.

2.3. The paradigm shifts in China's legislation

To address the governance challenges of assisting in cybercrime activities, the country has established CHINCA to achieve a transformation in the legislative paradigm. Firstly, it has filled the penalty loopholes for new criminal forms such as "chain assistance" and "weakening of intent connection", and made up for the insufficient adaptation of the traditional accomplice theory to the cyber space; Secondly, it has promoted the formation of a "full-chain" crackdown model, which has achieved a transformation from single-point crackdown to system governance, providing key institutional support for legal governance in the cyber space [8,9].

However, the rapid expansion of the application of this crime has raised concerns about the "pocketization" problem. "Pocketization" refers to the situation where, due to ambiguous provisions and save clauses in the law, the scope of application of the crime has been continuously expanded, including behaviors that were not explicitly targeted by the legislation in the punishment. Additionally, the particularity and controversy of this crime have led to an explosive increase in the number of cases, which has triggered concerns about the excessive expansion of the boundaries of the crime. Both the academic community and the practical field are focusing on how to effectively combat crimes while avoiding the situation where it becomes a "pocket crime" in the digital age.

3. The cause of "pocketization" of CHINCA

From the judicial practice in recent years, the crime of "aiding in information crimes" shows a tendency of "pocketization". In the cybercrime cases from 2020 to 2025 (as shown in Figure 1), this crime accounted for over 90% and became the "main crime name" for punishing the assisting behaviors in online crimes. This indicates that CHINCA has a significant effect in cutting off the criminal chain and curbing upstream crimes. However, at the same time, it also directly reflects the actual trend of its significant expansion in application, and "pocketization" has become the most prominent practical feature of this crime in judicial activities.

DOI: 10.54254/2753-7048/2026.ZJU31409

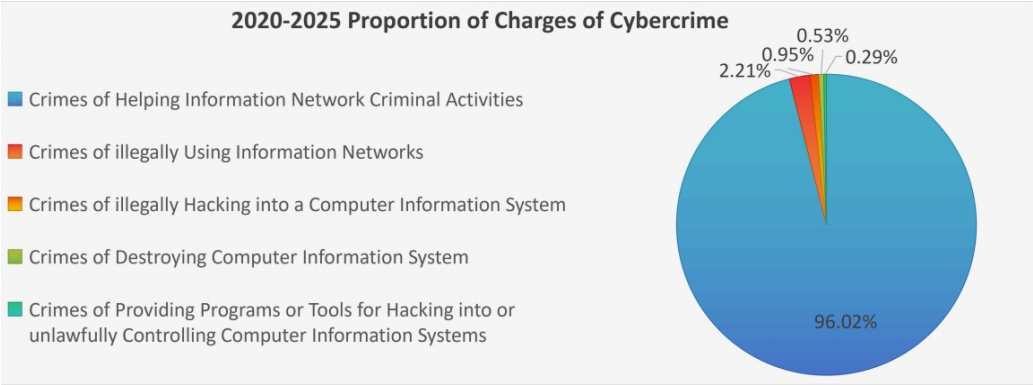

Figure 1. The proportion of charges in cybercrime in China from 2020 to 2025

Data Source: China Judicial Big Data Research Institute.

The causes of the "pocketization" of CHINCA are as follows.

3.1. The ambiguity of the constitutive elements

The generalization of the "knowing" determination criteria. The empirical data from the China Judgments Online show that in the judgments of CHINCA, the proportion of cases applying the "possibly knowing" standard reached 54.2%, which exceeded the proportion of 45.1% for the "definitely knowing" criterion [10]. This data fully demonstrates that the determination standard of "clear knowledge" in the legislative intention has gradually expanded in judicial practice to "should know" and "possibly knowing", resulting in an inappropriate expansion of the subjective liability scope.

The expansion of the "any other assistance" clause and the blurring of boundaries. The judgment document shows that due to the open nature of the legal provisions regarding "any other assistance", judicial decisions often interpret this vague expression as "any other technical support and assistance" or even simplify it to "providing assistance". This simplification of the objective behavioral elements reflects the arbitrariness in the determination of behaviors in judicial practice, seriously challenging the clarity of acts required by the principle of Nulla poena sine lege. The ambiguity of the behavioral elements further leads to the dissolution of three boundaries in judicial practice: neither can the specific types and characteristics of various assistance behaviors be strictly distinguished, nor can the boundaries between this crime and related crimes as accomplices or principal offenders be clarified, nor can the punishable and neutral assistance behaviors be accurately divided. This multiple ambiguity of boundaries further leads to the improper expansion of the application of the CHINCA, resulting in some neutral assistance behaviors being included in criminal evaluation [11].

3.2. The dual expansion of the criteria for criminalization

The criteria for criminalization of CHINCA show a dual expansion feature. This expansion is mainly manifested in the combined application of a mechanized amount standard and an open-ended save clause - the current judicial interpretation adopts the "listing plus 'other serious circumstances'" blanket provision for the determination of "serious circumstances", and this legislative technique, although aiming at formulating a comprehensive application scope, actually has structural flaws [12]. Specifically, it is manifested in the following two aspects:

DOI: 10.54254/2753-7048/2026.ZJU31409

Firstly, the clearly specified quantitative standards (such as "more than three" objects, "two hundred thousand yuan" and other amounts) possess a distinct mechanical nature. They fail to take the subjective and objective reasons of the actors, as well as personal circumstances and other comprehensive factors, into account, thus falling into the trap of the "amount-oriented" approach.

Secondly, the deeper issue lies in the dualization of the criminalization criteria. As the crime of disturbing public order, the determination of the circumstances of CHINCA simultaneously adopts the amount standard of economic crimes and the default circumstances standard of disorder crimes. This mixed application of standards has produced a significant "superposition effect". Judicial authorities can either charge based on the quantified amount or rely on the default clause to determine "other serious circumstances". These two paths proceed concurrently without contradiction and can be arbitrarily chosen to apply. Essentially, this doubles the possibility of criminalization, leading to an inappropriate expansion of the scope of punishment and becoming an important institutional factor that promotes the "pocketization" of this crime [11].

3.3. The "palliatives" predicament of organized crime

CHINCA faces a "treatment of symptoms but not the root cause" governance dilemma when dealing with organized cybercrime. This is manifested in the following two aspects.

Firstly, the current judicial practice of CHINCA has exhibited a peculiar judicial phenomenon of "combating but still increasingly emerging". This is due to two structural factors. On one hand, the judicial authorities are constrained by the difficulty of obtaining evidence and judicial inertia, and are more inclined to handle cases with clear evidence and simple collection methods, such as those involving "canongs" - individuals who provide bank cards and phone cards to assist information network criminals in illegal profit-making activities. On the other hand, the chain of gray industries has strong regenerative capabilities. Their core organizers can quickly replace the bottom-level participants who have been investigated, making it difficult for judicial strikes to cause substantial damage to criminal organizations.

4. The corrective path and future direction of CHINCA

4.1. Clarifying the nature of this crime should be a substantive preparatory offense

To establish a clear theoretical position for the crime of CHINCA, it is necessary to return to its essence as a "substantive preparatory offender".

As a substantive preparatory offender, the objective unlawfulness requires CHINCA must meet the establishment requirements of an "independent danger source". Only when the assisting behavior actually creates an independent danger source that can be utilized by subsequent criminal actors, and possesses the "qualification of preparatory behavior", can it meet the objective unlawfulness requirements of a substantive preparatory offender [13,14]. Even if the objective requirements are met, in specific cases, the subjective unlawful purpose still needs further examination. In judicial practice, it should be allowed to exclude the subjective unlawfulness purpose of the offender when the subjective and objective elements cannot mutually confirm, or there is contrary evidence. Adhering to the principle of "unification of subjectivity and objectivity", conducting a substantive examination of the subjective unlawful intention, and avoiding falling into the wrong region of objective criminalization [13,15]. The establishment of this theoretical positioning enables CHINCA to break away from its dependence on the conviction and sentencing of upstream crimes.

DOI: 10.54254/2753-7048/2026.ZJU31409

4.2. The refined determination of subjective knowing and objective circumstances

To address the deviations in the application of the CHINCA in judicial practice, relevant departments should formulate special judicial interpretations and issue guiding cases to promote the refinement and classification of the rules and establish a clearly structured and clearly targeted identification system.

In terms of the determination of subjective elements, China has currently established a hierarchical classification system: On one hand, it has established a general "knowing" rule, requiring judicial personnel to consider the specific circumstances of the case, as well as the perpetrator's cognitive ability, behavior pattern, and profit situation, etc.; on the other hand, special "knowing" rules have been set up specifically for high-incidence cases involving "two kinds of cards", through more specific and operational presumptive standards to achieve precise crackdown. This differentiated arrangement reflects the classification response strategy for different forms of cybercrime.

The objective circumstances have formed a preliminary systematic standard. General technical support and advertising promotion assistance behaviors are subject to ordinary regulations, while cases involving "two kinds of cards" are handled according to the specialized standards stipulated in Article 6, Paragraph 1 of the "Opinions of the Supreme Court, Supreme Procuratorate and Ministry of Public Security" issued in 2025. This standard clearly specifies quantitative indicators such as transaction amounts [16]. However, the provisions only make non-exhaustive enumerations for "other serious circumstances" and do not substantially limit them, leaving room for expansive application. To avoid the "pocketization" of circumstance determination, both directions of regulation are needed. In judicial practice, various circumstances should be applied in a coordinated manner, without separating the enumerated circumstances from the specialized standards, and without mechanically applying a single quantitative indicator; subsequent interpretative documents need to further refine the boundaries for determining "other serious circumstances" and impose restrictions on expansion at the normative level [17].

4.3. The modesty of judicial concepts: implementing the principle of "incrimination in form, but acquittal in essence"

To effectively narrow the scope of punishment for CHINCA, it is necessary to achieve a conceptual transformation at the judicial level from form-based judgment to substantive judgment, and to establish a systematic channel for substantive exoneration.

In the "Zheng's CHINCA Case", Zheng provided assistance in payment and settlement, and the amount of funds involved reached the 200,000-yuan threshold set by the judicial interpretation, meeting the constitutive requirements of the crime of assisting in CHINCA. However, upon a substantive examination, it was found that 40,000 yuan of the involved amount might belong to other crimes, and his actual profit was only 6,000 yuan, which did not reach the 10,000-yuan threshold for criminal liability. This case indicates that relying solely on the formal criteria may lead to an excessive expansion of the penalty scope. Therefore, it is urgent to establish a judicial channel for substantive exoneration. First, CHINCA involves emerging technological fields, so the evaluation of technological behaviors should go beyond mechanical formal judgments, and those who have reasonable flaws in their technical cognition should be exonerated. Secondly, the penalty is intended to punish behaviors with a substantive punitive nature. For behaviors that merely meet the criminal liability threshold in terms of form but have significantly minor comprehensive

DOI: 10.54254/2753-7048/2026.ZJU31409

circumstances and do not have a substantive punitive nature, they should be exonerated through substantive judgment [18].

4.4. Coordination between administration and criminalization: establishing a multi-level governance system

It is important to establish a hierarchical governance system for administrative violations and criminal offenses and improve the interconnection mechanism between administration and criminal justice to optimize the governance structure. The "Anti-Telecommunication and Internet Fraud Law" regulates the acts that provide communication and internet assistance for telecommunications and internet fraud and also introduces corresponding administrative penalties. By establishing administrative responsibility as a pre-emptive barrier, it lays a normative foundation for the comprehensive governance of the interconnection between administration and criminal justice.

In terms of operation, clear standards for case classification should be established. For minor helping behaviors, administrative penalties should be given priority, achieving "substantive exoneration" and controlling the criminal penalties. The case of Zhu, released in July 2025 in the "Typical Cases of Punishing CHINCA and Related Crimes," reflects this approach: Although the amount involved was large and criminal charges were involved, the procuratorial authorities made a relatively non-prosecution decision considering factors such as being an accessory, self-reporting, and returning the stolen funds. Later, the public security authorities imposed administrative penalties. The handling logic of this case clearly demonstrates the concept of "interconnection between administration and criminalization, and graded handling", providing practical reference for the handling of helping behaviors in cybercrime, such as CHINCA. Such mechanisms not only ensure the appropriateness of sanctions but also avoid the generalization of criminal penalties, which are the key path for building a multi-level governance system [18].

5. Conclusion

The creation of CHINCA is a positive legislative exploration in the context of the digital age. It indicates that in the face of the industrialized and chain-like cybercrime ecosystem; by legislating to categorize the assisting behavior as a separate crime and constructing a "full-chain" governance system, it can effectively fill the regulatory blind spots of the traditional accomplice theory. However, this study also reveals that this legislative tool aimed at enhancing governance efficiency has gradually shown a "pocketed" tendency and even fallen into the governance paradox of "combating but still increasingly emerging" in practice due to the generalization of "knowing" determination, the ambiguity of behavioral boundaries, and the mechanized application of the "serious circumstances" standard. To address this predicament, this paper systematically reviews corrective paths such as the reconstruction of the "substantive preparatory offense" theory, legislative refinement, and judicial limitation in an attempt to maintain the effectiveness of the crackdown while strengthening the observance of the principles of criminal law's restraint and the balance of punishment and crime. At the same time, through presenting the "accommodation and dilemma coexisting" practical example of China's CHINCA, this paper provides a profound reference for global cybercrime governance: In order to seek a sustainable balance between crime crackdown and justice, countries should not only attach importance to the construction of legislative tools, but also pay attention to the clarity of the constituent elements, the constraint mechanism of judicial power, and the protection of citizens' rights.

DOI: 10.54254/2753-7048/2026.ZJU31409

References

[1] Jiang, L. (2025) From the Perspective of 'Duality': Judicial Determination of 'Knowing' in the Crime of Assisting Information Network Criminal Activities - Based on 1082 Relevant Judgments as Research Samples. Journal of Law, 46(05), 73-93.

[2] Shao, D. (2024) Constraints and Breakthroughs in Proving "Knowing" for the Crime of Assisting Information Network Criminal Activities. Journal of Gansu University of Political Science and Law, (02), 123-134.

[3] Chen, B. (2024) On the Judicial Determination of the Crime of Assisting Information Network Criminal Activities. Journal of Henan University (Social Sciences Edition), 64(02), 53-57 + 153-154.

[4] Yue, H. (2022) Judicial Limitations and Specific Expansions of the Crime of Assisting Information Network Criminal Activities. Journal of the National Prosecutor Institute, 30(06), 101-113.

[5] Lu, J. & Yan, E. (2023) The Positioning and Identification of the Crime of Assisting Information Network Criminal Activities: Empirical, Theoretical and Regulatory Perspectives - Based on 26 Criminal Second Instance Rectification Judgments. Criminal Law Review Series, 75(03), 1-26.

[6] Yan, E. (2024) Legislative Interpretation and Judicial Correction of the Crime of Assisting Information Network Criminal Activities. Legal Science (Journal of Northwest University of Political Science and Law), 42(05), 117-128.

[7] Zhou, Z. & Zhao, C. (2022) Empirical Study on the Crime of Assisting Information Network Criminal Activities - Based on 1, 081 Judgments as Samples. Legal Application, (06), 83-93.

[8] Chen, H. (2022) Rectifying the "Pocketization" of the Crime of Assisting Information Network Criminal Activities. Journal of Hunan University (Social Sciences Edition), 36(02), 127-135.

[9] Jing, L. (2025) On the Normative Attributes of the Crime of Assisting Information Network Criminal Activities. Jurist, (02), 116-130 + 194-195.

[10] Gu, J. & Song, S. (2022) The Nature and Restriction of the Crime of Helping Information Network Crime. In 2022 8th International Conference on Humanities and Social Science Research (ICHSSR 2022) (pp. 2343-2347). Atlantis Press.

[11] Cheng, H., Li, P. & Li, S. (2022) Definition of “Knowing” of Internet Service Providers in Helping Cybercrime. In 2022 6th International Seminar on Education, Management and Social Sciences (ISEMSS 2022) (pp. 3645-3655). Atlantis Press.

[12] Wang, S. (2025) Analysis of Difficult Issues in the Judicial Application of the Crime of Assisting Information Network Criminal Activities. Chinese Applied Law, (04), 58-69.

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

[14] Cernomoreț, S. & Nastas, A. (2023) Comparative Analysis of Cybercrime in the Criminal Law System(1st ed.). Adjuris - International Academic Publishers.

[15] Baker, D.J. & Robinson, P.H. (Eds.) (2021) Artificial intelligence and the law : cybercrime and criminal liability. Routledge.

[16] Interpol (2023) Creating Communities to Protect Communities, Interpol Global Cybercrime Conference 2023 Outcome Report. https: //www.interpol.int/content/download/20960/file/INTERPOL%20Global%20Cybercrime%20Conference%202023%20-%20Outcome%20Report(Last visited Dec. 13, 2025).

[17] Supreme People's Court & Supreme People's Procuratorate (2019) Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network.

[18] Supreme People's Court, Supreme People's Procuratorate & Ministry of Public Security (2025) Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Handling Criminal Cases Involving Aiding Criminal Activities on an Information Network, Among Others