Proceedings of ICSPHS 2026 Symposium:Ethics, Law, and Psychology: Interdisciplinary Reconstruction of Humanities in Medicine
DOI: 10.54254/2753-7048/2026.ZJU31706

The Dilemma and Solutions in Determining "Knowing" for the Crime of Assisting Information Network Criminal Activities

Fengxuan Wang

College of Humanities and Social Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing, China
wangfengxuan@nuaa.edu.cn

Abstract. Since the addition of the crime of assisting in the commission of information network criminal activity to the Criminal Law in the 2015 Amendment IX. This offense has continuously increased in judicial application due to its alignment with comprehensive governance demands for cybercrime. It has become the number one or two most prosecuted crimes in China. "Knowing" is the essential core of this crime, which is the distinction line between bearing criminal responsibility and not bearing criminal responsibility, as well as the demarcation line for defining a person's criminal liability. However, because of its covert and chain-like characteristics, it often makes it hard to get some direct evidence for the crime of "knowing", judicial proceedings have begun to see more problems with words slipping down, lower standards, more generalized presumptions, and lack of reasons. This paper systematically studies practical problems and underlying causes when determining "knowing" for aiding and abetting crimes by using the logical method of "problem identification-root cause analysis-solution construction" It proposes solutions including establishing a scientific determination system, standardizing presumption applications, refining comprehensive assessment criteria, and strengthening policy and case guidance. These aim to provide theoretical support for judicial practice, achieving a balance between precision in combating cybercrime and the principle of restraint in criminal law.

Keywords: Cybercrime, accessory, knowing

1. Introduction

With the rapid development of the digital economy, cybercrime will show the features of industrial chain formation, cross-regional development and technological sophistication, which brings great challenge to the traditional criminal governance. To address this reality, the 2015 Amendment IX to the Criminal Law introduced the crime of assisting and facilitating cybercrime, criminalizing the act of aiding within the cybercrime chain and providing a normative basis for combating cybercrime across its entire spectrum. As shown by the data released by the Supreme People's Procuratorate, since the criminalization of the crime of assisting and facilitating cybercrime, the application field of it has been constantly expanding. In 2021, procuratorial organs across the country prosecuted nearly

DOI: 10.54254/2753-7048/2026.ZJU31706

130,000 people, 9.5 times increase from 2020. Now it's the third most frequent criminal allegation after dangerous driving and theft. And cases that include "two cards" - phone cards and bank cards - made up as much as 80% of the total. In the end, put forward the solution of building a scientific identification system, regulating presumptive application, improving all-round identification standards, and improving policies and case guidance.

"Knowing" is the subjective aspect for the crime of assisting and facilitating information network crime. Its correctness directly determines the justice of single cases and the effectiveness of cybercrime administration. The crime is completed only when "the perpetrator is aware and knowingly assists others who use information network to commit the crime using internet access, server provision, network storage, communication transmission or provides other assistance such as publicizing, promoting, final payment settlement" under serious circumstances, thus the prerequisite of "knowing" is the essential condition for the crime of helping and facilitating criminal activities. Without "guilt," those who commit the "crime" lack the criminal intent and should not bear criminal responsibility. But it is not easy to prove the criminal's subjective aspect because of the covert characteristic of cybercrime. Judges usually make an inference to make out what does "knowing" by referring to the objective facts, and the process has brought out problems like inconsistent standards, non-standardized operations, and inconsistent rulings for similar cases. Therefore, this article intends to analyze the practical dilemma and deep-seated cause in the determination of "knowing" in the crime of helping and facilitating criminal activities. It ended up putting out solutions like setting up an objective determination system, changing presumptions according to rules, making improvements to all-around determination standards, and strengthening policies and cases guidance.

2. Practical chaos in determining "knowing" for aiding and abetting cybercrime

2.1. Semantic slippage from "explicit knowing" to "should have known"

"Knowing" is usually understood as "explicit knowing," that is, the perpetrator holds specific and accurate knowledge about the other party who uses information networks to engage in criminal activities. It's about the wrong person knowing about the criminal situation. It's usual for the court not to be able to verify "clearly aware." So, the courts use both "should have known" and "knowing" [1].

This semantic confusion has expanded intentional crime. As for should have known there are also two different interpretations: First," should have known" bearing negligence means" should have known" perpetrator don't find something because they don't use reasonable care. This state of "ignorance" itself is a kind of attributable mental state, serving as the standard for establishing fault. Second, "presumed knowing" means a legal presumption, in accordance with statutory conditions, or facts already known, the law directly assumes that the perpetrator is aware of the facts, irrespective of their subjective state.

Judges also saw things like continuing to provide a bank card after a frozen one was a case of "presumed knowing." Even if the rural middle-aged and elderly lend their bank cards when they are led by others, it is also written in judicial documents as "presumed knowing" cases. This has caused people's standard of cognition to shift to the negligent meaning of should have known, ignoring the inherent distinction between actual cognition possibilities of the actor and their subjective intent [2].

This violates the unity of subjective opinions with objective facts. As a basic principle of Chinese criminal law, such a requirement is that a crime can only be created when there is a subjective fault and an objective act at the same time, the two are united and cannot be separated. As intentional

DOI: 10.54254/2753-7048/2026.ZJU31706

crime, the perpetrator of the crime of assisting and facilitating cybercrime must have the subjective "knowing" to commit the crime and, objectively, do something to help a cybercrime. When it's true that both conditions have to be met, then the crime can be committed. Using should have known within the scope of knowing in the crime of assisting and facilitating cybercrimes, this means it is the same as committing the crime intentionally when people are negligent, when people have knowledge of something. This violates the criteria for distinguishing between intentional and negligent culpability and exceeds the constitutive requirements of the crime of assisting and facilitating cybercrimes as an intentional offense.

2.2. Abuse of "likely to know" and "knowing the likelihood"

There are two inappropriate applications for "knowing" on aiding and abetting cybercrimes: First low threshold for criminal liability. The main problem is that the actor only has some hazy ideas about others committing crimes through informational networks, with unclear ideas. Not only does it fail to meet the subjective criteria of intentional crimes, but it also violates the proof standard of "beyond reasonable doubt," and thus does not constitute grounds for criminal liability. However, in practice, some case's rulings have mistakenly regarded this low-probability awareness as "knowing", like in the technical support case, where the defendant was convicted based on "should be known", he was also charged with a service fee slightly higher than the market price, which blurred the line between crime and non-crime [3].

Second, the vague application of "knowing of possibility," this cognitive state is in the middle "knowing" and "probably knowing," the perpetrator obviously understands the possibility of a cybercrime, but don't get to the stage of "quite certain." There is no clear standard, and the application is inconsistent. For example, in two payment settlement cases, it convicted the offender based on knowing the "possibilites", regardless of whether the possiblity was explicit that the payment interface was to be used for online gambling, or that the payment interface was to be used for fraud with extremely low chance [4].

2.3. Simplified determination methods: overreliance and overgeneralization of legal presumptions

Mechanical Application prescriptive rules. To fill in for the lack of direct evidence demonstrating "knowing" in aiding and abetting cybercrime, article 11 of the 2019 interpretation of aiding and abetting cybercrime provides for 7 scenarios in which "knowing" may be assumed. It includes after receiving a notice from regulatory authorities, continuing to carry out related acts; transaction price or method is obviously abnormal; It refers to programs, tools, or other technical support designed specifically for illegal or criminal activities. The presumption rules provide important operation guide for judicial practice. It has positive significance for solving the problem of evidence. But in judicial practice, the judicial staff mechanically apply these presumption rules without examining the connection between the underlying fact and the presumed fact, and thus directly draw unreasonable presumption conclusion [5]. For example, some judicial documents directly classify "using someone else's bank card for compensation" as "obviously abnormal transaction methods" and then presume that the actor "knowing". They neglect the specific context and reasonable range of the bank card lending and the transaction price.

Abuse of Catch - all Clauses and Failure of Rebuttal Mechanisms. Article 11 (7) of interpretation on the crime of helping and facilitating criminal activities gives a catch all provision for" other circumstances sufficient to establish the perpetrator has knowledge", hence flexibility. However,

DOI: 10.54254/2753-7048/2026.ZJU31706

under practical situations, some judicial staff tend to rely on it too much and incorporate situations without valid reasons as possible scenarios for presumption, thereby leading to the abuse of this provision [6].

And at the same time, the rebuttal for presumption rule is also nearly powerless. Under the basic principle of the Criminal Procedure Law, defendants have the right to make their own defense. Judges need to look at and find out if the evidence that is not reasonable backlash from the defendant is true. But in terms of how "knowing" applies to aiding and abetting crimes, defendants don't always have the ability to give solid proof, so their "not knowing" argument is hard to believe. For a defendant may say that he is "deceived by others and does not know that his bank card will be used for cybercrime," and it makes no difference whether there is evidence proving that he is deceived, such a defense will be boldly rejected.

3. Causes of the dilemma in determining "knowing" for the crime of assisting and facilitating criminal activities

3.1. Theoretical roots: conceptual discrepancies

As for the difficulty in establishing "knowing", the root cause is the ambiguity regarding the core meaning of "knowing" and the unclear definition of related words by scholars, resulting in judicial application ambiguity [7]. As for the different meanings of "knowing," there are three schools of thought: the explicit knowing theory, the knowing or should-have-known theory, and the high probability theory. And those terms like 'should have known' and 'could have known' as well: For example, some scholars classify it as implied intent by some scholars, and some classify it as negligence. The "could have known" and "knew it was possible" attributes, as well as what constitutes "knowing," have not been defined.

Another major root cause is the inconsistent doctrinal stance regarding the crime of assisting and facilitating criminal activities, with two prominent views: "treating accomplices as principal offenders" and "sentencing rules", according to the former view, this crime is unrelated to upstream crime, some judicial personnel lower the bar for knowing, broaden the scope of punishment. The latter maintains that it depends upon the existence of upstream crime, and some judicial personnel have raised the bar for establishing knowing, thus allowing actions that should have been criminalized to slip by [8].

3.2. Regulatory roots: conflicting judicial interpretations and rule design flaws

The core "knowing" normative root of the determination of helping and assisting crimes is due to the conflicting normative document having no clear rule, resulting in different judicial applications. In 2019's interpretation on aiding and abetting cybercrime, they came out with an approach that's called "presumption" which provided for a total of 7 presumption scenarios in which they infer the subjective knowing through objective facts. In 2021 Opinions on combating telecommunication fraud (II), it is stated that comprehensive determination must be conducted, where a full examination of numerous subjective and objective elements should be considered rather than relying on presumption. There's confusion when these two ways coexist.

And neither has operate standards. Presumption rules have problems like lack of necessary correlation between basic facts and inferable facts, insufficient ways to avoid it, and too broad a category provision. The comprehensive determination approach only lists the factors to be considered, without specifying the weight of these factors, the order of review, and the standards for

DOI: 10.54254/2753-7048/2026.ZJU31706

evidence, making it nothing more than a simple "stacking" of elements. In judicial practice, some people handling cases lack logical accuracy and jump straight to a conclusion by picking just one or a few elements, without considering the weight of subjective and objective factors or effectively corroborating evidence.

3.3. Practical roots: policy driven and judicial convenience

Excessive Policy Bias. In recent years, to address the severe threat of cybercrime, China has introduced a series of criminal policies aimed at combating cybercrime across the entire chain, such as the "Operation to Cut Off Card Fraud" and "Operation to Clean Up the Internet," emphasizing severe crackdowns on cybercrimes and their supporting acts. While these policies are crucial for curbing cybercrime proliferation, some judicial personnel have excessively accommodated policy directives in practice, prioritizing policy objectives over legal principles. This has led to an inappropriate relaxation of the standard for establishing "knowing" in aiding and abetting cybercrime cases. Under the influence of the "full-chain crackdown" policy, some judicial personnel have developed a "better safe than sorry" inertia in their determinations. They believe that as long as an individual’s actions objectively provided assistance to cybercrimes, they should be deemed to have had "knowing" whenever possible. This approach aims to broaden the scope of punishment and achieve the policy goal of combating crime. This policy-driven tendency has led to the widespread application of cognitive states like "should have known" or "might have known"—which should not fall under "knowing"—resulting in frequent semantic slippage and diminished standards.

Impact of Judicial Convenience. In judicial practice, faced with the reality of heavy caseloads, few judicial personnel, and the high application rate of the leniency system for guilty pleas. A few judicial personnel began using a "simplified determination" method. This way it can just directly infer that it knows something, so it saves on needing to prove it and makes cases go faster. Confirming This desire for judicial convenience also makes things even more unclear about what "knowing" is. There are lots of cases involving people who assist and help others do illegal things, and these cases have many parts from different places and require a lot of technical knowledge. Prove the guilty person's subjective "knowing" requires many judicial resources; Under the pressure of heavy caseload and few personnel, some judicial staff, in order to save time and avoid meticulous evidence examination and logical reasoning, But, instead of inference like "knowing", knowing is inferred from objective indicators like the transaction amount or profit amount. There is a strong tendency towards objective responsibility [9].

4. Establishing a framework for determining "knowing" in aiding and abetting information network crime

4.1. Establishing a scientific framework for determining "knowing"

Core meaning "knowing" is restricted only to "knowing" that is "explicitly known" or "highly probable known," and it excludes "should have known" and "might have known" from building up criminal liability [2]. "Explicit knowing" indicates the most usual type of "knowing," and "probably highly knowing" is indirect intention to create harmful effects being reckless about it, this corresponds to the subjective component required for "aiding and abetting" a crime" "should have known" amounts to negligence, which contrasts with the intent-based nature of "aiding and abetting" a crime [10]. It should be excluded from the scope of "knowing" "could have known" Due to the

DOI: 10.54254/2753-7048/2026.ZJU31706

uncertain nature of "could have known", it is also excluded from the "beyond a reasonable doubt" standard of proof.

As for doctrinal disputes surrounding the crime of aiding and abetting cybercrime, determining "knowing": must take into account the independence of "treating accomplices as principal offenders"; also consider the appropriateness of "sentencing rules": Where the upstream crime is unprosecuted but proven to be factual, the crime of aiding and abetting cybercrime can be established, but the requirement for knowing should be strengthened (such as needing to prove that the perpetrator knew what specific upstream crime), where the upstream crime cannot be verified, then knowing cannot be determined based on the transaction amount.

4.2. Standardizing the application of legal presumptions

To prevent the overbroad application of presumption rules, adhere to the principle of restraint in presumptions and establish the application sequence of "direct proof first, presumption second" [6]. When presumptions can only be made when direct evidence can be obtained but evidence is still lacking; indirect evidence does not have a continuous chain of evidence and can only be used as a judgment method. No explanations or comments. When judges deal with cases of aiding and abetting the use of illegal information networks, they can first use primary evidence that including the defendant's statement, witnesses and chat records to prove "knowing" the defendant "knowing". As long as there is any real evidence, it is not advisable to apply presumption rules, and the connection between the unseen facts and the presumed facts should be seriously reviewed.

To protect the lawful rights of the defendant, there must be further improvement of rebuttal mechanism of presumption rule, which should clarify the standard of proof for rebuttal and the form of rebuttal evidence. When the defendant presents rebuttal evidence, they need to prove the "overwhelming likelihood" of not knowing, so they only need to prove that the chances of not knowing are greater than those of knowing. There is no need for the burden of proof to reach "beyond reasonable doubt" [11]. Admissible rebuttal evidence includes: the perpetrator's previous legitimate professional career, evidence of fraud, evidence of insufficient cognitive ability [10]. Judicial personnel need to rigorously examine the counterevidence submitted by defendants and adopt reasonable rebuttals instead of summarily rejecting them. At the same time, the obligation to provide reasons in judicial documents should be strengthened, and judicial officials must explain in judgments how they apply the presumption, including the verification of the basic facts, the connection between the basic fact and the presumed fact, and the reasons for rejecting counterevidence, rather than merely listing circumstances to establish knowing [12].

4.3. Establishing substantive comprehensive determination standards

The comprehensive determination model is the core approach to resolving the "knowing" recognition dilemma in aiding and abetting cybercrime. A complete framework incorporating subjective and objective elements should be established to provide clear operational guidance for judicial practice. Subjective elements primarily include: (1) cognitive capacity; (2) prior experience; (3) consistency of statements and reasonableness of defenses; (4) relationship with the aided party, etc. Objective elements primarily include: (1) characteristics of the assistance provided; (2) transaction methods; (3) profit-making circumstances; (4) actions to evade regulatory oversight; (5) the criminal nature of the assisted conduct, etc. When making comprehensive determinations, judicial personnel should comprehensively examine the aforementioned subjective and objective elements to ensure rationality and accuracy of the conclusion [3].

DOI: 10.54254/2753-7048/2026.ZJU31706

To avoid becoming an "accumulation of all reasons" and to prevent comprehensive determinations, people need to establish a clear logical order and rules for assessing these elements. Review sequence follows "core elements first, supplementary elements second": Core elements like]"ontinue related action", "set up procedures / tools for illegal actions", reflect the actor's subjective state and require examination first. When there is a core element deficiency, supplementing elements such as abnormal transaction prices and profit situations should be conducted, with multiple supplementary elements averaged so as to make one supplementary evidence chain complete. Weighting should be decided according to the degree of correlation with "actual knowing", factors such as cognitive ability, regulatory warnings, and specialist assistance all have high correlation and should hold greater weight; factors like transaction prices and profits, their correlation is weak and should hold lesser weight and cannot form the sole basis of "actually knowing".

4.4. Policy improvement and case guidance

China’s fundamental criminal policy emphasizes a balanced approach of leniency and strictness. In determining "knowing" for the crime of assisting and facilitating criminal activities, this principle should be upheld to avoid a one-size-fits-all approach, achieving a balance between combating crime and safeguarding human rights. For professional facilitators or repeat offenders, strict determination of "knowing" should be applied with heavier penalties. Such conduct exhibits greater subjective malice and severe social harm, aligning with the legislative intent of the crime and warranting severe punishment.In cases warranting leniency, special consideration should be given to vulnerable groups such as the elderly or those with limited cognitive abilities, as well as situations involving minimal profit or deception. Where genuine lack of knowing is established, acquittal should be granted. Such acts demonstrate lesser subjective malice and reduced social harm. Applying leniency aligns with the principle of restraint in criminal law and facilitates the educational and rehabilitative functions of punishment [13].

In order to clarify the standards for judging whether it is "aware" and to reduce the differences in judgments of similar cases, people need to strengthen the construction of mechanisms such as case guidance and query of similar cases, Supreme People's Court and the Supreme People's Procuratorate should regularly release typical cases involving the determination of "knowing" in aiding and abetting crimes and make it clear what kind of "knowing" should be established in various situations. Also include the rule on how to determine what "knowing" is in situations such as "two-card" aiding and abetting, technical support aiding and abetting, and advertising promotion aiding and abetting, so that there is clear guidance for grassroots judicial practice. At the same time, improve the case retrieval mechanism. Judicial officials dealing with crimes of helping and facilitating criminals should find leading cases, typical cases released by the Supreme People's Court, and similar final judgments from their region and court to ensure similar or consistent judgments in similar circumstances. For rulings that are inconsistent with the rules set by rulings on cases similar to the current case, reasons must be given in the judgment so as not to result in different rulings on similar cases.

5. Conclusion

The crime of aiding and abetting online crimes, as a core offense designed to address the entire chain of cybercrime governance, relies on the accuracy of determining "knowing" to ensure the fairness of criminal prosecution and the effectiveness of cyber governance. In judicial practice, the determination of "knowing" has fallen into chaos characterized by semantic slippage, diminished

DOI: 10.54254/2753-7048/2026.ZJU31706

standards, and generalized presumptions. This essentially deviates from the principle of unifying subjective intent with objective conduct. Its root causes lie in theoretical conceptual disagreements, conflicting judicial interpretations, and judicial expediency driven by policy considerations. This not only blurs the boundaries between criminal and non-criminal conduct but may also lead to an improper expansion of the scope of criminal punishment.

TElementve this dilemma, a systematic approach must establish a multi-faceted, collaborative framework for determination: Define the core essence of "knowing" through "explicit knowing" and "highly probable knowing," clarifying the distinction between intent and negligence; Regulate presumption application through sequential requirements ("prove first, then presume") and robust rebuttal mechanisms to prevent rule abuse; Relying on substantive, integrated examination of subjective and objective elements, clarify the weighting of factors and the logic of review to avoid "element piling"; combine the policy of balancing leniency and severity with case guidance mechanisms to achieve precise determination in different scenarios.

This approach addresses practical demands in combating cybercrime while upholding the principle of restraint in criminal law, effectively resolving practical disagreements over "knowing" determinations. As the recognition system matures and judicial application becomes standardized, the crime of assisting and facilitating cybercrime will more precisely fulfill its function of punishing aiding acts in cybercrime. This achieves an organic unity between combating crime and safeguarding human rights, providing robust criminal legal support for cyberspace governance in the digital economy era.

References

[1] Jiang, L. (2025) The Judicial Determination of "Knowing" in the Crime of Assisting Information Network Criminal Activities from a "Dual Nature" Perspective: A Study Based on 1, 082 Relevant Judgments. Journal of Jurisprudence, 46(05), 73-93.
[2] Chen, B. Z. (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.
[3] Mao, B. (2022) The Dilemma and Reflection on the Determination of "Knowing" in the Crime of Assisting Information Network Criminal Activities. Evidence Science, 30(06), 730-742.
[4] Wang, H. (2024) Judicial Misconceptions and Theoretical Corrections Regarding the Crime of Assisting Information Network Crime Activities. Financial and Economic Law, (05), 179-192.
[5] Li, Y. (2023) Risks and Countermeasures of Presumptive Knowledge in the Crime of Assisting Information Network Crime Activities. Evidence Science, 31(05), 541-551.
[6] He, B. and Hu, L. (2023) On Proving "Knowing" in the Crime of Assisting Information Network Crime Activities: From Presumption to Comprehensive Determination. Journal of Liaoning Normal University (Social Sciences Edition), 46(02), 60-69.
[7] Yan, E. P. (2024) Legislative Interpretation and Judicial Correction of the Crime of Assisting Information Network Crime Activities. Legal Science (Journal of Northwest University of Political Science and Law), 42 (05), 117-128.
[8] Wang, S.-Z. (2025) Analysis of Difficulties in Judicial Application of the Crime of Assisting Information Network Crime Activities. Chinese Applied Jurisprudence, (04), 58-69.
[9] Shao, D. (2024) Obstacles and Breakthroughs in Proving "Knowing" for the Crime of Assisting Information Network Crime Activities. Journal of Gansu University of Political Science and Law, (02), 123-134.
[10] Long, Z. and Hu, J. (2024) Determining "Knowing" in the Crime of Assisting Information Network Crime Activities. Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), 45(01), 61-72.
[11] Wang, Y. and Ma, Q. (2023) Inclusive Regulation of the Presumption of Knowledge Rule in the Crime of Assisting Information Network Criminal Activities. Journal of Political Science and Law, 40(02), 13-24.
[12] Liu, S. and Jiang, L. (2025) Judicial Dilemmas and Solutions in Determining "Criminality" for the Crime of Assisting Information Network Criminal Activities. Journal of University of Chinese Academy of Social Sciences, 45 (07), 103-118+143-144.

DOI: 10.54254/2753-7048/2026.ZJU31706

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