

Analysis of the Causes of the Crime of "Naked Chat" Extortion and Prevention Measures to Explore

Lan Ding

Southwest Petroleum University Law School, Chengdu Sichuan, 610000, China

ABSTRACT

The rapid development of the Internet has brought convenience to people and at the same time given rise to the crime of "naked chat" extortion and blackmail. Although in the public security department's vigorous investigation and various departments of the coordinated governance, has solved a number of "naked chat" type extortion cases, but due to the criminal gang technology enhancement, the crime of geographic area wide, evidence fixing difficulties and other aspects of the reasons, "naked chat" type extortion crime is still very difficult to govern and combat. Extortion and blackmail crime of governance and combat is still very difficult. Therefore, this paper analyzes the reasons for the difficulty in combating the crime of "naked chat" extortion and blackmail from the three aspects of offenders, victims and platform supervision, and proposes to prevent and combat this type of crime by improving publicity and education, strengthening platform supervision and enhancing law enforcement coordination.

KEYWORDS

cybercrime; extortion; preventive measures

1 Introduction

With the rapid development of network technology in China, the traditional crime of extortion has gradually given rise to a new model of cybercrime. Unlike traditional crime, network extortion does not require actual contact, the offender directly through the network platform to create psychological coercion, forcing the victim to deliver property. The common forms of such crimes include "loans", "malicious claims" and "nude chat extortion", etc., of which the "nude chat" type of crime is particularly special: First, the criminal means to privacy threat instead of traditional violence, through social software to induce victims to participate in the nude chat and record video, and then the implementation of persistent extortion; Secondly, some of the victims due to their own participation in the nude chat fault, often for fear of damage to the reputation of the choice to hold back. Data show that nearly 40% of the nude chat case victims even if suffered multiple blackmail still refused to report, this "double concern" not only contributes to the spread of crime, but also increase the judicial authorities to collect evidence, cross-regional tracing and other difficulties in handling the case (Li&Wang,2021). According to statistics, since the emergence of the "naked chat" type of crime in 2012, most of the early crimes were committed alone, and the amount of money involved and the loss of victims were relatively low. However, after 2018, with the development of the Internet, the number of such crimes has increased significantly, and the number of gangs has increased, with the amount of money involved reaching up to 1.83 million yuan(cheng,2023). This shows that it is necessary and urgent to carry out systematic research on the crime of "naked chat" extortion. At present, there is relatively little academic research on this crime, which is both a cybernetic crime and a telecommunication fraud crime, and there are many difficulties in practical combating and prevention. Therefore, this paper analyzes the current situation of "naked chat" type of extortion, explore the causes of this type of crime, and combined with the current judicial authorities to combat crime to put forward "naked chat" type of extortion prevention and control measures.

2 Reasons for the crime of "Naked Chat" extortion and blackmail

"Naked chat" refers to through the network channel, one or more people will show their sexual organs to others to watch, accompanied by other sexual action and obscene language and others to communicate, so as to achieve stimulation or solve their own sexual needs of a chat(Wang&Dong,2023). "Naked chat" extortion crime is criminals in advance organized strategy, inducing the victim to 'naked chat', take the opportunity to obtain the victim's indecent photos and video information, so as to coerce the victim, to achieve illegal acquisition of other people's property Purpose. Currently, this type of crime is frequent, and the amount of money involved in the case is gradually increasing, there are platform supervision, offenders, victims and other levels of reasons.(Mou,2023)

2.1 Platform regulatory level

The entire process of the "naked chat" type of extortion and blackmail crime takes place in the virtual space of the

Internet, which is currently a blind spot for monitoring and control. "Naked chat" usually involves a private one-on-one chat between two parties, so it is very difficult to directly monitor the specific two users. And the perpetrators usually use chat accounts are not registered with real names, and it is difficult for the platform and the police to lock the perpetrators afterward. Secondly, the "naked chat" type of extortion also involves the result of illegally obtaining other people's property. Offenders in this type of extortion will first provide the victim with a remittance account, allowing the victim to make online transfers. However, such accounts are usually purchased by the perpetrator of other people's legitimate accounts, the victim to transfer funds, the perpetrator will quickly transfer funds, so the process of transferring funds is very difficult to monitor. Therefore, "naked chat" extortion in the whole process of extortion, unless the offender himself to the police, or various regulatory platforms are very difficult to monitor and defend the rights and interests of the victim (Zhao,2023).

There are impediments to monitoring and combating the crime after it has occurred. First, the spatial scope of "naked chat" extortion cases is very wide, not only in China, but also in various countries outside the country. Therefore, the public security departments need to investigate this type of case, it is necessary to local public security departments to coordinate, however, the collaboration process requires a variety of processes and approval procedures are more stringent, it is difficult to realize the rapid coordination of work between the departments around the world. And such cases involving foreign countries also face problems such as the right to investigate and language barriers between different countries, making it even more difficult for public security departments to carry out investigations. Secondly, the fixing of electronic evidence after a crime has been committed is also a major problem. Common electronic evidence usually includes chat records, transfer records, screenshots, cell phone text messages, etc., but with the improvement of the technical level of the criminal gangs, nowadays the criminal gangs will remotely erase the criminal information on a regular basis, which brings great difficulties to the police in fixing the evidence(Chen&Yang,2021).

2.2 Offender level

First of all, "naked chat" type extortion can bring low-cost high-yield pleasure to the perpetrators. "Naked chat" type extortion offenders are often their own poor economic conditions, lower education, most of them belong to the unemployed, this kind of group is difficult to get through the legitimate means and ways to have a stable high income job. Long-term low-income status is very easy to make the individual's physiological and psychological condition is not sound, which led to the emergence of illegal and criminal behavior. "Naked chat" type extortion and blackmail crime for them is a low-cost criminal behavior, only need a cell phone, using certain words can chat with the victim, and then take the opportunity to obtain the victim's private information for extortion and blackmail, you can get income. "Naked chat" type criminal groups usually publish information containing 'high salary', 'no educational requirements', "quick to get started The "nude chat" groups usually post recruitment information containing "high pay," "no education requirements," "quick start," and similar phrases to attract this type of person to join them. Stimulated by the thrill of such low income and high earnings, offenders will be more and more immersed in criminal behavior, unable to wake up.

Second, the perpetrator of "naked chat" type extortion subject to criminal penalties by chance. Through the above analysis of the offender's own situation can be learned that the offender is usually difficult economic situation, lower education, their own inevitable lack of awareness of the rule of law, a lack of awareness of the consequences of crime. And the victim himself is not willing to occur in the virtual space of the naked chat behavior is known, therefore, when the victim was extortion amount within the scope of their ability to bear, the victim will not choose to report to the police. This is one of the reasons why offenders are lucky. On the other hand, some offenders have superiority in location, offenders choose to commit crimes outside the country, our public security organs are difficult to further track down, but also can not achieve a comprehensive crackdown on such crimes.

2.3 Victim level

"Naked chat" type extortion at fault party is more special not only includes the perpetrator but also the offender, due to multiple reasons at the level of the victim also leads to the public security organs to investigate and combat the crime is difficult. Offenders in the implementation of the crime will usually choose the right target, this type of person for the offender to approach and implement extortion, out of shame will respond in time to the offender's demand, so that the offender quickly get economic benefits. Generally speaking, the victim's physical, psychological, behavioral and other aspects will affect whether it will become a potential target of the offender.

Physical and psychological factors of victims. In recent years, analysis of "naked chat" extortion crimes has shown that the proportion of male victims is much higher than that of women. The 2021 Telecommunications Network Fraud Governance Research Report shows that the proportion of male victims in pornography fraud reached 93%, and the proportion of male victims in naked chat fraud reached 85%. Male victims mostly in the late night "naked chat", the lack of third-party supervision, more likely to fall under the temptation to become a victim. From the perspective of

psychological factors, victims have a weaker sense of prevention and are prone to gullibility. They often believe in the image portrayed by the offender because of his or her words, exposing their privacy. Afterwards, victims often use "hot-headedness" as an excuse, but in essence, it is the existence of the pursuit of excitement, frivolity and other psychological (Shen,Wang&Zhang,2023).

The manner in which the victim behaves. The victim's behavior and his frequent exposure to dangerous environments make him an easier target for crime. In today's network era, people's friendship is no longer limited to the reality of contact, "naked chat" type of crime can be implemented only through the social platform communication. Victims initially to meet the social needs of the extensive use of social software, but was attracted to the network of pornography, undesirable information. Such behavior exposes them to the virtual environment of the network, making them ideal targets for offenders and increasing the likelihood of the crime being committed.

3 Countermeasures against the crime of "naked chatting" extortion and racketeering

3.1 Improvement of publicity and education

In order to prevent the "naked chat" type of extortion crime, the police have taken a variety of ways to publicize, but the effect is still not obvious. The reason is that the means of crime is becoming increasingly diversified, and the publicity is not targeted. Therefore, preventive publicity should be a long-term work. First of all, the police can develop a long-term network security publicity program to ensure the continuity and systematic publicity, and in important festivals and anniversaries to carry out thematic publicity activities to enhance the publicity effect. Second, broaden publicity channels and utilize social media, short video platforms, live broadcasts and other emerging media to produce easy-to-communicate and attractive publicity content to attract more people's attention. Once again, interactive publicity and education is carried out, designing online games so that participants can learn preventive knowledge in the game; offline, network experts are invited to explain the crime process, so as to enhance the infectious power of publicity. Finally, precise publicity was conducted for teenagers, young people, singles and groups with weak awareness of cybersecurity, emphasizing the importance of personal information protection and informing them of the legal consequences of leaking their personal information, thereby deterring them from illegal cyberinformation and lowering the risk of being extorted and blackmailed.(Wang,2023)

3.2 Strengthening platform regulation

Strengthening the regulation of Internet platforms is also a key aspect of preventing the crime of "naked chat" extortion. Internet platforms should also assume their own responsibilities when they reap the benefits of the Internet (Yang, 2022). First of all, we should formulate clear legal provisions to establish the main responsibility of Internet platforms in preventing and combating cybercrime, including but not limited to the review of user uploaded content, the monitoring of abnormal behavior. And during peak hours, the number of content reviewers should be increased to ensure that a large amount of user uploaded content can be effectively reviewed. Secondly, platforms should further improve their own regulatory technology. The state should encourage Internet platforms to adopt artificial intelligence, big data analysis and other technical means to monitor user behavior in real time, and automatically identify and block content and activities suspected of extortion. And further develop a cybercrime early warning system to predict and prevent potential extortion and blackmail activities through pattern analysis of user behavior. Again, establish a user reporting and feedback mechanism, simplify the user reporting process, provide convenient reporting channels, and encourage users to actively participate in the prevention and treatment of cybercrime. And the platform should give a timely response after the user report, and feedback the results to the reporter after processing, so as to enhance the user's sense of trust and participation. Finally, for Internet platforms that fail to fulfill their supervisory responsibilities, severe penalties are imposed according to the law, including fines, restrictions on business scope, and revocation of business licenses.

3.3 Promoting law enforcement synergies

With regard to "naked chat" extortion and blackmail crimes, improving public security investigation and coordination mechanisms is the key to enhancing the efficiency and success rate of the fight. With the technological upgrading of criminal groups and the expansion of criminal regions, it is crucial to establish cross-regional coordination mechanisms. Special working groups can be set up in public security organs at all levels to coordinate the handling of such cases, break down geographical restrictions, and build a nationwide information-sharing platform to realize rapid information exchange and collaborative operations. At the same time, it is necessary to enhance the technical investigation capabilities of public security, increase investment in technical equipment such as network monitoring equipment and

data analysis software, and adapt to the high-tech characteristics of cybercrime; regular training in cyberinvestigation techniques should be carried out to improve the professional skills of public security personnel, especially in cybercrime investigation and the extraction of electronic evidence. In addition, detailed contingency plans should be drawn up and the command system optimized to ensure rapid response and coordinated action(Xu,2024). In view of the fact that this type of crime involves foreign countries, it is also necessary to strengthen cooperation with international police organizations and the police of other countries, share intelligence resources and work together to combat transnational "naked chat"-type extortion and racketeering crimes.

4 Results

The crime of "naked chat" extortion is a product of the Internet, and the occurrence of this type of crime is not only related to the perpetrator, but also to the victim and the Internet monitoring platform. Although the public security organs continue to crack down on this type of crime, but the victim's weak sense of prevention, the Internet platform for more illegal information and other factors are also invisible to promote the occurrence of such cases. Therefore, the governance and prevention of "naked chat" extortion and blackmail cases is a long-term and arduous work that requires the joint efforts of citizens, Internet platforms and public security departments to improve the prevention of "naked chat" crime propaganda, Internet platforms to strengthen the supervision, and strengthen the coordination of public security departments. By improving the prevention of "naked chat" crime publicity, Internet platforms to strengthen the supervision, and strengthen the public security departments of the coordinated governance, I believe that the future "naked chat" type of extortion and blackmail crime governance can be effective.

About the Author

Lan Ding, Graduate student of law (non-legalstudies) at the Law School of Southwest Petroleum University, Criminal law.

References

- [1] Li J. J., & Wang M. S. (2021). Characteristics, root causes, and prevention of "naked chat" extortion crimes: An analysis based on 131 criminal cases. *Journal of Shanxi Police College*, (4), 69-76.
- [2] Cheng Y. Y. (2023). Research on "naked chat" related extortion crimes [Master's thesis, East China University of Political Science and Law]. CNKI Theses. <https://doi.org/10.27150/d.cnki.ghdzc.2023.000485>
- [3] Wang Y. H., & Dong J. (2023). Analysis and countermeasures of "naked chat" extortion crimes. *Network Security Technology and Application*, (1), 135-136.
- [4] Mou J. Y. (2023). Research on the identification of cyber extortion crimes [Master's thesis, Lanzhou University]. CNKI Theses. <https://doi.org/10.27204/d.cnki.glzhu.2023.000841>
- [5] Zhao T. S. (2023). Theoretical review and doctrinal interpretation of the criminalization of online "naked chat". *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)*, (5), 36-46.
- [6] Chen Z. J., & Yang Y. X. (2022). Judicial determination of downstream crimes in online "naked chat" extortion cases. *Chinese Prosecutors*, (6), 70-72.
- [7] Shen X. Z., Wang T., & Zhang S. R. (2023). Practice and reflections on handling cross-border "naked chat" extortion cases: A case study of the Hongmouduet al. extortion case. *Chinese Prosecutors*, (6), 12-15.
- [8] Wang L. (2023). Research on the investigation of cyber extortion crimes [Master's thesis, Zhongnan University of Economics and Law]. CNKI Theses. <https://doi.org/10.27660/d.cnki.gzczu.2023.003046>
- [9] Yang K. (2022). Research on psychological control and prevention strategies in "online naked chat" extortion crimes. *Network Security Technology and Application*, (12), 143-145.
- [10] Xu L. X. (2024). Crime script analysis and investigative countermeasures of online "naked chat" extortion crimes. *Network Security Technology and Application*, (3), 148-152.