ISSN: 2688-8653

The Difficulties and Approaches in Investigate Evidence of New Types Cybercrime

Ziyue Ding

School of Law, Anhui University of Finance and Economics, Bengbu 233000, China

Abstract

As one of the most prominent and controversial types of cases in current criminal justice practice, the new type of cybercrime faces both difficulties in investigation and evidence collection, as well as difficulties in judicial determination. The new type of cybercrime has become one of the mainstream crimes in China, and its characteristics of complex criminal subjects, diverse criminal methods, chained criminal patterns, and cross regional crimes make it difficult to meet the investigation requirements of new network crimes under new technologies relying on traditional criminal investigation methods. In the practice of investigation, there are practical difficulties such as difficulty in collecting evidence, difficulty in extracting electronic evidence, and the need to strengthen cross regional and cross departmental cooperation. The specific solution approach is to improve the investigation capability of public security departments for cybercrime, standardize electronic evidence collection for new types of cybercrime, and strengthen cooperation in investigating cross regional and cross-border new types of cybercrime.

Keywords

New type of cybercrime investigation, evidence collection, electronic evidence investigation.

1. Introduction

With the vigorous development of China's internet economy and online social networking, cybercrime has also emerged and presented a diversified development trend, with its number of cases and proportion in the total number of criminal cases continuing to rise. Cybercrime not only has the common feature of disrupting public order, but also exhibits unique attributes, such as the specificity of criminal methods and the non presence of perpetrators. Cybercrime is a crime committed against or using the internet, with up to 47 charges committed. Especially after the implementation of the Ninth Amendment to the Criminal Law in November 2015, with the addition of new charges in criminal legislation, the number of charges committed in cybercrime has significantly increased. According to the differences in criminal behavior or infringement of legal interests, cybercrime can be divided into two main categories: the first category is traditional crimes committed using online forms, which mainly target computer systems, data, and information, such as fraud (including telecommunications fraud) and destruction of computer information systems; The second type is the new type of cybercrime, which uses the internet as a tool or means to cause harm to society or infringe on the legitimate rights and interests of citizens, such as the crime of fabricating and intentionally disseminating false information, and the crime of illegally using information networks. "Although a considerable proportion of cyber crimes are pure cyber crimes such as crimes against the security of computer information systems, the more common situation is that traditional crimes are increasingly migrating to the Internet, and information technology is used to obtain new fields and tools." [1]In judicial identification, new cyber crimes have typical problems such as difficult investigation and evidence collection, difficult extraction of electronic evidence, large disputes over the nature of virtual property, and difficult determination of the illegality of

ISSN: 2688-8653

new cyber technologies. In order to effectively regulate new types of cybercrime, timely refinement of judicial interpretations, and expansion of theoretical and practical cooperation are necessary means to govern cybercrime, and are also necessary for the expansion of criminal law in the digital age[2].This article will conduct an in-depth analysis of the investigation difficulties of new types of cybercrime, and based on the analysis of problems and the summarization of experience, propose targeted response measures.

2. The Development Trend of New Types of Cybercrime

In the process of helping global economic, political and cultural exchanges and cooperation, and innovating human thinking patterns, living habits and codes of conduct, Internet technology has also become a tool for criminal forces and groups to implement illegal acts, posing a major challenge to the domestic regulatory system and international coordinated governance of cybercrime. At present, the governance system of cybercrime in China mainly covers two types of criminal forms: traditional and new. Observing the evolution trend of crime structure, the total number of serious violent crimes and criminal cases continues to decline, while the new type of cybercrime, represented by the crime of aiding information network criminal activities, has developed into the main form of crime. The inherent virtual characteristics, non-contact properties, and convenient access features of cyberspace have led to substantial changes in the modus operandi, behavioral subjects, and organizational forms of new types of cybercrime compared to traditional crimes. This poses multiple challenges to the coordinated prevention and comprehensive governance of criminal behavior.

2.1. Diversified criminal methods

Cybercrime has entered the stage of intelligence and precision, and the criminal subjects are accelerating their transformation towards technology intensive ones. Specifically, the criminal methods exhibit technological leaps, with traditional attack methods gradually being replaced by new technological means such as intelligent attacks based on deep learning algorithms and social engineering attacks relying on big data analysis; Secondly, the criminal technology ecosystem continues to evolve, and the commercialization process of cutting-edge technologies such as quantum computing and 5G communication provides new technological carriers for cybercrime, making criminal activities more covert and destructive; Thirdly, the iteration cycle of criminal technology has been significantly shortened, forming a "technology black industry" chain that enables criminal groups to quickly obtain the latest technological tools. The continuous expansion of this technological gap requires the establishment of a technical warning mechanism for cybercrime investigation and the continuous updating of investigation methods.

2.2. Complexity of criminal subjects

In the early stages of computer crime and traditional cybercrime, the main perpetrators were individuals who possessed professional network technology knowledge and skills. They usually committed crimes by illegally infiltrating computer information systems or disrupting network information system security. With the popularization of Internet technology and the addition of misdemeanor charges, the threshold for the implementation of new network crimes has gradually decreased, and the subject of crime has also expanded from the past professional and technical personnel to the general public[3]. Many individuals without professional technical backgrounds may unintentionally become participants in new types of cybercrime, and even become helpers in the criminal chain. This type of assistance behavior is usually arbitrary and non-specific. For example, in judicial practice, a large number of non professionals who rent, lend, or sell phone cards, bank cards, etc. at will may be suspected of providing payment and

ISSN: 2688-8653

settlement assistance for cybercrime and committing the crime of aiding information cybercrime activities.

2.3. Chainization of criminal patterns

The downstream of the industrial chain will monetize the obtained data through theft, fraud, and other forms. At the same time, the involved criminals or criminal organizations in the upstream, midstream, and downstream of the industrial chain have a single line of contact with each other, and most of them do not know each other. The perpetrators of upstream crimes and the main offenders of criminal organizations have strong anti investigation capabilities, making it difficult to trace and crack down on them, as well as to recover their assets and losses. For example, in the upstream of the industrial chain, criminals provide technical tools for stealing information from users' computers or directly controlling user devices. In the middle of the industry chain, criminals use data platforms to clean user accounts, passwords, and other information obtained, and then carry out property theft or directly resell user information for profit. In addition, the "zombie networks" controlled by them also play an important role in launching large-scale cyber attacks. At the same time, the perpetrators of upstream crimes and the main perpetrators of criminal organizations have strong anti investigation capabilities, making it difficult to trace and crack down on them. The difficulty of cracking down on and recovering stolen goods and losses is also high. The involved criminals or criminal organizations distributed in the industrial chain, middle and downstream, have single line connections with each other, and most of them do not know each other, which increases the difficulty and steps of investigation.

2.4. Cross regional crime

The new type of cybercrime presents significant cross regional characteristics, mainly reflected in the following aspects: firstly, the criminal subjects show a trend of cross regional and cross-border flow; secondly, the use of online resources has broken through geographical limitations; again, the implementation of criminal acts has cross regional and cross-border characteristics; Finally, the victims of crime are widely distributed and often involve multiple countries and regions. The complex characteristics of such crimes make it difficult for a single government department or sovereign state to independently conduct comprehensive investigations and effective crackdowns on such crimes, and there is an urgent need to establish a transnational and cross departmental collaborative governance mechanism. Although the international community has fully recognized the importance of collaborative prevention and control of new types of cybercrime, in practical operation, the differences in legal systems and differences in law enforcement and judicial practices among countries have led to uneven participation and insufficient coordination in international cooperation. The limitations of this international cooperation mechanism not only weaken the overall effectiveness of preventing and combating new types of cybercrime on a global scale, but also enable new types of cybercrime with transnational characteristics to continue to spread, posing serious challenges to national sovereignty and security, citizen rights protection, and cyberspace governance.

3. The Development Trend of New Types of Cybercrime

Compared to traditional criminal patterns, the implementation of new types of cybercrime exhibits significant non-contact characteristics. The criminal subject mainly relies on cyberspace for remote connection and criminal activities, which brings multiple challenges to case investigation: in the investigation process, the virtual identity of the criminal is difficult to track; in the process of collecting evidence, the collection, fixation, and identification of electronic evidence face technical bottlenecks; In terms of law enforcement cooperation, the mechanism for cross regional and cross departmental information sharing and collaborative

ISSN: 2688-8653

case handling is not yet perfect. These factors together constitute the main obstacles in combating new types of cybercrime.

3.1. Difficulty in investigating and collecting evidence of new types of cybercrime

With the rapid development of network technology, the forms of cybercrime are undergoing profound evolution. Against the backdrop of the continuous growth of traditional cybercrime and the upgrading of criminal methods, new types of cybercrime exhibit significant characteristics of increased intelligence, complex criminal methods, and diverse forms of crime[4].What is even more serious is that cybercrime has formed a complete industrial chain, and its degree of organization is increasing day by day. In this criminal ecosystem, upstream crimes focus on providing technical support, equipment supply, and platform construction, while downstream crimes use the technical tools provided by upstream to carry out diverse criminal activities, including but not limited to the dissemination of false information, infringement of citizens' personal information, online fraud, cyber attacks, extortion, etc., seriously endangering social order and public interests. Based on the differences in criminal intent, behavior patterns, and subjective purposes between upstream and downstream criminals, their criminal combinations exhibit a high degree of flexibility and can give rise to various specific charges. Compared with foreign countries, the industrialization characteristics of cybercrime in China are more prominent, manifested in a more specialized and refined division of labor, and a high number of criminal cases. Participants of different types of crimes, in pursuit of greater economic benefits, form highly organized and industrialized crime chains through online platforms, posing new challenges to cybersecurity governance.

The virtualization characteristics of cybercrime provide technical possibilities for tracking the source of the crime, which can lock criminal clues through information such as computer devices, IP addresses, and login accounts. However, due to the lack of deterministic correlation between network identity and real identity, as well as the common phenomena of account theft and false registration in practice, criminals are often able to commit crimes through identity forgery, impersonation, and other means, and quickly destroy electronic traces after succeeding. The concealment and anti investigative nature of this criminal method have enabled the harm of cybercrime to break through geographical boundaries, leading to increased difficulty in case investigation, rising costs of evidence collection, and a sustained increase in judicial resource investment.

3.2. Difficulty in extracting electronic evidence in new types of cybercrime

The integrity and accessibility of electronic evidence face multiple challenges. Firstly, the massive and dispersed nature of electronic data makes it highly susceptible to human destruction. Criminals often cause the loss or damage of key evidence through targeted attacks, data tampering, and storage media concealment, which not only increases the technical difficulty of evidence recovery and fixation, but also may cause the breakage of the evidence chain, seriously affecting the investigation of cases. Secondly, the internationalization trend of cybercrime has further intensified the complexity of electronic evidence collection. The reality of a large number of cross-border deployment of criminal servers has forced evidence collection work to face legal differences and cooperation barriers in different jurisdictions. The temporal and spatial scalability of this cyberspace significantly increases the cost investment of cross-border evidence collection, including multiple dimensions such as manpower allocation, technical support, and time consumption, thereby objectively increasing the difficulty of electronic data extraction. These factors collectively constitute the main obstacles to the collection and utilization of electronic evidence at present.

ISSN: 2688-8653

Although China has made significant progress in the institutional construction of electronic evidence collection for new types of cybercrime, and the Criminal Procedure Law of the People's Republic of China and relevant judicial interpretations of the "Two Highs and One Ministry" have systematically regulated the collection, fixation, and application of electronic data, the current legal framework still shows a certain lag with the rapid iteration of network technology and the continuous upgrading of criminal methods. Specifically, in the face of increasingly complex forms of cybercrime and constantly evolving technological means, there is still room for improvement in the existing legal provisions in terms of evidence collection procedures, evidence validity determination, and cross-border evidence collection cooperation. It is urgent to optimize them through legislative revisions and judicial interpretations to meet the practical needs of combating new types of cybercrime. Although China's current legal system has made fundamental provisions for electronic evidence collection procedures for new types of cybercrime, there are still significant challenges in practice. Due to the inherent lag characteristics of the law and the rapid iteration of cybercrime methods, investigators often encounter many difficulties in handling such cases. Especially for criminals, their modus operandi often goes beyond conventional knowledge, which puts higher demands on law enforcement personnel who are new to such cases. The existing evidence collection procedures still have ambiguous areas in specific operational aspects, making it difficult to fully adapt to the complex and ever-changing realities of case handling. Therefore, it is urgent to gradually fill the legal gap and build a more comprehensive electronic evidence collection program standard system by summarizing practical experience, improving implementation rules, and other methods[5]. In recent years, new types of cybercrime have shown an explosive growth trend, characterized by rapid evolution of criminal forms, increasingly complex organizational structures, diverse and technologically advanced modus operandi, and increasing social harm. These characteristics directly lead to unprecedented challenges in case investigation work: on the one hand, investigators need to handle massive amounts of electronic data, and the workload is increasing exponentially; On the other hand, the investigation of cases has raised higher requirements for law enforcement teams, requiring both sufficient professional personnel and interdisciplinary knowledge reserves - not only proficient in electronic evidence collection technology, but also familiar with relevant laws and regulations. Under this dual pressure, it is inevitable that there will be problems such as non-standard operation or procedural flaws in the electronic evidence collection process, which highlights that the current evidence collection mechanism still needs further improvement. In the practice of electronic evidence collection for new types of cybercrime, investigative agencies generally use various technological means to carry out investigation work, including real-time monitoring of electronic data, tracking of network account trajectories, precise positioning based on the Beidou system, and advanced technologies such as remote digital evidence collection. These technological means have significantly improved the efficiency of public security organs in intelligence gathering, criminal fact determination, and case investigation, providing strong support for combating cybercrime. However, while these evidence collection measures enhance investigation efficiency, they may also pose potential threats to basic rights such as citizens' privacy and personal information rights, so some evidence collection measures are not allowed by law.

3.3. Cross regional and cross departmental collaboration needs to be strengthened in the investigation of new types of cybercrime

The downstream of the industrial chain will monetize the obtained data through theft, fraud, and other forms. At the same time, the involved criminals or criminal organizations in the upstream, midstream, and downstream of the industrial chain have a single line of contact with each other, and most of them do not know each other. The perpetrators of upstream crimes

ISSN: 2688-8653

and the main offenders of criminal organizations have strong anti investigation capabilities, making it difficult to trace and crack down on them, as well as to recover their assets and losses. For example, in the upstream of the industrial chain, criminals provide technical tools for stealing information from users' computers or directly controlling user devices. In the middle of the industry chain, criminals use data platforms to clean user accounts, passwords, and other information obtained, and then carry out property theft or directly resell user information for profit. In addition, the "zombie networks" controlled by them also play an important role in launching large-scale cyber attacks. At the same time, the perpetrators of upstream crimes and the main perpetrators of criminal organizations have strong anti investigation capabilities, making it difficult to trace and crack down on them. The difficulty of cracking down on and recovering stolen goods and losses is also high. The involved criminals or criminal organizations distributed in the industrial chain, middle and downstream, have single line connections with each other, and most of them do not know each other, which increases the difficulty and steps of investigation.

Due to its cross regional nature, cybercrime has been granted extensive jurisdiction by law, and the place of commission, outcome, and destination of the criminal act can all serve as connection points for criminal jurisdiction. However, there are still problems such as dispersed jurisdiction and imperfect cooperation mechanisms in the investigation of cross regional cybercrime cases, which have led to many challenges for public security organs in their investigative work. The virtual, real-time, and uncertain nature of cybercrime poses greater challenges to investigation and evidence collection. Criminals may be scattered around the world, using anonymous technology to hide their identities and breaking through geographical limitations to commit crimes. At the same time, there is often a temporal and spatial separation between criminal behavior and harmful consequences, which makes it more difficult to discover criminal clues, advance investigation work, collect evidence, and determine crimes[6].

The virtualization characteristics, real-time performance, and uncertainty of the targets of cybercrime have brought unprecedented challenges to the investigation and evidence collection work. Criminals may be spread all over the world, using anonymous technology to conceal their true identities and easily breaking through geographical boundaries to carry out criminal activities. At the same time, there is often a phenomenon of temporal and spatial separation between criminal behavior and harmful consequences, which further exacerbates the difficulty of discovering criminal clues, making the development of investigation work, the construction of evidence chains, and the determination of criminal facts face greater obstacles. For cases involving cross-border crimes, when domestic law enforcement agencies discover that key evidence is located overseas, they usually need to coordinate four levels: domestic law enforcement agencies, domestic competent authorities, overseas competent authorities, and overseas law enforcement agencies, and complete a series of cumbersome evidence collection procedures to obtain evidence. This process often takes months or even years. Scholars generally believe that the traditional criminal judicial assistance system is inefficient, with procedures that are "complex, lengthy, slow to progress, and severely bureaucratic"[7].

In cross-border cyber crime, suspect often choose to commit crimes abroad in order to avoid domestic legal sanctions, evade judicial investigation and seek shelter for criminal activities. This behavior inevitably leads to conflicts of criminal jurisdiction between countries. Currently, with the increasingly prominent value of data, many countries have regarded "data" as an important component of national sovereignty, and some countries even position it as a strategic resource for future national development. The Tallinn Handbook of International Law on Cyber Warfare, published by NATO, elaborates on cyber security as a "sovereignty" issue, which to some extent reveals the "cyber warfare" intentions of the United States and some Western countries. Due to the potential impact of cross-border electronic evidence collection systems on the sovereignty of other countries, countries often exhibit a cautious attitude towards

ISSN: 2688-8653

collaborative governance of cybercrime. According to traditional criminal justice theory, the criminal jurisdiction system is divided into four types: territorial jurisdiction, personal jurisdiction, protective jurisdiction, and universal jurisdiction. Among them, territorial jurisdiction is judged based on whether the place of the criminal act is located within the territory of the country. However, the location of cybercrime usually involves multiple countries, which not only makes the determination of the location of the crime complex, but may also lead to conflicts or vacuum of jurisdiction, and even different treatments for the same behavior due to differences in legal standards in different regions. This situation not only increases the difficulty of combating transnational cybercrime, but also to some extent contributes to the rampant trend of cross-border cybercrime [10].

4. The Solution to The Dilemma of Investigating New Types of Cybercrime

Based on the investigation dilemma of new types of cybercrime, typical problems in the investigation of new types of cybercrime can be solved from the following aspects:

4.1. Enhance the investigative capability of public security departments towards cybercrime

Integrating modern technologies such as big data and cloud computing into the daily work of public security organs is an important direction for improving policing efficiency. The "integration" mentioned here is not limited to the field of criminal investigation, but covers various public security work closely related to the safety and interests of the people, such as investigation, public security, registered residence, etc. There is an organic connection between these jobs, which mutually influences and supports each other. Currently, although big data investigation has become a trend, its effectiveness is often limited if it is only limited to the field of criminal investigation. In fact, investigation work is closely related to public security management, registered residence management, position control and other work. Only by applying big data technology to all aspects of public security work, can the overall efficiency of investigation work be comprehensively improved. In the long run, this comprehensive application not only helps improve the quality of investigation work, but also promotes the overall level of public security work. Due to the close connection between investigation work and other work of public security organs, the widespread application of big data technology in various aspects of public security work will undoubtedly lay a solid foundation for further improving the quality of cybercrime investigation work.

Establish and deploy mechanisms for investigating and preventing cybercrime. Cybercrime is essentially a non-contact type of crime, which can only be investigated after the incident. On the one hand, the investigation is difficult and requires a large amount of police resources, and on the other hand, it is difficult to curb the arrogance of criminals. So we should shift from passive investigation from case to person to active investigation from person to case. The use of big data prediction technology to predict the criminal behavior, activity time, and activity patterns of cybercriminals in advance, and nip the crime in the bud, not only helps to protect citizens' property safety, but also has a strong deterrent effect on first-time offenders of cybercrime. By utilizing big data mining techniques, typical cybercrime cases can be analyzed to summarize the patterns of different types of cybercrime cases, which can provide experience for future investigation work and avoid detours.

4.2. Standardize electronic evidence collection for new types of cybercrime

At present, China lacks specialized legislation for electronic data, and there are fewer procedures for electronic evidence collection of new types of cybercrime. There is also a lack of independent and unified rules and procedures for electronic evidence collection, and a lack of institutionalized laws and regulations. The standardization of electronic evidence collection

ISSN: 2688-8653

for new types of cybercrime should be approached from two perspectives: first, to address the issue of legislative integrity, and second, to address the issue of legislative lag. In terms of the integrity of legislation, it is necessary for China to formulate a new law related to electronic evidence collection for cybercrime at an appropriate time, and to clearly define the principles, procedures, subjects, methods, and other related issues of electronic evidence collection for cybercrime. Only in this way can forensic personnel have clear, detailed, and strict legal basis when obtaining electronic data, and the probability of illegal evidence collection will be greatly reduced. The detection rate and efficiency of cases will also be improved, and a lot of manpower and material resources will be saved. As for the issue of legislative lag, it is necessary for the legislative body to carefully explore the specific situation and draw conclusions, and ultimately publish them in the form of legislation to facilitate clearer, faster, and more efficient identification of charges in practice.

In the investigation of new types of cybercrime cases in our country, electronic data can play an important and crucial role, which will directly affect the development trend of the entire case. The correctness of the evidence collection procedures often affects the legality and value of electronic data. In that case, the new electronic evidence collection procedures for cybercrime must be comprehensive, meticulous, and standardized in order to provide forensic personnel with a clear legal standard for conducting evidence collection activities. Firstly, the operational norms of electronic forensics procedures need to be clarified. China should clearly stipulate that operators such as WeChat platforms have the responsibility to cooperate with case investigations, so as to solve the problem of the integrity of electronic data being damaged due to malicious evasion of investigation by the parties involved during search and seizure, but the investigating authorities do not have great power to ask operators to cooperate with the investigation. Secondly, remedial measures should be taken for data obtained through illegal means. The adoption of electronic data related to criminal cases in our country follows the exclusionary rule of illegal evidence. If electronic data is obtained through illegal means in handling new types of cybercrime cases, it cannot be used in determining the facts of the case. Even if this electronic data is crucial, it cannot be used as data to influence the conviction and sentencing of the case. The legal provisions in our country do not allow illegal means such as electronic monitoring and tracking to obtain electronic data, but the authenticity of these defective data is very high. Therefore, corrective and remedial measures should be taken for their defects. However, reasonable remedial measures should be set up for defective data to prevent the widespread use of remedial measures. Finally, improving the legal knowledge and literacy of electronic forensics personnel for new types of cybercrime is also one of the ways to avoid using illegal means to obtain electronic data.

In electronic data collection, various technologies such as data interception, data replication, data repair, and data scanning are usually used[11].Learning and applying the above search and collection technology is of great guiding value for combating new Internet crimes. Therefore, it is necessary to increase the training of professional technical talents in electronic forensics in China, further enhance the cooperation between network forensics institutions and personnel, and greatly reduce the development, maintenance, and upgrade costs of network forensics tools, so as to effectively respond to the complex new types of cybercrime. In our country, it is necessary to establish and improve a specialized training mechanism, establish a specialized training institution, hire a group of high-quality technical talents to train our country's characteristic electronic evidence related technical talents, and set up a regular assessment mechanism. At the same time, legal issues need to be evaluated, and only qualified technical personnel can enter actual cases to obtain electronic data. Only with a qualified and powerful team of new electronic evidence collection technology for cybercrime can we better crack down on the endless stream of new cybercrime cases and effectively crack down on and punish criminals.

ISSN: 2688-8653

4.3. Strengthen cooperation in investigating new types of cybercrime across regions and borders

The new types of cybercrime are diverse, evolving rapidly, and have a wide scope. Establishing a regional law enforcement organization coordination system, intelligence information sharing system, and other systems is a practical problem that must be solved in the process of regional law enforcement cooperation. Investigation agencies in different regions need to develop investigation strategies, adopt investigation measures, unite multiple forces, and establish investigation cooperation mechanisms based on the case. In the context of the continuous enrichment of new types of cybercrime investigation subjects and relatively complex investigation processes, division of labor and connection have become the two core elements of investigation cooperation mechanisms, which to some extent determine the effectiveness of investigation cooperation. From the perspective of division of labor and connection, comprehensively considering factors such as intelligence strategy, crime patterns, evidence standards, and investigation efficiency, improving relevant investigation cooperation mechanisms is an effective way to enhance the quality and efficiency of combating new types of cybercrime.

Firstly, based on the concept of intelligence sharing, it is necessary to improve the collaboration process and connection procedures. In the context of the new type of cybercrime breaking geographical limitations, only by fundamentally eliminating the shackles of intelligence sharing in investigation cooperation and smoothing the information flow channels of all parties involved can we achieve a comprehensive crackdown on new types of cybercrime. To achieve this, firstly, it is necessary to use information technology to break down the barriers of criminal investigation departments in various regions in the sharing of new network crime information, and realize the synchronous input and real-time sharing of criminal information. Secondly, it is necessary to use information technology to improve the investigation collaboration process, achieving online input, online application, online handling, and online response, so that the collaboration process can be traced and standardized on the work platform. Thirdly, in the context of differences in information technology investigation and case handling capabilities in various regions, a parallel case handling linkage procedure of "paper documents+electronic documents" can be adopted to recognize the authority of electronic documents, gradually realize the electronic transmission of collaborative documents, and reduce cumbersome and complex case handling processes.

Secondly, based on the laws of criminal behavior, the jurisdiction and division of responsibilities of the case should be determined. The implementation process of new types of cybercrime has the characteristic of technological dependence, which requires the use of information networks and related technological equipment in the preparation, implementation, collection of criminal proceeds, and processing of criminal traces. With the assistance of relevant black and gray industries, the new channels for disseminating information on cybercrime have broken through geographical boundaries and changed people's traditional way of defining the crime scene. Therefore, based on the characteristics of criminal behavior patterns, using jurisdictional levels, work convenience, information advantages, etc. as the basis, scientifically delineating the jurisdiction scope between investigation cooperation departments[12],determining a relatively complete system of division of responsibilities, promoting the construction of police cooperation mechanisms and "point-to-point" cooperation in demand intensive areas will be conducive to improving the effectiveness of investigation cooperation and enhancing the quality of case handling.

Finally, based on the requirements of evidence standards, standardize the collection of evidence and document circulation in different locations. The new types of evidence in cybercrime, represented by telecommunications fraud crimes, are diverse and require high

ISSN: 2688-8653

technical requirements for the extraction of relevant evidence. Investigation agencies often face many difficulties in obtaining evidence, determining the guilt of suspects, and verifying related crimes. At the same time, in the context of comprehensively promoting the "trial centered" litigation system reform, the evidence obtained from investigative activities needs to meet the relevant requirements of the evidence standards in the trial stage, which puts high demands on the collection of evidence and the circulation of evidence documents in investigative cooperation. Therefore, all parties involved in investigation cooperation need to examine evidence collection cooperation from the perspective of investigation rule of law, unify evidence collection standards, standardize evidence collection processes, reduce differentiated evidence collection behaviors among different investigation departments, and properly handle the difficulties faced by evidence collection cooperation in new types of cybercrime work. Specifically, one is to scientifically carry out cross regional evidence collection work. The second is to standardize the circulation of evidence documents.

5. Conclusion

At present, the basic situation of crime in China is still in a high incidence and transformation period, and various new types of cybercrime represented by telecommunications fraud are still operating at a high level. The means and methods of cybercrime will continue to innovate with the upgrading of information technology, and new forms of crime will continue to emerge. The challenges faced by investigative agencies are also increasing. However, the continuous updating of big data also provides new ideas for the investigation of cybercrime. Although cybercrime investigation currently faces many difficulties in the perspective of big data, from a dialectical perspective, with the application of big data technology, the continuous accumulation of cybercrime investigation experience, and the improvement of communication technology for investigators, the efficiency and quality of cybercrime investigation will continue to improve.

References

[1] Haisong Yu:Fragmentation of Cybercrime Forms and Systematization of Criminal Governance, Legal Science (Journal of Northwest University of Political Science and Law), Vol.40 (2022) No.03.58-70.

[2] Haisong Yu:The legislative expansion and judicial application of cybercrime, Application of Law, (2016)No.09.2-10.

[3] Yongfu Qi, Ruixuan Cao:Thoughts on the construction of a diversified prevention and control system for new cybercrime,Journal of Shanghai Public Security University, Vol.32(2022)No.06.25-33.

[4] Hongyan Hua:Exploring the difficulties and countermeasures of public security organs in cracking down on new types of telecommunications network fraud crimes,Public Relations World, (2020)No.20.170-172.

[5] Jiahua Zhang:The dilemma and approach of punishing new types of cybercrime in the era of big data,Learning and Practice, (2022)No.05.85-95.

[6] Xuan Zhang,Jiguo Jiang:Construction of Network Investigation Mechanism under the New Situation，China Security Prevention Technology and Application, (2018)No. 4.54-60.

[7] Wei Pei:The key to future crime governance: Cross border data forensics, China Information Security, (2019) No.5.35-37.

[8] Xiaomin Wu,Shuo Jia:Collection of Electronic Evidence in Cross border Cybercrime Investigation, Journal of Guangxi Police College, Vol35 (2022)No.02. 46-52.

[9] Zhichao Bai:Research on the Standardization of Electronic Evidence Collection for New Cybercrimes in China(MS.,Gansu University of Political Science and Law, China 2021).

ISSN: 2688-8653

[10] Shuai Qin: The current situation and approach of new collaborative mechanisms for cybercrime investigation, Journal of Beijing Police College, (2022)No.06.95-101.

[11] Weijun Liu:Regional police cooperation in the context of the new mechanism to combat crime, Journal of the People's Public Security University of China: Social Sciences Edition, (2015)No.6.65-70.

[12] Yingying Wang: Analysis of Governance Strategies for Cross border Cybercrime, Journal of Heilongjiang Provincial Political and Legal Management Cadre College,(2016)No.3.34-37.