Research Article
Volume 15:02, 2024

Journal of Forensic Research

ISSN: 2157-7145 Open Access

Study on the Evidence Collection of Public-related Cybercrime in China

Zhanfeng Hu*

School of Law, China University of Political Science and Law, 25 Xitucheng Road, Haidian District, Beijing, China

Abstract

Public-related cybercrime is a new type of crime that relies on science and technology, and has the characteristics of public-interested, cross-regional, and virtuality compared with traditional crimes. Punishment by the law is inseparable from evidence, and public-related cybercrime mainly occurs in the virtual space, which makes it significantly more challenging to investigate and collect evidence. Gathering evidence for public-related cybercrime, many problems have emerged, mainly including the lack of professionalism of the forensic subject, the non-standard forensic procedures, and the impact on the evidentiary ability and probative power of digital evidence. At present, these problems have seriously hindered the comprehensive, objective, and timely collection of evidence by the judicial authorities to crack down on public-related cybercrime. The primary evidence for determining the public-related cybercrime is digital evidence, so the discussion of the evidence collection and issues of the public-related cybercrime revolves around digital evidence. In response to problems in the process of evidence collection for public-related cybercrime, it shall be based on the characteristics of the cybercrime itself, the evidence collection system, and combined with the characteristics of digital evidence, such as the volatility, virtuality, and easy and accurate reproducibility of digital evidence, to find targeted and effective countermeasures. The targeted measures mainly include that increasing the professionalism of the forensic subject, promoting the censorship of forensic procedures, clarifying the legal principles of collecting evidence in cybercrimes, improving the mechanisms for the assessment and preservation of evidence and improving the application of relevant rules on primary evidence.

Keywords: Public-interested • Cybercrime • Digital evidence • Forensic system

Introduction

Cybercrime has social severe harm, because it has the characteristics of low crime cost and high concealment, which makes cybercrime different from traditional crime [1]. Nowadays, cybercrime is increasing, especially involving people. Public-related cybercrime has the characteristics of public interest, cross-domain, large amount of funds involved, difficulty in recovering stolen goods, and difficulty in maintaining social stability. Evidence is the basis for the correct application of the law [2], and digital evidence is the primary evidence for the determination of this type of public-related cybercrime. Still, because digital evidence itself has the characteristics of easy and accurate reproducibility, virtuality, and changeability, it is difficult to ensure the originality and integrity of digital evidence, which in turn affects the critical role of digital evidence in the proof system of public-related cybercrime. According to the general evidence theory and judicial practice, to ensure the originality and integrity of digital evidence, it is necessary to strictly regulate the procedures for extracting and preserving digital evidence from the source [3]. In the process of cracking down on public-related cybercrime, the issue of evidence collection has always plagued judicial case handlers. For example, the lack of professionalism of evidence collection, the non-standard evidence collection procedures, and the evidentiary capacity and probative power of digital evidence are impacted. This article intends to provide solutions to the above problems.

***Address for Correspondence:** Zhanfeng Hu, School of Law, China University of Political Science and Law, 25 Xitucheng Road, Haidian District, Beijing, China, E-mail: huzhanfeng01@163.com*

Received: 01 April, 2024, Manuscript No. jfr-24-132003; **Editor Assigned:** 03 April, 2024, PreQC No. P-132003; **Reviewed:** 16 April, 2024, QC No. Q-132003; **Revised:** 23 April, 2024, Manuscript No. R-132003; **Published:** 30 April, 2024, DOI: 10.37421/2157-7145.2024.15.607

The concept of public-related cybercrime

The literal meaning of "public-related" is usually understood as the number of people involved, as opposed to the individual and the separate. In the context of cybercrime, "public-related" have multiple meanings. From the perspective of the subject of the crime, "public-related" can refer to the number of people involved in the subject of the crime more than one. From the standpoint of the victim, "public-related" can refer to the number of victims involved in more than one. From the standpoint of the criminal process, "public-related" can refer to one or more crimes involving multiple victims, to numerous people committing one or more crimes against the same victim, or numerous people committing one or more crimes against multiple victims. There are various perspectives on the understanding of "public-related", but in the final analysis, it is inseparable from the essential characteristic of "many".

There is currently no authoritative legal definition of the term "cybercrime" [4]. The main viewpoints of the academic community have not clarified the characteristics of the network in cybercrime, nor have they explained the degree of cyber involvement in the crime, nor have they separated the distinctions between the cybercrime and the traditional crime. In other words, China's current theoretical discussion cannot provide accurate opinions on whether an act is a cybercrime. From the perspective of China's current legislation, the 2014 *"Opinions of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases"* (after this referred to as *"the Opinions"*) pointed out the scope of cybercrime cases, but still did not clarify the legal concept of cybercrime. From the issued regulations in China, cybercrime is not regarded as a criminal law concept, but as an intuitive description of the type of crime. Whether the concept of cybercrime is clear or not does not have a substantial impact on the judgment of the crime. To understand the concept of cybercrime, it is possible to analyze the difference between the behavior after the intervention of cyber factors and the traditional behavior, to grasp the essence of cybercrime.

In the *Opinions*, the concept of public-related cybercrime is not explicitly expressed, but the characteristics of public-related cybercrime are vaguely

pointed out. According to the *Opinions*, we can further deduce that the concept of public-related cybercrime refers to the crime of the perpetrator publishing information on the Internet or setting up websites or communication groups mainly used to carry out criminal activities, targeting or organizing, instigating, or aiding an unspecified number of people. However, in a strict sense, "public-related cybercrime" is not a legal concept in itself, but a type of crime concept proposed after a general analysis and induction based on the form of the perpetrator's crime [5].

There are three main methods of evidence collection in China for public-related cybercrime: cross-regional forensics, digital evidence forensics, and technical investigation and forensics. Essential data such as websites, account information, and other important data related to public-related cybercrimes are often distributed in different regions, and according to China's traditional evidence collection procedures, it is usually necessary for the case-handling area to send the police to carry out the collection of relevant legal documents to the location of the evidence. However, the workload of cybercrime forensics is enormous, and it is difficult to effectively extract relevant evidence when the resource of forensic personnel is not enough [6]. Judging from the current status of China's technical investigation and evidence collection legislation, the application conditions, scope of application, and approval subjects of China's technical investigation measures are not clear enough. There are still many aspects that need to be improved to meet the current demand of technical investigation and evidence collection of public-related cybercrime.

Problems in the forensics of public-related cybercrimes

The professionalism of the forensic entity is insufficient: At present, China's cybercrime investigation lacks the participation of investigators with specialized skills, and most of the force are front-line criminal police to participate in cybercrime investigation activities, and these criminal police often rely on the experience of traditional crime investigation during the detection, and lack of new cybercrime investigation concepts as guidance. The collection of evidence of public-related cybercrime is different from the collection of ordinary evidence [7]. The virtualization and digitization of cyberspace and the variability of digital evidence are significant in number, making it difficult for ordinary forensics personnel to extract adequate evidence, so it is necessary for staff with specialized skills to guide and operate. However, in the system of China's investigative authorities, most of the personnel who have mastered computer information technology are specialized technical personnel within the departments, and the technical personnel usually do not directly participate in the search and evidence collection, resulting in a lack of specific practical experience in investigation and it isn't easy to directly guide the actual work of collecting evidence from digital evidence. Since cybercrime takes place in a "dual space", i.e., virtual space and real space, this means that not only do investigators need to have sufficient experience in handling cases offline, but they also need to master specific professional skills related to computers and networks [8]. However, at present, there is a severe shortage of such compound talents in the public security authorities, which cannot meet the actual needs, which directly increases the risk of flaws in the form, source, and content of evidence in public-related cybercrime. Currently, China's digital evidence forensics equipment is in a state of shortage as a whole. In addition, many areas in China have not yet set up specialized appraisal institutions for digital evidence, resulting in the inability to judge the authenticity of the extracted digital evidence promptly, and ultimately resulting in a significantly reduced efficiency in the collection of evidence in public-related cybercrime.

Procedures for collecting evidence are not standardized: Digital evidence is the primary evidence of public-related cybercrime. In China's existing legal norms for digital evidence forensics, problems such as the lenient limitation of self-discretion and self-supervision by investigative organs, and insufficient third-party supervision and approval have become increasingly prominent [9]. The regulations for the extraction of digital evidence are mainly concentrated in the *"Notice of the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security on Issuing the Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases"* (after this referred to as *"the Digital evidence Provisions"*). The Article 9 requires that the investigating authorities shall comply with the corresponding approval procedures in the process of using technical investigative measures. However, this provision is too general, and the subject and procedure for examination and approval of technical investigation measures are not yet explicit. The lack of clarity in the provisions can easily lead investigators to understand the content and scope of the approval procedures without authorization in practice, which also leads to less electronic evidence extraction in practice for approval and supervision by the regulations.

In addition, China has not yet set up an external review and supervision procedure for the collection of digital evidence, but has only set up an internal approval procedure for the extraction of digital evidence. For example, when searching the suspect's cellular data information, the U.S. Supreme Court requires the police to be authorized a warrant in case of a digital evidence collection. This kind of internal digital evidence extraction review procedure does not require an explanation of the reasons for the digital evidence search, which makes it difficult to guarantee the inquiry of the digital evidence collection become legal and reasonable. At the same time, in the absence of supervision by external organs, investigators and forensics often do not distinguish between ordinary and sensitive digital evidence, and directly search and extract all of them. According to the principle of proportionality, a review and approval procedure should be established with differential treatment and moderate leniency and severity [10]. Still, China has not yet established a similar review procedure. Comparing China's legislative experience and judicial practice with foreign countries, the necessity of adopting technical investigation measures in China is still not clear enough in the legislation, and the scope of application and conditions for the application of technical investigation is too general, and there is a lack of further detailed provisions and explanations. In the process of examination and approval of technical investigations, the investigating organs often ignore the details of whether the targets of the technical investigation measures are determined, as well as the time, space, and scope of the technical investigation measures, which often leads to the failure of the technical investigation methods adopted by the investigating organs in the process of extracting digital evidence, and is even not conducive to the realization of the goals pursued by the technical investigation, resulting in a waste of judicial resources.

The evidentiary capacity and probative power of digital evidence have been impacted: In judicial practice, the prosecution and defense often dispute whether digital evidence is forged or altered because of its volatile and fragile characteristics. Explaining the authenticity of digital evidence requires: first, a description of the source of the digital evidence and its storage medium; second, the integrity of the digital evidence is described [11]. In addition to the irregularities in the operation of investigators, the gaps in the relevant legal documents and the lack of specific operating procedures also seriously threaten the integrity of digital evidence. In addition, the adjudication organ also needs to determine whether the critical evidence has been extracted and whether the unique record of the critical evidence carrier is missing. The Digital evidence Provisions do not distinguish between authenticity and completeness review methods. If the two are not distinguished legislatively, it is easy to lead to confusion in the application of judicial personnel in judicial practice.

Based on perspectives such as whether the content reflected in the digital evidence is related to the facts of the case, and whether the digital evidence is generated from the process of the case, it is to be judged whether the digital evidence can play a role in proving the main facts of the public-related cybercrime. When digital evidence is used in a verdict, it must meet the dual relevance of the content of the evidence and the material carrier. However, relevance, as the primary criterion for judging the evidentiary capacity and probative power of digital evidence, has not received due attention for a long time [12]. Digital evidence is digital scientific and technological evidence in the form of numeric letters, symbols, which also leads to the fact that the judgment of its relevance is not as easy to grasp as traditional evidence as documentary and physical evidence. During the prosecution of public-related cybercrime, whether digital evidence can be accepted must first determine whether it is relevant to the case, and the following issues must be resolved: first, what can be proved by digital evidence; second, whether the facts proved by digital

evidence help resolve case disputes, and third, whether relevant laws and regulations have specific requirements for the relevance of digital evidence.

The legitimacy of digital evidence mainly needs to meet three aspects: the legality of the form of evidence collection, the suitability of the subject of evidence collection, and the proper procedures for evidence collection. Judging from China's current provisions on excluding illegal evidence, the legislator has not stipulated the circumstances of the unlawful exclusion of digital evidence, nor has it set up a sanction mechanism for the unlawful acquisition of digital evidence [13]. Strictly speaking, there is no clear legal norm in China to supervise and exclude the extraction of digital evidence. The legality of digital evidence is often questioned by the defense. Legislators maintain a conservative attitude towards the rule of illegal exclusion of digital evidence, which will also lead to judges evading the application of the rule of exclusion of unlawful evidence of digital evidence in public-related cybercrime. In current judicial practice, digital evidence that does not meet the requirements is usually used as evidence using supplementation and reasonable explanation; that is, judicial practice understands digital evidence as a type of evidence that can be supplemented. However, the rule that all illegally obtained digital evidence can be corrected is problematic. Judging from the current legislative status of our country, the procedures and methods for supplementing illegally obtained digital evidence are not precise. That is to say, there is no corresponding supporting solution system for correcting digital evidence defects. If digital evidence that should be excluded can be made lawful again using supplementation or reasonable explanation, then it may cause investigators and evidence collectors to not pay attention to the procedural and normative nature of their behavior in the process of collecting evidence, and even adopt excessive and transgressive methods to facilitate the extraction of digital evidence.

Improve paths for collecting evidence for public-related cybercrime

Increase the professionalism of the subject of evidence collection: Due to the characteristics of public-related cybercrimes, the collection of evidence cannot be entirely and directly applied to the traditional evidence collection methods [14]. Public-related cybercrime needs to be guided by a new forensic concept different from conventional forensics. Updating the concept of forensics and establishing a new type of concept of forensics for public-related cybercrime can start from the following two aspects: first, constantly update the professional knowledge of forensics, grasp the frontier of forensics technology for cybercrimes, and establish the concept of forensics for cybercrimes that keeps pace with the times; second, strengthen exchanges and training on forensics in cybercrime investigation and forensics, and summarize the experience of different regions and types of cybercrime investigation and forensics.

To build a professional forensics team and cultivate compound forensics talents, we can start from the following aspects: first, establish a forensic professional skills evaluation mechanism, and strictly enforce the access conditions for forensics personnel; second, establish a regular training and exchange mechanism for forensics to ensure the sustainable development of forensic skills; third, establish a reward and incentive mechanism to motivate forensic personnel to improve their forensic ability continuously.

Because digital evidence is accessible to tamper with and easy to copy accurately, investigators and forensics personnel shall employ professional forensic equipment in the process of extracting and fixing evidence to ensure the originality and integrity of digital evidence. In intermediate links such as inspections and appraisals, judicial organs shall also employ professional data replication and backup equipment, and specific staff should correctly copy and back up digital evidence files for subsequent inspections and appraisals. In the process of updating digital evidence forensics and backup equipment, on the one hand, it is necessary for the investigative organs to increase the intensity of capital investment and improve the advanced nature of the digital evidence forensics and backup equipment; on the other hand, it is also necessary to strengthen the combination of "production, education, and research" and promote the joint research and development of the investigative organs, institutions, and scientific research institutes to independently develop and improve forensic backup equipment.

Improve the system for the examination and approval of evidence collection: Investigation and evidence collection in physical space is mainly carried out through on-site investigation, investigation and questioning, etc., and the entire evidence collection process could be visible. It can be regulated through means such as setting up procedures and strengthening supervision. Improving systems for the approval and oversight of digital evidence forensics shall be based on the virtuality of cybercrime space, and investigation and evidence collection activities shall follow the fundamental laws of virtual cyberspace, and understand its basic technical principles and operational models. In the process of improving the system for the approval and supervision of digital evidence forensics, professional and technical personnel shall be ensured to participate in internal audits, and specifically, professional and technical personnel shall first conduct a review and assessment from the technical level, and then submit them to the examination and approval personnel for review and evaluation from the legal level after forming relevant recommendations. To a certain extent, the practical difficulties of those who understand the law do not necessarily understand the technology, and those who understand the technology do not necessarily understand the law, and the examination and approval supervision of digital evidence forensics is prevented from becoming a mere formality.

Based on the current mode of criminal procedure in China and the judicial status quo of a few court cases, it is not feasible to determine that the court will review and supervise the application for digital evidence collection and technical investigation. In the process of improving the system for the examination approval and supervision of digital evidence collection and technical investigations, it may be suggested that the procuratorate is responsible for review and supervision. Specifically, it may be clarified that the investigation organs and the procuratorate jointly examine and approve the collection of digital evidence, while the procuratorate independently examine and approve technical investigations. In the process of improving the system of examination and approval and supervision of evidence collection, the regulation of technical investigation should be strengthened, and in the current methods of investigation and evidence collection, technical investigation is the most hidden. It is more likely to cause abuse and misuse of investigative power in the absence of effective restraint and supervision based on the easy expansion of power.

Clarify the legal principles for the collection of evidence in cybercrimes: The principle of collecting evidence by law requires that the subject of evidence collection, the procedures for gathering evidence, and the fixation of evidence for public-related cybercrime all comply with legal norms. Regarding the subject of evidence collection, it shall be ensured that the person collecting evidence has the certificates to be the entity and has a certain amount of investigative experience and professional skills. In terms of evidence collection procedures, the first is to comply with the statutory methods and means of evidence collection, the second is to comply with the statutory authority, and the third is to adhere to the approval and supervision procedures, and ensure that all aspects of evidence collection are effectively connected. Regarding fixation of evidence, legally-prescribed storage media and display forms shall be taken, and confidentiality measures shall be used to prevent contamination of evidence in production, storage, and other links.

The principle of timely evidence collection requires that the investigating organ should extract and fix evidence in a timely and expeditious manner as soon as possible [15]. The storage of most online data is interim and temporary. If the digital evidence is not extracted and preserved promptly, it will be challenging to recover it after it is automatically deleted or destroyed by the criminal suspect, which will hinder the proof of the facts of the public-related cybercrime. Public-related cybercrime involves many people and a wide range, and timely extraction and fixation of digital evidence is helpful to clarify the facts of the case, especially the sentencing facts. This principle also requires the investigating agency to fix and preserve evidence on time.

The principle of complete evidence collection requires that the investigating agency should try its best to ensure that the integrity of the evidence has not been compromised in the process of collecting and fixing evidence. There is a one-to-one correspondence between the complete chain of digital evidence

and the facts to be proven. Still, incomplete one-sided digital evidence cannot wholly reflect the facts of the case. The complete extraction and preservation of digital evidence is the premise of ensuring its authenticity, originality and integrity. So far, in China's current legislation, there is no clear and detailed provision that forensics personnel should completely extract and fix digital evidence. Therefore, given the current severe situation of cybercrime in China and a legislative vacuum, the principle of complete evidence collection should be clarified in the legislation.

The principle of comprehensive evidence collection requires that when collecting digital evidence, the investigating organ shall gather evidence of the perpetrator's guilt, innocence, and minor crime, as well as direct and circumstantial evidence. At present, in judicial practice, it is common for investigators to collect only incriminating and serious evidence in retaliation, and this is easier to achieve in digital evidence forensics. The proof of the facts of a case by digital evidence is often combined with traditional evidence to accomplish the probative effect. A lot of digital evidence that seems to be unrelated to the crime can play a huge role in proving the identity of the perpetrator and the criminal act, such as the login record of the QQ account at a specific time [16]. Digital evidence for public-related cybercrimes exists on both the criminal suspect's and the victim's side, and evidence cannot be selectively extracted and fixed because of the large variety and quantity of evidence for public-related cybercrimes. The comprehensive collection of evidence shall consider significant factors such as the subject involved in the case, time, location, and the process of extraction and fixation.

The principle of non-destructive forensics is to ensure that digital evidence is collected as safe and credible as possible, which is to prevent it from being damaged in the process of extracting and fixing [17]. Non-destructive forensics collection shall include the following requirements: first, after the original digital evidence is accurately reproduced, it shall be verified, and the copied digital evidence can only be followed up under the condition of ensuring that the copied digital evidence is consistent with the original data; second, when the digital evidence is accurately reproduced, clean storage equipment shall be used to prevent evidence contamination, and at least two copies shall be made for subsequent use; third, encryption security measures shall be used in the process of extraction and fixation to prevent tampering with the originality of the digital evidence. Fourth, ensure the safety and credibility of the hardware system, software system and analytical methods for analyzing digital evidence, and prevent deviations in the process of analysis, inspection and identification; fifth, in the process of extraction and fixation, analysis, inspection and identification, specific personnel should be recorded in detail and supervised.

Improve mechanisms for the assessment and preservation of evidence: Compared with traditional evidence such as documentary evidence and physical evidence, digital evidence has apparent characteristics such as being easily destructible and easy to tamper with, and is manifested in the process of fixation, preservation, and transfer, which needs to be further proved in the litigation of public-related cybercrime. It is necessary for China to construct a complete set of simplified proof mechanisms to resolve the problem of proof of public-related cybercrime. Specifically, it is to reduce the burden of proof on cybercrime by constructing a simplified proof mechanism for cybercrime [18]. The specific measures include methods such as expanding the interpretation of the law, shifting the burden of proof, and lowering the standard of proof, and directly confirming the relevant facts based on non-evidentiary proof methods such as presumption and judicial cognition. To construct a simple proof mechanism, we should focus on the identity and relevance of digital evidence. The simplified proof mechanism can alleviate the deadlock of digital evidence proof to a certain extent, and then help the contradiction between the legal provisions or the absence of legal requirements and the actual situation in the process of evidence collection.

Digital evidence has the characteristics of easy changeability, virtuality, and easy accurate reproducibility, which gives rise to the issue of the authenticity of digital evidence in the process of determining at trial. It is necessary to improve the rules for the authenticity of digital evidence to identify the authenticity of digital evidence. The core content of the digital evidence authentication rules is: if the extracted digital evidence can guarantee its authenticity, legitimacy and relevance, it can be used as evidence for the adjudicator to form the evidence of the heart; if the digital evidence collected in violation of the authentication rules should be differentiated in accordance with the different specific circumstances, which digital evidence are directly excluded, and which digital evidence can be used after correction.

At present, digital evidence preservation in China is mainly in the form of seizing, sealing, and operating in the form of written records of digital evidence carriers. At the same time, synchronous audio and video recording are used as an auxiliary method. At present, in the legislative process, China should clarify the steps, forms, and contents of digital evidence forensics and preservation records, and build a complete digital evidence restoration system. The existing theory of evidence preservation holds that evidence can only be preserved when there is a risk of loss or when it is difficult to obtain in the future. This kind of preservation system cannot meet the current needs of public-related cybercrime for digital evidence preservation. If the preservation time is delayed, it will lead to the destruction, loss or defects of digital evidence. To address the above issues, the legislator should lower the conditions for the application of digital evidence preservation. Due to the large amount of digital evidence and the high requirements for the professionalism of evidence collection, legislators should expand the scope of digital evidence preservation subjects, and digital evidence can be preserved by forensic appraisal institutions, third-party neutral preservation institutions, etc.

Improve the application of relevant rules on primary evidence: The best evidence rule was originally a rule of evidence for documents. However, the concept of "instrument" can be broadly understood in modern society, which has been extended to include photographs, videos and records. Digital evidence breaks down the boundaries between originals and copies, and it is difficult to distinguish between the two, and the premise of applying the best evidence rule is undermined. If the digital evidence can be extracted and transferred with the original storage medium, there is no question of applying the best evidence rule, and if the digital evidence cannot be extracted or transferred with the original storage medium, the application problem arises. The best evidence rule is applied with the aim of providing the best and most probative evidence for the case. In practice, the original digital evidence may no longer be required to be of a strict nature. A copy may be used as a basis for the determination of a case if the copy substantially and accurately reflects the information in the original and its evidentiary value. At present, science and technology have been able to ensure the accurate reproduction of digital evidence. In this case, it is difficult to distinguish between the original and the copy of digital evidence, so it is a waste of judicial resources to insist on the difference between the two. China's legislation can take "integrality" as the criterion for judging, that is, it no longer distinguishes between originals and copies, as long as the integrity of digital evidence in the extraction process can be guaranteed, it can be used as the best evidence.

The rule of reinforcing evidence is often applied to the confession of the prosecuted person or other verbal evidence. Still, with the development of judicial practice, especially the emergence of cybercrime, this understanding cannot be applied to judicial practice. Because digital evidence is accessible to tamper with, damaged, and not easy to discover, it is often included in the scope of supplementary evidence, which is a type of evidence with weak probative power. In the case of public-related cybercrime, the amount of digital evidence is large and complex to extract, and it is not easy to extract digital evidence from a large amount of data that can indeed prove the crime. In addition, digital evidence cannot be submitted to the court in its entirety, and only a segment of the digital evidence chain is submitted, which needs to be explained by other evidence [19]. Given the enormous tasks of cracking down on public-related cybercrime, China should improve the rules of supplemental evidence, establish a statutory presumption mechanism for evidence, and open up the path to accomplish the identity of the factual evidence of the crime and the person being prosecuted.

The legitimacy review of traditional evidence is mainly carried out from four perspectives: the form of evidence, the subject of collection, the content and the collection procedure, while the legality review of digital evidence is mainly carried out from two aspects: the subject of collection and the collection procedure. China stipulates the circumstances of illegal exclusion from the authenticity of digital evidence, and does not explicitly mention legality. China's

current rules for the unlawful exclusion of digital evidence are missing. In the process of improving the rules, China can set up a resource pool of experts specializing in the digital evidence to assist in evidence collection, combine the professional knowledge of investigators and technical personnel, enhance the professionalism of the subject of evidence collection, and solve the problem confusing the subject of digital evidence forensics [20].

Conclusion

In recent years, there has been a high incidence of public-related cybercrime, which has brought significant losses to citizens and undermined social stability. To improve the efficiency of combating public-related cybercrime, it is necessary to upgrade the evidence collection system to provide a factual basis for the identification of crimes. The efficiency of obtaining evidence for conviction depends on the rational design of the evidence collection system. The current problems in China's evidence collection system for public-related cybercrime have hindered the effectiveness of cracking down on this type of crime. At present, the main problems in evidence collection are the lack of professionalism of the evidence collection subject, the non-standard evidence collection procedures, and the impact on the evidentiary ability and probative power of digital evidence. The improvement of the evidence collection system can be based on the characteristics of public-related cybercrime and the characteristics of digital evidence as the primary evidence in a verdict, and combine judicial practice and the basic principles of the criminal procedure law and evidence law to reasonably construct the system. Specifically, China needs to improve the professionalism of the entities involved in the collection of evidence in cybercrimes, promote the system for the approval and supervision of evidence collection, clarify the legal principles for evidence collection in cybercrimes, improve the evidence assessment and preservation mechanism, and improve the application of relevant major evidence rules.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Xingan, L. İ. "Crucial elements in law enforcement against cybercrime." *Int J Inf Secur* 7 (2018): 140-158.
2. Morgan, Edmund M. "The law of evidence, 1941-1945." *Harv Law Rev* 59 (1946): 481-576.
3. Kerr, Orin S. "Digital evidence and the new criminal procedure." *Colum L Rev* 105 (2005): 279.
4. Payne, Brian K. "Defining cybercrime." The Palgrave handbook of international cybercrime and cyberdeviance (2020): 3-25.
5. Ward, Tony, Russil Durrant and Jacqueline Sullivan. "Understanding crime: a multilevel approach." *Psychol Crime Law* 25 (2019): 709-711.
6. Rogers, Marcus. "Forensic evidence and cybercrime." The Palgrave handbook of international cybercrime and cyberdeviance (2020): 425-445.
7. Kleijssen, Jan and Pierluigi Perri. "Cybercrime, evidence and territoriality: Issues and options." Netherlands yearbook of international law 2016: The changing nature of territoriality in international law (2017): 147-173.
8. Curtis, Joanna and Gavin Oxburgh. "Understanding cybercrime in 'real world'policing and law enforcement." *Pol J* 96 (2023): 573-592.
9. Yang, Fan and Jiao Feng. "Rules of electronic data in criminal cases in China." *Int J Law Crime Justice* 64 (2021): 100453.
10. Jackson, Vicki C. "Constitutional law in an age of proportionality." *Yale Lj* 124 (2014): 3094.
11. Wang, Bo and Yuxian Liu. "Collection and judgment of electronic data evidence in criminal cases: From the perspective of investigation and evidence collection by public security organs." *J Forensic Med* 5 (2019): 187-194.
12. Ribeiro, Gustavo. "Relevance, probative value, and explanatory considerations." *Int J Evid Proof* 23 (2019): 107-113.
13. Xu, Zhenyi. "The procedural dilemmas and improvement of excluding illegal evidence in Chinese courts." *Com L Rev* 6 (2022): 3-12.
14. Guo, Zhiyuan. "Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications." *CLSR* 48 (2023): 105774.
15. Kenneally, Erin E. and Christopher LT Brown. "Risk sensitive digital evidence collection." *Digit Invest* 2 (2005): 101-119.
16. Zhang, Aolan, Ben Bradford, Ruth M. Morgan and Sherry Nakhaeizadeh. "Investigating the uses of mobile phone evidence in China criminal proceedings." *Sci Justice* 62 (2022): 385-398.
17. Guo, Hong and Junlei Hou. "Review of the accreditation of digital forensics in China." *Forensic Sci Res* 3(2018): 194-201.
18. Al-Ali, Abdelrahman Abdalla, Amer Nimrat and Chafika Benzaid. "Combating cyber victimisation: Cybercrime prevention." Cyber Criminology (2018): 325-339.
19. Pillai, Dr Aneesh V. "Admissibility of digital evidences: An overview of the legislative and judicial perspectives." *Elen L R* 2 (2016): 60-72.
20. Zhao, Yue. "Constructing the exclusionary rule of illegal evidence in China." Atlantis Press (2020): 122-128.

How to cite this article: Hu, Zhanfeng. "Study on the Evidence Collection of Public-related Cybercrime in China." *J Forensic Res* 15 (2024): 607.