Analysis of the Crime of Damaging Computer Information System

Abating the Phenomenon of "Pocket Crime" of Cybercrime

Bixuan Hao[1, *, †], Xinya Xue[2, †], Ao Zhang[3, †]

[1]Faculty of Liberal Arts and Professional Studies, York University, Toronto, M3J 1P3, Canada
[2]Civil and Commercial Law School, Shandong University of Political Science and Law, Jinan, 250014, China
[3]Law school, Southwest Medical University, Luchou,646000, China
[†]These authors contribute equally.

beckyhao@my.yorku.ca

Abstract. In recent years, the number of judicial practice cases of crimes against damaging computer information systems has climbed with the rapid development of science and technology. The controversy about how to apply this crime has become increasingly controversial. Especially in the context of a risky society, the protection line of criminal law is in advance, making the boundaries of this crime extended and more ambiguous. From the perspective of legal interests protected by this criminal provision and its implementation, this paper clarifies the boundaries of this crime and analyses the significance of this crime in practice in the context of traditional crimes or new cybercrime. This paper also describes the implicated relation of the perpetrator for committing multiple acts and clarifies the criteria for conviction when there is a "concurrence of crime" with traditional type crimes. As a result, over-expansion of this crime that would blur the boundary between this and the other crime could be avoided. In order to further clarify the scope of application of crimes against computer information systems, this paper also advocates combining relevant judicial practice cases, drawing on the German "shortened two-act offenders" theory and advocating the unity principle of subjectivity and objectivity. These approaches can improve the efficiency of judicial application and provide powerful help for regulating and preventing cybercrime.

Keywords: Legal interests, Crime pattern, Damaging computer information system crime, Pocket crime.

1 INTRODUCTION

With the rapid development of science and technology and the advent of the era of big data, the judicial practice of this crime has gradually matured over the past 25 years and, to a certain extent, formed the general theory of adjudication standards and practices. However, the rising number of judicial cases of this crime in the context of risk

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 1138–1153, 2022.
https://doi.org/10.2991/978-2-494069-89-3_133

society seems to indicate that this crime tends to become a "pocket crime." It leads to the possibility that the reasonableness of sentencing for their criminal conduct will be gradually eroded, and the specific application of this crime would become a point of contention. For these issues, some scholars have provided suggestions for criminal justice determinations about specific criminal acts, such as the conviction standard of DNS hijacking-type traffic hijacking [1]. Others have analyzed the impact of subtle wording discrepancies on individual cases, such as clarifying the criminal meanings of controlling, acquiring and destructing computer information systems [2]. However, case-by-case analysis and the distinctions in wording do not provide a universal principle and path for defining this crime. Therefore, there is a lack of an overarching analytical framework to develop a basic consensus for people on the definition of this crime. The reasons may be that this crime contains or are capable of containing many heterogeneous and different types of conduct, making it difficult to generalize the legal interests they protect. Meanwhile, the corresponding criminal intent, means and results, and the object or objects infringed have become increasingly complex and networked. Besides, this crime is easily confused with traditional crimes against property or crimes against the economic order category. It is currently possible to regulate the vague definitions of individual terms of this crime based on the relevant judicial interpretation documents. It might assist judges in clarifying the constituent elements of this crime in practice and applying them specifically. However, there is still the inconsistency of the relevant guiding cases in identifying this crime and the problems of "concurrence of crime" related to traditional crimes. Therefore, reducing the phenomenon of "pocket crime" of this crime can be achieved by clarifying the legal interests protected by this crime and the boundary between this crime and the other crime. In other words, these approaches can uphold the statutory principle of offence, thereby preventing obstruction of judicial fairness and efficiency.

2 THE RAISING OF QUESTIONS

2.1 Potential factors for the expansion of crimes against damaging computer information systems

Contemporary social conditions have undergone and are continuing to undergo a fundamental transformation, which not only brings more uncertainty but also promotes the dominance of a risk consciousness in social management. Some sociologists describe the current era as "liquid modernity" [3], the "network society" [4], or the age of "mobile hybrids" [5]. While this modernization process is conducive to the accumulation of material wealth for people, people cannot ignore its double-edged sword effect. In other words, technology has promoted a significant increase in social productivity, but at the same time, it has also pushed the dangers or potential threats to a state that is difficult for people to perceive. Ulrich Beck, a leading German sociologist, conceptualized this phenomenon as a "risk society" [6]. In such a society, increasingly advanced science and technology improve people's quality of life, but the risks it poses place people in an unsafe environment [6]. People can also not manage these risks based on their cognitive and practical abilities [6]. As the COVID-19 out-

break that the world is experiencing and the ensuing issues of personal information collection and information security demonstrate, a risky society, country, or even world is something that people have to face and deal with.

In addition, there is a mutual construction relationship between law and risk. In responding to risk, law, as one of the most important instruments for managing society, has advantages unmatched by other mechanisms for intervening in risk. Thus, the criminal law system is bound to bear the brunt of responding to a risky society. However, there is a mismatch between the regulatory means of traditional criminal law and the emerging risks. This gap reflects the contradiction between the limitations of traditional criminal law and the uncertainty of emerging risks. The former involves the passive idea of modesty, the retrospective response mechanism, and the individual-centred definition of legal interests. These fail to recognize and deal with the new risks emerging endlessly and accessible out of control. They also could not prevent catastrophic consequences of risks in advance and the infringement of those legal interests that fails to manifest themselves in the materialized form [7]. Therefore, based on the sociolegal perspective that regards the law as a social construction, the contemporary criminal law will inevitably change from traditional criminal law to risk society criminal law. At the level of legal interests, it has gained new development opportunities. For instance, it has developed from a material perspective to a spiritual one [8], raised a spiritualized legal benefit of universal social security values, and appeared the diversification of the legal benefit structure [7]. These developments strengthen the ability to recognize and deal with emerging risks.

However, based on the ambiguity and expansion of the concept of legal interests in a risk society, the determination of some crimes shows a trend of improper expansion and "pocket crime." It is mainly reflected in the competition between the materialized personal legal interests and the spiritualized transpersonal legal interests [8] and the competition between legal interest structures such as the monistic legal interest theory and the dual legal interest theory. Similarly, the confusion of crime patterns and emerging crimes with traditional crimes is also a problem arising in the process of the transition of traditional criminal law to risk society criminal law. The definition of the legal interests, crime patterns, and the concurrence of new crimes with traditional crimes influence the conviction or non-conviction, the degree of crime and the distinctions of this crime from the other crime. Therefore, the clarification of them has a crucial role in insisting on the statutory principle of offence.

The Issues of Definition of Legal Interests. According to the different subjects of legal interests, legal interests are usually divided into individual legal interests and collective legal interests. In its literal meaning, personal legal interest protects individual interests, such as personal property and liberty. Collective legal interests, also known as transpersonal or public legal interests, are related to collective interests such as public order. When different legal interests are defined for a particular offence, they can have completely opposite results about conviction or non-conviction. In determining the legal interest of the crime of damaging the computer information system, there is a case of collective legal benefit to expand the crime and individual legal benefit to narrow the crime.

Moreover, the provisions in the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases Endangering the Security of Computer Information Systems have the potential to unduly expand the scope of this crime. For instance, the third paragraph of Article 4 provides that "illegal income of more than five thousand yuan or cause economic losses of more than 10,000 yuan," and the fifth paragraph of Article 4 requires that "cause other serious consequences." The former's amount of money for incrimination is obviously easy to reach based on today's level of socio-economic development. The latter gives courts at all levels a great deal of discretion. It makes people sufficient in practice for committing a crime if they perform any kind of deletion, modification or/and addition to any data stored, processed or transmitted in any computer information system [9].

Therefore, some scholars suggest that the legal interests of the act of this paragraph should be appropriately narrowed down by the criterion of the same kind of object of the crime [9]. In other words, the legal interests protected by the act of this paragraph should be measured from the perspective of the entire criminal law system. For example, Article 286 of the Penal Code, the crime of damaging computer information systems, is located in Chapter 6, Section 1 of the Penal Code—the crime of disturbing public order. Therefore, it seems that according to this classification, it should locate the legal interest of the crime at the social level. Specifically, people should measure whether the act involved in the crime is sufficient to disturb the public social order and to reach the degree of "serious consequences." This classification is prone to the occurrence of this non-conviction situation. The perpetrator uses his position or job to gain access to the company's network and delete, modify or/and add to the data. They might ultimately profit themselves by upgrading the account without monetary gain [9].

Admittedly, a large number of scholars oppose the above view and believe that the legal interest protected by the crime of damaging the computer information system is an individual legal interest rather than a kind of social order legal interest. Specifically, some traditional views and even authoritative jurisprudence support that the object of the crime is "the state management order of computer information system security." Although this understanding has a certain basis and guidance, this perspective is not in line with the current development of the network society [10]. The crime is under Chapter 6, Section 1 of the Criminal Law, the crime of disturbing public order, but this does not mean that all the provisions in this section necessarily have to protect a social interest first and foremost. In addition, from the legislator's intention, the addition of this crime in 1997 sought to strengthen the management and protection of computer information systems to ensure their proper functioning and safe operation. Therefore, if it is assumed that the crime mainly protects the legal interests of the social order, it will weaken the original legislative intent of the crime to protect computer information systems. This crime's application could be unduly limited [10]. It is also difficult to find the limitation of cybercrime to the level of social order if this article draws on the relevant legislative experience abroad. For example, the Computer Fraud and Abuse Act in the United States and the provisions related to computer

crimes in the Japanese Penal Code do not consider disturbance of public order as their primary consideration [10].

Unclear Perception of Crime Patterns. In judicial practice, there are often unclear definitions of crime and non-crime as well as this crime and that crime. These result in the expansion and contraction of judicial interpretation at will. Thus, it can decrease the acceptability of judicial decision results. The cause of the above problems is, in the final analysis, the unreasonable use of discretionary power and the blind expansion of the interpretation of the law [11].

The third paragraph of Article 286 is related to the determination of the subjective aspect of "intentional", to determine whether the defendant's subjective intentional crime can be its defense. For judicial practice, the prosecution looks for the "ghost-like" subjective consciousness of the defendant, especially when the defendant made a denial of intentionality. In particular, when the defendant negates the intentional, how to determine the concept of intentional, such as partial knowledge, determinate intention, and actual knowledge. The author believes that the subjective intention should be confirmed by the judge through social experience, testimony, etc., that his behaviour is intentional.

The serious quantitative part of the consequences, still for personal, general computer information system sentencing protection lack relevant judicial interpretation [12]. The judicial interpretation only clearly put forward the "amount", but not the "personal" computer damage severity consequences to explain, which is the missing part of the legal provisions. It does not comply with the principle of legality and security principle in the logic of the legal norms proposition. As well as too quantitative "serious consequences" will be contrary to the spirit and purpose of the legislation. Computer security is not effectively protected, and not every crime is carried out through the amount. The seriousness of the consequences is limited to the amount. The criminals may well bypass the "serious consequences" of their suffering and determination of the behaviour. At the same time, with the quantifiability of the provision, the scope of its legal application, and the interpretation of the expansion, is easy to become a pocket crime in the network era.

However, the emergence of pocket crimes on the effectiveness of other similar laws, whether the priority will cause a weakening, such as becoming a pocket crime [13]. In terms of sentencing, standards should be carefully divided, for different circumstances should be clearly defined, and sentencing serious or not to be carefully considered. To determine the economic loss in cybercrime, whether it should be seen from the maintenance or replacement costs of the system caused by the inability to operate. Or it is determined by the damage caused in the period between the destruction of its system and its re-operation. The latter will be non-indirectly caused by the expected economic loss. Thus, this is non-indirectly caused by the intention of the saboteur loss, whether the economic loss should be included in the judicial interpretation.

Unclear boundaries with traditional crimes. The unclear boundary with traditional crime is one of the main reasons for the "Pocket Crime" phenomenon of this crime. In the current era of technological updates, crime areas are increasingly closer to cyberspace, and crime methods are constantly updated. At present, Chinese scholars mainly divide cybercrime into two categories. One category is not pure cybercrime, i.e., networked traditional-type crimes that use the Internet as a tool for crime. This crime still essentially violates traditional legal interests. The other category is pure cybercrime. It is the network as the object of crime, infringing on the legal interests of computer information system security specialized cybercrime. This classification basically covers all types of cybercrime. It provides a favourable analysis basis for the increasing number of cybercrimes in judicial practice [14].

Among the many emerging cybercrimes, crimes committed by damaging and intruding into information systems are particularly rampant. The increasing number of judicial precedents of crimes against computer information systems in practice is one of its typical manifestations. In recent years, the COVID-19 epidemic has had a huge impact on economic and social development. At the same time, with the increasing popularity of the Internet, the phenomenon of damaging computer information systems occurs frequently. Due to the substantive flaws inherent in legal language, it is often difficult for words to convey their actual meaning. The different interpretations of the same term are the key to the different trials of this crime in judicial practice. This different interpretation is the main reason why some scholars believe that the crime has the tendency to gradually become a "pocket crime". At the same time, because of the diversity of the act of committing this crime and the easy interconnection with other crimes. It is easy to combine this crime with traditional crimes in practice. This leads to a great controversy in the specific application of this crime in judicial practice. To sum up, this article should strictly regulate the criteria for determining the crime, and interpret it in a limited way. Meanwhile, the judges should clarify the protection value of the crime and the interpretation position. People should avoid expanding the scope of interpretation and lowering the standard of incrimination as the primary issue.

3 REASONS FOR THE PROBLEM OF “POCKETING” OF CRIMES AGAINST COMPUTER INFORMATION SYSTEMS

3.1 Reasons for the divergence existence of individual and collective legal interests

The misalignment and opposition mentioned above derive from the certain abstraction and spiritualization of the theory of legal interests itself as a conceptual form and the diversity of types of legal interests and their theoretical positions. According to the different subjects of legal interest, this paper focuses on distinguishing the theoretical position of individual and collective legal interest in the crime of damaging computer systems. There is a view argued that collective legal interest cannot be denied because

their absence would render criminal law incapable of dealing with the security problems based on risk society. However, its excessive promotion would reduce criminal law to an instrument of risk prevention at the expense of human rights protection mechanisms. In other words, the collective legal interest is a necessary component of the protection of criminal law that existed at the very beginning of the theory of legal interest. Thus, the controversy is not about whether it is protected but about the form of its existence, its relationship with the individually legal interest, and the extent to which it is protected [15].

In the current legal interest theory framework, one of the primary debates is about using either the monist legal interest theory or the dualist legal interest theory. Some believe that collective legal interests should be regarded as individual legal interests. However, others argue that collective legal interests can simultaneously be considered the public interests as a whole and have the self-purpose. Individualistic monism holds that collective legal interests do not have the need or value to exist independently. Alternatively, it denies the existence of collective legal interests on its own but holds that they can only be protected by criminal law because they are conjunctive to individual legal interests. The dualistic legal interest theory is understood into value-independent and value-connected models [15]. Individual and collective legal interests exist independently and have no derivative relationship, so collective legal interest has an independent, self-centred purpose. Also, protecting collective legal interest is preserving individual freedom, and individual legal interest is the ultimate value dependence of collective legal interest. The latter perspective of the dualistic legal interest theory can moderate the tension between collective and individual legal interests by embedding an element of individual legal interest and using it as a threshold for protecting collective legal interests [15].

3.2 The crime extends to the interpretation of the problem

The scope of literal interpretation is too large, resulting in different disagreements on the extent of the crime in practice. Because the overgeneralization of legal interpretation and discretion is demonstrated, despite the existence of relevant judicial interpretations of vague words. The essay believes their interpretation is still limited to literal interpretation, without relevant systematic interpretation and teleological interpretation [16].

For example, the first paragraph of Article 286 of the Criminal Law regulates the implementation of acts of sabotage of computer information systems. The term "sabotage" includes the perpetrating acts of deletion, modification, addition, interference, etc., to the functions of computer information systems. The perpetrating acts committed by the perpetrator that causes the computer information system to fail to operate normally are all acts of implementation of this crime. The above-mentioned acts of execution against the computer information system are all within the extension of "sabotage" stipulated in this crime. Different interpretations of this kind of sabotage are the key to the phenomenon of improperly expanding the application of this crime in practice.

First of all, the act of sabotaging a computer information system is itself directed, direct and destructive in nature [10]. The "act of sabotage" should be based on the substantial damage to the function of the computer information system. More precisely, it is physical or functional damage to the system itself. Since this crime is a destructive crime, it leads to the concept of "normal operation of computer information system" having two meanings. One is the normal operation of the data processing functions of the computer information system. The other is the normal operation of the important usage functions of the computer information system [10]. Under different interpretations of the circumstances, there may be imaginary competition with other crimes.

The lack of clarity in the regulation of the concept of computer information system is one of the reasons for the judicial divergence in practice and the overlap with other crimes. For example, in Xu Qiang's case of Sabotaging Computer Information System [17], defendant Xu Qiang used a GPS jammer to interfere with Zoomlion's IOT GPS information service system. He later used the GPS to unlock Zoomlion's monitoring of the pump truck. From the surface, the defendant Xu Qiang's behavior only excluded Zoomlion's monitoring control of the pump truck and did not cause substantial damage to the service system. However, the service system itself was developed for the purpose of recovering the pump truck on schedule. The defendant's actions, in essence, caused the controller on the pump truck will no longer judge the timing activation command of the Zoomlion GPS. His behavior in essence destroyed the normal use function of Zoomlion's IOT GPS service system, which is a crime of damaging computer information system. However, the conviction of this case is highly controversial in reality. Some scholars believe that the defendant Xu Qiang violated the national business regulations for the illegal operation and should be found guilty of illegal operation. Other arguments are that Xu Qiang should be recognized as an accomplice to contract fraud and theft, and Xu Qiang belongs to the joint crime of this crime to help commit. The issues mentioned above might easily result in the phenomenon of disagreement in practice. The reasons are that people might question whether the monitoring system belongs to the concept of the computer information system. People usually have different understandings on issues such as whether the act of damaging surveillance systems constitutes a crime of damaging computer information systems.

Secondly, a variety of intentional identification of the way of uncertainty resulting in different adjudication results is due to the failure to combine the principles of other crimes. Its penalties are embodied in criminal law to regulate the results of the system of interpretation. Not in advance to build a good three-dimensional thinking and interpretation framework, results in most of the relevant decisions being limited to the scope of the crime. It is not from the common principles presented in criminal law. Thus, in the process of adjudication of the case, the same case has different judgments. However, people should also combine the method of purpose interpretation to achieve the idealized results of our "limitation". "Economic loss determination" and other problems that do exist in concrete practice, include the hypothetical problem raised above. These should be correctly and scientifically defined as economic loss. Some scholars believe that the interpretation of purpose is a kind of expanded inter-

pretation, which will intensify the emergence of pocket crimes. This paper believes that the interpretation of purpose cannot be generalized as expanded or reduced. From what this article considers, it should be regarded as a "proportional interpretation". In other words, the subjective purpose of the offender should be interpreted in terms of the importance of the relevant object and the actual percentage of infringement. To sum up, the problem of the number of crimes is the incomplete and unspecific consideration of the interpretation system. The failure to think comprehensively is for the reasonable use of discretion. The path of the judicial solution to the crime of damaging computer information system.

4 THE PATH OF JUDICIAL SOLUTION TO THE CRIME OF DAMAGING COMPUTER INFORMATION SYSTEM

4.1 Appropriate treatment of the relationship between collective legal interests and individual legal interests

This article believes that the identification of legal interests should not only stay in the categories of legal interests but should also return to the relationship between individuals, society and the state. Under the framework of the monistic legal interest theory, the only meaning of collective legal interests is to provide the pre-protection for individual legal interests, which degrades the status of collective legal interests. Also, it is difficult to prove the causation between criminal conduct of composition and hazardous results in particular cases. Therefore, this sort of crime usually presents in the way of defending independent collective legal interests, in which it is hard to define legal interests for individuals. However, the individuals' legal interests could be seen as the terminal goal of protecting collective legal interests.

In the case of Sen Li and others destroying the computer information system [18], the defendants used cotton yarn to block the sampler of the auto-monitoring station for ambient air in Chang'an District, Xi'an, many times during the period from February to March 2016. This case interferes with the data collection of the auto-monitoring system of ambient air quality inside the station and causes the monitoring data of the station to be seriously distorted in multiple periods. As a guiding example, this case aims to clarify whether the perpetrators' direct or indirect behaviour toward the computer information system meets the elements of criminal composition. Some scholars believe that the conviction of Sen Li and others is a typical misreading of the crime based on the analysis of the behaviour itself. However, this case can also be analyzed from the perspective of legal interest. Although the court's decision does not explicitly mention it, the judge might have considered this aspect.

First, scholars who are critical of the court's decision base their discussions on whether the acts of Sen Li and others have endangered the individual legal interests of the auto-monitoring station for ambient air in Chang'an District, Xi'an City. This view from monistic legal interest theory automatically ignores the social reality that the auto-monitoring of ambient air is associated with the interests of the whole society.

Hence, if the interest of the monitoring business of the ambient air to society is considered, the collective legal interest should be considered independent of the individual legal interest in terms of value and purpose. Secondly, according to the theory of dual legal interest, the collective interest, in this case, is also based on the individual legal interest to establish. Its original value depends on the preservation of the computer information system of the auto-monitoring station for ambient air in Chang'an District, Xi'an. Its core value is on the maintenance of this social order of environmental monitoring. In other words, stable individual freedom can only be achieved through various institutional arrangements in the social community. The inner logic of freedom determines that the collective legal interest protected by criminal law is usually the preserve of individual freedom. Hence, the unspecified and the scaled new modern risks that are difficult to be integrated effectively with the traditional individual legal interest can be dealt with through the imputation model protecting the collective legal interests [15].

However, pocket crime usually reflects that it is a crime against collective legal interests but not against individual legal interests [19]. Therefore, in the process of attaching importance to the conservation of collective legal interests, the possibility of personal legal interests should also be fully considered. It can help to avoid damaging the freedom guarantee function of criminal law and limit the undue expansion of this crime.

First, not all the collective legal interests belong to the legal interests that are worth being protected by the criminal law. That is to say, only the collective legal interests that have significant values are deserved to be protected, namely considering whether this collective legal interest serves to enhance the vital interests of citizens. Additionally, when the violation of collective legal interests is likely to infringe the individual legal interests, people are necessary to safeguard this legal interest by the criminal law. Second, even though criminal punishment may be a reasonable means to secure the collective legal interests, it also is needed to judge the impact of the application of punishment on the protection of social-legal interests and the various activities of all citizens [19]. If the criminal regulation of certain network activities leads to the shrinking of national economic behaviour, it will seriously hinder the development of the economy. Thus, the gains outweigh the losses.

Third, whether a crime infringes public legal interests need to be judged according to the provisions of the criminal law itself. Crimes infringing on individual legal interests cannot be identified as a crime infringing public legal interests just because the act is related to public affairs. For instance, the sabotage of a computer system in a company is a crime against individual legal interests. Although this computer system may connect to public administration affairs, it is still a crime against individual legal interests. The act should not be characterized as a crime infringing upon the collective legal interests because it involves public affairs and is seen as endangering public order. It could make the conviction aggravating. Fourth, the best way to justify whether a behaviour violates the collective legal interests is to characterize whether the behaviour ultimately violates the individual legal interests. If a negative conclusion is reached, it cannot be considered that it violates public legal interests [19].

4.2 Further standardize the implementation of the act of interpretation standards

Therefore, the appearance of "pocket crimes" is inevitable and contradictory. In the long run, only by constructing the unity, standard, and science of the legal logic reasoning of the judicial judge is the correct way. It should look deeper into the purpose of the legislation, and the benefits of law sociology. Legal professional community recognition avoids the emergence of pocket crimes. It also shows the effective application of the principle of modesty in criminal law. The absence of the constituent elements must be further supplemented from the legislative text. That will clarify the provision in the semantic interpretation of the specific embodiment of the spirit of criminal law. The trend of a single provision of "pocket crimes", relies only on the discretion of generalization. That will not achieve the actual connotation of the law in line with the community. Thus, the specific approach should expand the provisions of the sub-articles, not only to clarify the object of legislative protection and not limited to a quantitative interpretation. It also comes from the specific effects of criminal behaviour to better adapt to the justice and flexibility of judicial decisions.

From the effects of the crime of damaging computer information systems discussed in this paper, the trend of pocketing is explained, as the lack of protection for the integrity of general data. The consequences of damage are limited to the narrow regulation of causing the computer system not to operate normally. As reflected in the guiding cases of the Supreme People's Court pointed out through the decision points "by modifying [20], increasing the computer system data. The implementation of illegal control of the computer information system did not cause substantial damage to the system function or cannot operate normally. This should not be recognized as a crime of destruction of computer information systems. Lack of data protection in general and the composition of the elements set specifically and independently. The definition of "not functioning properly" for "function", and "data and application" is firstly judged by whether it affects the function or only the effect. The impact is focused on the computer server's computing, storage, and other characteristics of interference, damage, and another behavioural impact. The effect of the impact will be the view of the single existence of the act of access, the basic nature of the computer is that non-authorized access to the system functions will not cause damage. The existence of possibility of damage to the independent conditions will be caused by an uncertain effect. Meanwhile, how to correctly determine the nature of this potential factor is essential. Whether the uncertainty of the future consequences of its existence can be confirmed to cause the "crime of destruction of computer information systems". It appears in Article 286 of the Criminal Law. Thus, there is a lack of judicial interpretation between the deterministic and uncertain effects. The part left blank for such factors that potentially affect computer functions cannot be determined by the discretion of judicial judges alone. The supplement of legislation and judicial guidance is the standard principle of unified adjudication results. In addition, the degree of destruction is utility infringement or exclusion and restriction of the right holder's application of possession or control. That involves the specific distinction between Article 286 of criminal law. It also involves the civil law of unauthorized possession on the premise

of judicial construction of such sectoral law identification requirements. For example, the defendant's defense counsel in the defense opinion pointed out that it did not carry out "destructive behaviour. This inference is based on the legal provision causing the computer information system to fail to function normally" as stipulated in Article 286 of the Criminal Law. This presupposes that the defendant did not materially damage the function of the target computer. The valuable data modification, then from the perspective of sectoral law this belongs to the civil law adjustment scope or criminal law jurisdiction is open to question. At the same time, it should be noted that the potential damage effect and the degree of destruction at all times should be closely linked, the two should be mutually sufficient and cannot be separated separately. In that case, it better serves as an important jurisprudential basis for the legislation and justice of the vacancy part of the crime. All in all, the key to the effect of the specific actions to expand the legal understanding of the consequences, is the legal protection of the general destruction of the way. The crime of "pocketing" understanding, the authors think is dialectical, and relative, and cannot be rejected or generalized. It should be combined with judicial practice, the spirit of the legislation, and social impact. These three comprehensive considerations, to the optimal effect of the protection of the interpretation of the standard system, can build the judicial framework.

Hence, in the actual judicial activities, the interpretation standard of the crime should adopt the theory of "bounded restriction". The above-mentioned "proportional interpretation" should be adopted from the three influencing factors of law sociology, law interpretation, and the laws in force. The mainstream trend of "pocket crimes" in justice should be curbed. Thus, the methodology described here can be used as a standard of interpretation for the entire criminal law enforcement act of "limitation".

4.3 Reference to the German "The Shortened Two-action Crime"

The theory of "The Shortened Two-action Crime" is used to analyze the subjective purpose of the perpetrator. In practice, there is no clear boundary between this crime and the crime of illegal control of computer information systems and other cybercrimes in practice. Therefore, this article can use the theory of "shortened two-action crime" in German criminal law to help us distinguish them. The rules of justice are established by analyzing the relationship between the purpose of the crime and its act. At the same time, the impact on the composition of the crime is analyzed according to the specific subjective purpose of the perpetrator [21].

The emphasis of this theory is on the subjective purpose of the perpetrator, which is what our Criminal Law calls a purpose crime. From the perspective of whether the subjective and objective are consistent, "The Shortened Two-action Crime" theory is also known as the indirect purpose offense. The purpose of the crime need only exists within the actor's heart and does not require the existence of objective facts corresponding to it [22]. For example, the crime of kidnapping requires the purpose of "extorting property from a third person or making other unlawful demands." In fact, the perpetrator only needs to have control over the hostage to constitute an attempted crime. The perpetrator does not need to actually commit the perpetrating act of extorting property from the third person. Because the indirect purpose does not require the

existence of its corresponding objective behavior. It is easy to lead to shortcomings in the objective aspect.

The general theory of criminal law in China believes that the purpose of the crime can only be constituted by direct intention. If the criminal law will be a certain crime the purpose of the crime will certainly exclude the possibility of indirect intention of the perpetrator. It is obviously unreasonable. This article believes that the purpose of the crime is not directly equivalent to the intentional crime. The crime "purpose" is not exactly the same as the subjective elements of the crime of the will factor. It is far more complex than the intentional will factors. Therefore, this article should use the theory of "shortened two-action crime" to clarify the relationship between purpose and intent. For example, disrupting the normal operation of the system is the fundamental reason that drives the perpetrator to commit an intrusion into the computer information system. Judges can establish judgment rules to determine what kind of criminal purpose is required for the crime to constitute a criminal attempt [21]. Meanwhile, the relationship between the purpose of the crime and the perpetrating act is analyzed, so as to recognize the illegality of the subjective "purpose" of the perpetrator in a particular crime. Judges can distinguish crime from non-crime by the presence or absence of illegality, and distinguish this crime from the other crime by the specific content of the "purpose". At the same time, it is clear that the psychological state of the perpetrator at the time of committing the crime, so as to distinguish the boundary between this crime and the other crime. To make a limited interpretation of the incrimination criteria in order to suppress the trend of "pocketing" the crime.

In judicial practice, the relationship between the subjective criminal purpose of the perpetrator and the function of the computer information system being damaged can be taken as the core judgment element. Secondly, in addition to focusing on the differences between the apparent objective constitutive elements of the crime and other crimes, the subjective purpose of the perpetrator should be examined in depth. Combining the computer technology behavior itself with the constitutive elements, using the instrumental and functional evaluation of the system itself. Thirdly, combining it with the general human cognitive state of the perpetrator's use [10]. For example, the core concepts in the law are judged. First, judges can confirm whether the system that the perpetrator intruded into is a computer information system. Secondly, whether the perpetrator's practice causes the system to be unable to function properly. Finally, the subjective purpose of the perpetrator will be measured in terms of the amount of illegal proceeds as well as the degree of damage. The Judges then combine the actual establishment of a specific data standard system. People should pay attention to the systematic regulation of the criteria for incrimination of acts. It is up to the judge to prevent the situation in practice where the criminal purpose of the perpetrator exceeds the constituent elements of the crime. People should adhere to the "unity of subjective and objective" and attach importance to the subjective purpose of the perpetrator. With this principle as the basis, to judge to distinguish between crime and non-crime, this crime and the other crime.

Due to the rapid development of information technology, the cyberspace is more and more expanded. This development has also led to an increasing range of applications for disrupting computer information systems. Therefore, it is very necessary to

strictly limit the implementation behavior as well as the elements of the crime in judicial practice. In this theory, judges can further distinguish this crime from the other by referring to the subjective purpose of the perpetrator. Judges in practice should strictly follow the principle of "statutory crimes" and adhere to the principle of "no more punishment for one thing". Judges in the trial cannot be superimposed on the degree of wrongdoing of the crime, to avoid the expansion of the scope of application of the crime.

5 CONCLUSION

In the context of the current technological updates and intergenerational differences of the Internet, the crime area is getting closer to cyberspace. The number of judicial cases of crimes against computer information systems is rising. This article systematically analyzes the protection of legal interests, the crime volume elements and the crime number's form. This article also draws on the best theoretical achievements of other countries, such as the theory of value connection and the theory of shortened two-action crime, and chooses to apply them to our national conditions. Besides, this paper considers that this crime is to maintain the regular operation of computer information systems under the premise of protecting the legal interests of individuals. Moreover, this research further explains the specific elements of this crime on the basis of combining the excellent legal achievements of other countries. At the same time, the criminalization criteria are strictly limited. Criminal punishability is clearly defined to clarify the boundary of judicial review with other crimes and avoid the further proliferation of the phenomenon of "pocketing" of the crime in judicial practice. Finally, some issues still have not been addressed in this paper due to the article's length. The specific distinction of the crime in the context of risk society during the epidemic and how to judge it in different situations, such as joint criminality, remains unresolved. Due to the intergenerational transition of the Internet and the increasing number of cybercrimes, this research has further analyzed the evolution of this crime and its characteristics. This research found that further standardization of this crime in terms of preventive supervision is an effective way to eradicate the ambiguity of the "pocket crime" phenomenon.

REFERENCES

1. J. Li, Y.L. Bai, L. Shi.: The understanding and reference of the case of Fu Xuanhao and Huang Zichao: criminal judicial determination of DNS hijacking-type traffic hijacking. People's Justice 17, .90-94 (2021).
2. Y. H. Chen.: "Controlling", "acquiring" or "destroying": An analysis of the crime of traffic hijacking. Journal of Northwestern University for Nationalities (06), 95-103 (2019).
3. Z. Bauman.: Liquid Modernity. 1st edn. Cambridge Press, Cambridge (2000).
4. M. Castells.: The Rise of the Network Society. 1st edn. Blackwell Press, Liphook (2000).
5. J. Urry.: Mobile Sociology. British Journal of Sociology 51(1), 185-203 (2000).
6. U. Beck.: Risk Society. 2nd edn. Yilin Press,China (2004).

7. Y. Y. Liu.: Theoretical transformation of criminal law: from traditional criminal law to criminal law in risk society. Journal of Henan Normal University40 (4), 54-57(2013).
8. F. Fan.: Consideration of Legal Interests of Criminal Law in Risk Society. Journal of Shandong Police College 28(4), 63–69 (2016).
9. N. Zhao.: Research on the Difficult Issues of Determining the Crime of Destroying Computer Information Systems in Judicial Practice. Journal of Shanghai Police College 31(4), 45-49 (2021).
10. H. W. Wang.: The dogmatics reflection and reconstruction of the crime of destroying computer information systems. Journal of Southeast University 23(6), 93-147 (2021).
11. M. X. Gao, D. Z. Sun.: Theoretical evaluation and systemic advancement of criminal law interpretation in the Internet era. Journal of Law and Order Research (1), 23-37 (2021).
12. X. H. Yu.: Analysis of judicial practice and reconstruction of the normative meaning of the crime of damaging computer information system. Journal of Jiaoda Jurisprudence (4), 140-154 (2015).
13. L. B. Zhou.: Analysis of judicial practice of crimes against computer information systems and the adjustment of criminal law norms--an empirical investigation based on 100 judicial precedents. Journal of Research on the Rule of Law (4),67-76 (2018).
14. X. W. Zhang.: Research on the interpretation of criminal law under the dichotomy of cybercrime. Journal of University of Science and Technology Beijing (Social Science Edition) 37(6), 679-688 (2021).
15. P. Huang.: The Academic Genealogy of Legal Interests in Criminal Law. Western Law Review 3, 20–32 (2020).
16. W. Chen, Y. Z. Yang.: The Expanded Application and Rational Restriction of the Crime of Obstruction. Journal of Wuhan University of Science and Technology (Social Science Edition) (4), 419-426 (2022).
17. People v. Xu Qiang, the Supreme People's Court Guiding Case No. 103, December 25, 2018.
18. Li Sen, He Limin, Zhang Fengbo and others to damage the computer information system case, the Supreme People's Court Guiding Case No. 104, December 25, 2018.
19. M. K. Zhang.: Exploring the crime of provoking and provoking trouble. Politics and Law (2),122–129 (2008).
20. Case of Illegal Control of Computer Information Systems by J. J. Zhang and Other Persons, the Supreme People's Court Guiding Case No. 145, September 16, 2019.
21. G. Li, T. Li.: " Discerning the crime of illegal control of computer information system and the crime of damaging computer information system - a perspective of shortened two-action crime." Chinese Prosecutor 14,38-41 (2021).
22. M.K. Zhang.: On the shortened two-action crime. Chinese Jurisprudence (3), 149-158 (2004).