# Research on the Identification Standards of "Destructive Programs" in the Crime of Damaging Computer Information Systems - Based on the Analysis of 35 Judgments

**Xiaotong Ye**[1.2.3.4]

[1]Southwest University of Political Science and Law, Graduate School, 401120, Chongqing, China

[2]DeRUCCI Healthy Sleep Co., Ltd., 523000, Dongguan, China

[3]Henan University, International Business School, 475001, Kaifeng, China

[4]Jinan University, Extension School, 510632, Guangzhou, China

**Keywords:** Crime of Damaging Computer Information Systems; Destructive Programs; Identification Criteria

**Abstract:** This article delves into the criteria for identifying "destructive programs" in the context of the rapidly developing information technology and the crime of damaging computer information systems. Through the analysis of 35 judicial decisions, employing legal empirical research, case studies, and comparative law methodologies, the study systematically examines the concept, characteristics, and challenges in identifying "destructive programs." The research unveils the ambiguities in current legal determinations and puts forward suggestions for optimizing the identification criteria from both legislative and judicial perspectives. The aim is to enhance the fairness and accuracy of judicial decisions and provide legal support for the security protection of information systems. This study offers significant reference value for improving regulations, guiding practices, and raising public awareness of information security. It establishes a multi-dimensional framework for identification criteria, providing guidance for legal practice and laying a foundation for academic research.

## 1. Raising the issue

The continuous innovation in internet technology has brought sustained benefits to related fields. Meanwhile, the forms of computer and cybercrime have also undergone constant evolution. Based on the crackdown on traditional computer crimes, China's criminal regulations have played a crucial role in preventing criminal acts that damage computer information systems [1]. However, with the application of new technologies and the emergence of innovative criminal methods, the essential characteristics of criminal behavior have become increasingly unclear, posing significant challenges to the accurate enforcement of crimes against computer information systems and the identification of destructive programs.

Article 286, paragraph 3, of the "Criminal Law of the People's Republic of China" (promulgated on December 26, 2020, and effective as of March 1, 2021) clearly stipulates that the intentional creation and dissemination of destructive programs such as computer viruses are considered a serious threat to the security of computer information systems. The "Law of the People's Republic of China on Public Security Administration Punishments" (promulgated on October 26, 2012, and effective as of January 1, 2013) also establishes penalties for acts that disrupt public order, including those that affect the normal operation of computer information systems, such as the intentional creation and dissemination of destructive programs like computer viruses.

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 of Jeopardizing the Security of Computer Information Systems," there is a further clarification of what constitutes a "destructive program such as a computer virus," including programs that can replicate, propagate, and damage computer systems, programs that are automatically triggered under preset conditions,

  DOI: 10.25236/icssem.2024.036

and other programs specifically designed to damage computer systems. Both the "Regulations of the People's Republic of China on the Security Protection of Computer Information Systems" and the "Regulations of Chongqing Municipality on the Security Protection of Computer Information Systems" define "computer viruses," emphasizing their self-replicating nature and their ability to damage data or functionality.

Through these laws, regulations, and interpretations, the identification of "destructive programs" involves not only the destructive characteristics of the program but also its means of dissemination, automatic triggering conditions, and the specific threats it poses to the normal operation of computer information systems. In actual judicial practice, the identification standards for destructive programs need to be combined with the circumstances of specific cases through a combination of technical

## 2. Criteria for identification of destructive procedures

Paragraph 3 of Article 286 of the Criminal Law stipulates that "whoever intentionally creates or disseminates destructive programs such as computer viruses, which affect the normal operation of computer systems and have serious consequences, shall be punished in accordance with the provisions of the first paragraph," explicitly singling out computer viruses as a typical manifestation of destructive programs. Computer viruses can be further categorized as file viruses, boot viruses, chain viruses, and macro viruses [2]. However, destructive programs are not limited to computer viruses and can also include, but are not limited to, logic bombs, Trojan horses, rabbits, worms, and others. These programs can cause computer malfunctions, corrupt computer data, and inflict serious damage on information systems. Destructive programs typically exhibit the following main characteristics: infectivity, latency, triggerability, and destructiveness [3-4]. They can hide in executable programs or data files, exhibiting strong concealment and dissemination capabilities. For instance, computer viruses can infect other programs or files by replicating themselves, while Trojan horses may execute malicious operations without the user's knowledge.

From a legal perspective, the Criminal Law does not limit destructive programs solely to computer viruses. For example, Yan Yan and Wei Li point out that the wording of Paragraph 3 of Article 286 of the Criminal Law indicates that destructive programs are not limited to computer viruses alone. Other malicious programs, such as Trojan horses, should also be included in the scope of destructive programs due to their similar characteristics and dangers [5]. In determining crimes related to destructive programs, it is necessary to comprehensively consider the specific behavior of the perpetrator, the consequences of the behavior, and its impact on the functions, data, and applications of the computer information system. Tingguang Zhao and Huachi Zhu note that destructive programs (such as computer viruses) have a wide range of effects, infecting both software and hardware, and pose a direct threat to the functions, data, and applications of computer information systems. However, merely utilizing these destructive programs for destruction without directly involving the creation or dissemination of these programs does not directly constitute the crime of creating or disseminating destructive programs such as computer viruses from a legal standpoint [6]. Meanwhile, the illegal implantation of destructive programs, if it results in serious consequences such as the inability of the system to operate normally, should also be identified and punished as the crime of damaging computer information systems [7].

Technology plays a crucial role in aiding legal practice. For instance, the analysis and forensics system developed by Shanghai Qiming Information Technology Co., Ltd. in 2005 provided powerful technical support for combating computer crimes [8]. The evolution of the definition of "destructive programs" reflected in several legal documents and technical specifications, such as Article 5 of 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 of Endangering Computer Information System Security" published in 2011, the judicial appraisal technical specification "SF/Z JD0403002-2015 Operating Specification for Destructive Program Examination," and "GA/T 1713-2020 Forensic Science - Technical Methods for Destructive Program Examination," demonstrates a deepening understanding of destructive programs while

considering technological advancements and the evolution of criminal methods. Initially, the focus was on the replication, dissemination, and automatic triggering capabilities of destructive programs, as well as their targets of destruction (system functions, data, or applications). This evolved to include a wide range of unauthorized behaviors such as obtaining, deleting, modifying, interfering, etc., expanding the scope of the definition of destructive programs. Finally, the importance of replication, dissemination, and automatic triggering was reaffirmed while maintaining attention to a wide range of unauthorized behaviors, forming a comprehensive and holistic definition. Technological innovations have facilitated judicial forensic analysis, but at the same time, they have also presented new technical challenges for the identification of destructive programs.

## 3. Practical review of destructive procedure identification

The empirical analysis samples in this article are all from the "China Judgment Document Network", with a case type of "criminal case" and a document type of "judgment letter". The cause of the case is "crime of damaging computer information systems", and the fact is "destructive procedures". The judgment period is from January 1, 2010 to January 1, 2024. Based on the above search conditions, a total of 37 criminal judgments were obtained as the initial sample. Among them, 2 criminal judgments were consistent with the content of the other 2 criminal judgments ((2014) Yan Xingchu Zi No. 391, (2016) Hei 0103 Xingchu 584), and a total of 35 criminal judgments were obtained as the inspection sample.

### 3.1. Regional distribution of cases and number of cases

Through the statistics and summary of 35 cases of crimes against computer information system in criminal judgment, this paper makes a detailed analysis of the geographical distribution and number of crimes against computer information system during the research period.

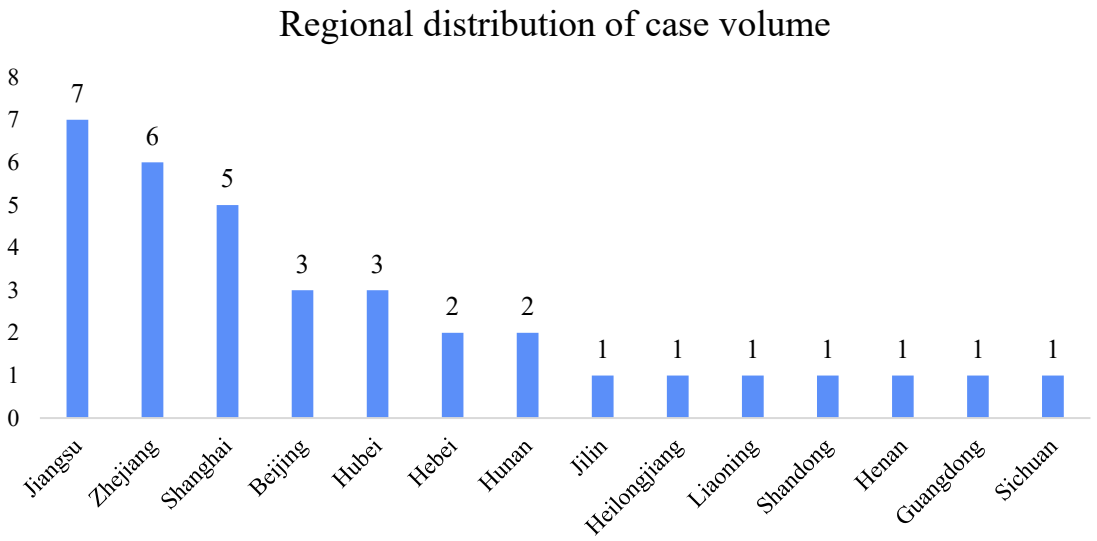


Figure 1 Geographical distribution and number of cases of destroying computer information system crime

Based on the statistical data in Figure 1, there are significant regional disparities in the occurrence of computer information system destruction crimes across China. The developed eastern coastal regions, such as Jiangsu, Zhejiang, and Shanghai, have a relatively high number of cases, which may be related to their higher levels of economic development and informatization. On the other hand, the central and western regions have fewer cases, which may be linked to the local application and popularization of information technology.

This regional distribution characteristic is of great significance for understanding and preventing the crime of computer information system destruction. Relevant policy development and law enforcement efforts need to consider regional disparities, strengthen the popularization of

information security awareness and the construction of technical protective measures, especially in economically developed regions with a high concentration of information technology. Additionally, for relatively underdeveloped regions, it is also necessary to improve regulatory and response capabilities to prevent criminals from exploiting vulnerabilities in these areas to commit criminal activities.

### 3.2. The trial level, time distribution, and number of cases of the incident

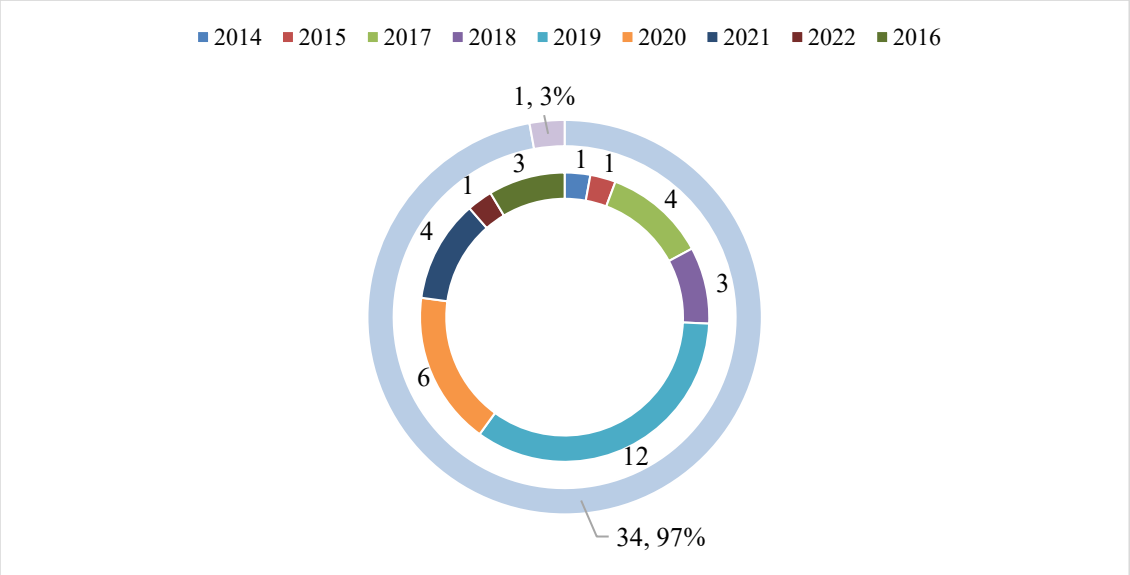


Figure 2 Trial level, time distribution and number of cases of destroying computer information system crime

According to the statistical data in Figure 2, the number of cases of computer information system destruction crimes fluctuated from 2014 to 2022. There was only one case in 2014, followed by slight fluctuations in the number of cases until a peak of 12 cases was reached in 2019. After that, the number of cases showed a downward trend, dropping to one case in 2022. Overall, the number of cases increased year by year until 2019 and then decreased annually, indicating that there may have been fluctuations in the crackdown efforts and social attention towards this type of crime during specific periods.

From the perspective of court trial levels, the vast majority of cases were handled at the first instance stage, with only one case in 2016 reaching the second instance stage. This suggests that first-instance courts play a dominant role in dealing with such crimes and reflects that computer information system destruction cases often have relatively clear rulings at the first instance stage, rarely progressing to the second instance.

By analyzing the number of cases and the levels of trial courts in chronological order, it is possible to observe clearly the trend in the development of computer information system destruction crimes and the usual procedures for courts to handle such cases. In particular, the significant increase in the number of cases in 2019 may indicate an increase in the use of destructive programs in computer information systems during that year, or intensified crackdowns by the police and judicial authorities, or a deepening of social awareness of such crimes.

## 4. Judicial practice of determining destructive procedures

The so-called computer virus refers to a type of computer program that can repeatedly self-replicate and proliferate during the operation of a computer system, endangering the normal functioning of the computer, wasting system resources, and damaging stored data. Such programs can generally gain system control at appropriate times to exert their various functions.

Destructive programs are not limited to computer viruses, but computer viruses are the most common, typical, and extremely harmful type. Article 5 of the "Interpretation of Several Issues

Concerning the Application of Law in Handling Criminal Cases of Endangering Computer Information System Security" (hereinafter referred to as the "Computer Interpretation") issued by the Supreme People's Court and the Supreme People's Procuratorate clearly defines computer viruses and other destructive programs as those that can replicate and disseminate part or all of themselves, or their variants, through media such as networks, storage media, and files, and disrupt computer system functions, data, or applications; or those specifically designed to disrupt computer system functions, data, or applications that can be automatically triggered under pre-set conditions. The disruption caused by destructive programs to computer systems naturally originates from within the computer system because, to achieve their destructive effects, destructive programs need to operate within the computer system, while disruptive behaviors such as interference do not necessarily need to start from within the computer. Depending on the source of interference, it can be classified into two types: internal interference and external interference. In practice, the former is more common, that is, using the computer operating system to interfere and disrupt the system's normal data processing functions from within the system, with common methods such as DDOS attacks and maliciously occupying system resources to paralyze the target server. The fundamental attribute of destructive programs is their destructiveness. As mentioned earlier, computer viruses are enormously harmful. As a representative of explicitly enumerated destructive programs, legally recognized destructive programs should possess destructiveness comparable to that of computer viruses, which is also clarified in judicial interpretations. However, when identifying destructive programs in judicial practice, it is important to distinguish between two levels: the technical level and the legal level.

### 4.1. The constitutive characteristics of the crime of producing and disseminating computer destructive programs

This crime refers to the deliberate creation and dissemination of destructive programs such as computer viruses, which affect the normal operation of computer systems and have serious consequences. Its main constitutive characteristics are:

1) The subject of this crime is a general subject, but specifically speaking, in terms of creation behavior, the perpetrator is often a technician who has received higher education, especially in computer science. In terms of dissemination behavior, it can be any natural person.

2) Deliberate subjective aspect. Negligence cannot constitute this crime.

From actual cases, the motives for perpetrators to create and disseminate destructive programs such as viruses generally include the following:

Firstly, deliberately creating destructive programs such as viruses, which is the most common form of creation and dissemination behavior.

Secondly, revenge. For example, an engineer from a computer company in China once created a virus program to retaliate against the company for unfairly dismissing him, causing severe damage to the company's computer system.

Thirdly, illegal copying, that is, creating viruses as a punishment to prevent others from unauthorized copying of files and programs. The initial computer viruses originated from this.

Fourthly, unfair competition. Specifically, there are two manifestations of creating and disseminating computer destructive programs for this purpose. One is to use destructive programs such as viruses to destroy competitors' computer system data files. For example, a Japanese company once used middle school computer enthusiasts to study computer viruses to plot against Sharp. The second is to use destructive programs such as viruses to expand its sales market. It has been discovered domestically that some people use the sale of computer virus prevention and treatment products for this purpose.

3) The objective aspect is manifested as the creation and dissemination of destructive programs such as computer viruses, which affect the normal operation of computer systems and have serious circumstances.

### 4.2. Practical cognizance standard of the crime of making and disseminating computer destructive programs

Regarding this crime, besides whether serious consequences have ensued, the key issue in distinguishing between guilt and innocence lies in determining whether the program created and disseminated by the perpetrator is a destructive program, especially in distinguishing and identifying destructive computer viruses.

Based on the intentions of computer virus designers and the impacts of virus programs on computer systems, computer viruses that have been discovered can roughly be classified into two categories:

Firstly, viruses with obvious destructive capabilities, destructive purposes, or destructive targets. Such viruses are highly destructive and dangerous. The most common malicious viruses can eliminate or modify data, delete or alter files, or reformat disks, potentially disrupting the normal operations of a large computer center or paralyzing a computer network, leading to disastrous consequences. These types of computer viruses clearly belong to the category of destructive programs. Creating and disseminating such viruses with serious consequences certainly constitutes this crime and the perpetrators should be held criminally responsible.

Secondly, dramatic viruses such as the IBM virus, which makes the computer system display greetings and other images on the screen, or the Mathematician virus, which forces computer users to solve math problems by displaying them on the screen during startup. These types of viruses have minimal or no impact on other aspects of the computer system besides consuming some system resources. Some people refer to these types of computer viruses as "benign viruses." Due to their non-destructive nature, these viruses, despite being categorized as computer viruses, do not belong to the category of destructive computer viruses referred to in this crime but are instead non-destructive programs. Therefore, creating and disseminating such viruses does not constitute this crime.

However, it should be noted that since any benign virus consumes some system resources and is an unauthorized intrusion into the computer system, creating and disseminating such non-destructive viruses may not constitute this crime but may still constitute other crimes. The behavior described in this objective aspect is the creation and dissemination of computer virus destructive programs. Thus, the scope of destructive programs is broader than that of computer viruses, which are only one of the main manifestations of destructive programs, and there are numerous other forms as well.

## 5. Conclusions

As the application of computers becomes increasingly widespread and socialized worldwide, computer crimes are rapidly proliferating. Computer crime has become a major social issue faced by both developed and developing countries. Among various computer crimes, the crime of creating and disseminating destructive programs with computer viruses as the mainstay is gradually revealing its destructiveness and serious social harmfulness. Currently, there are many controversies surrounding the crime of creating and disseminating computer viruses and other destructive programs, with relevant legislation being neither comprehensive nor reasonable and operable. Complicated phenomena in judicial practice also pose many difficulties in convicting and punishing crimes involving the creation and dissemination of computer viruses and other destructive programs. Destructive programs should arise from the intentional intent of malicious destruction. In contrast to the behavior of damaging computer information systems stated in the first two paragraphs of Article 286, the legal provision explicitly stipulates that the creation and dissemination of computer viruses and other destructive programs must be intentional. This is because destructive programs represented by computer viruses are quite difficult to create and generally require intentional creation by the perpetrator. Therefore, the regulated behavior of creating destructive programs in this provision must be intentional. Although there may be cases of negligence or accidents in the dissemination of destructive programs, such negligence or accidents causing the dissemination of

destructive programs do not constitute destructive behavior as stipulated in Paragraph 3 of Article 286 of the Criminal Law. That is, such cases are not punished as the crime of damaging computer information systems. Therefore, destructive programs should be specifically designed and created for the purpose of damaging computer resources. Destructive programs refer to computer programs that can remotely control or automatically operate to damage, tamper with, delete, etc., computer information systems. These programs may include viruses, trojans, worms, and others. Comprehensive considerations must be given to relevant laws and regulations, technical countermeasures, user education, and other aspects. Enhancing users' security awareness and knowledge of network security is also crucial.

## References


[1] Peng Zhang, Lihui Yin. Rule of Law Weekend [EB/OL]. (2024-01-17) [2024-02-05]. https://mp.weixin.qq.com/s/vMC-aK5h-6OThEL0iy-Gxg.

[2] Huachi Zhu. On the main characteristics of the crime of making and spreading destructive computer programs such as computer viruses [J]. Law Review, 1999,(05):108-112.

[3] Hao Jiang, Zhigang Yu. On the crime of making and spreading destructive computer programs [J]. Jurist, 1997,(05):18-24.

[4] Xinghua Xu, Xin Liu. Analysis of the crime of making and spreading computer viruses and other destructive procedures [J]. Journal of Yunnan Police College, 2003,(04):74-77.

[5] Yan Yan, Li Wei. Qualitative behavior of spreading Trojans [J]. Information Network Security, 2009,(11):14-15.

[6] Tingguang Zhao, Huachi Zhu. Determination of the crime of making and spreading computer viruses and other destructive programs [J]. Information Network Security, 2005,(10):44-45.

[7] Daocui Sun. Characterization of the behavior of implanting destructive programs into mobile phones and making illegal profits [J]. China Prosecutor, 2015,(14):45-47.

[8] Yan Li, Meiwen Ouyang, Hang Zhang, Qianli Yang, Jun Shen, Hui Huang, Xiaohuan Ruan, Shizhuo Zhang, Min Li, Guopeng Liu. Shanghai Venus Information Technology Co., Ltd., Common destructive program analysis and evidence collection system [Z]. Appraisal date: March 10, 2005.