On the Criminal Regulation of DNS Hijacking

Jin Liu [1, *, †], Ran Wu[2, †], Aolin Zhang[3, †], Jingwen Zhang[4, †]

[1] Law school, Tongji University, Shanghai, 200000, China.
[2] Law school, Dalian Maritime University, Dalian, 116000, China.
[3] Law school, Nanjing University of Science and Technology, Nanjing, 210094, China.
[4] International Law school, East China University of Political Science and Law, Shanghai,200000, China.

*Corresponding author. Email: 2141630@tongji.edu.cn
†These authors countribute equally.

ABSTRACT. In judicial practice, the conviction of DNS hijacking has been highly controversial. The relevant crimes of this act mainly include the crime of illegally controlling computer information systems, the crime of destroying computer information systems, the crime of theft, etc. However, the distinction between "illegal control" and "destruction" is not clearly defined in the Chinese Criminal or in related judicial interpretations. There are still no uniform rules on whether "Traffic" can be considered as a form of property. These all are important issues that affect the conviction of DNS hijacking. Therefore, it is necessary to set a unified criminal control standard for the identification of this act. By distinguishing between different subjective purposes of DNS hijacking and different functions of the means of hijacking, it is easy to identify "illegal control" and "destruction". Meanwhile, by reasonably considering "Website Traffic" as a "property", the act of DNS hijacking could also be regulated by the crime of theft. Therefore, DNS hijacking constitutes both the crime of theft and a corresponding computer-based crime. According to the Chinese Criminal, this is an imaginary competition, and it should be punished as a felony.

Keywords: DNS hijacking, Illegal control, Website Traffic, Computer information systems crime.

1 INTRODUCTION

With the continuous development of the network economy in judicial practice, the proportion of network crimes has gradually increased. Among them, Traffic Hijacking with DNS hijacking accounts for a large proportion. Its power is particularly rampant. This type of crime is novel and special. The criminal methods are flexible and diverse while China's Criminal Law and related judicial interpretations have not yet clearly and uniformly defined the standards for the behavior. The Criminal Law research on the relevant links of Domain Name Resolution Traffic Hijacking is rare in theoretical circles. There are often many problems in judicial practice. For example,

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 3180–3194, 2022.
https://doi.org/10.2991/978-2-494069-89-3_366

there are different judgments in the same case, unclear criteria for criminalization, and insufficient reasoning for judgments.

DNS hijacking (domain name hijacking) is a way of an Internet attack, by attacking the domain name resolution server (DNS) or forging the domain name resolution server (DNS). The target website domain name is resolved to the wrong IP address to let the user cannot access the target website or requiring the user to access the specified website.

By using DNS hijacking, criminals can hijack the website traffic and take it as a key indicator of website profitability. The increasing number of DNS hijacking behaviors seriously threatens social order and economic development. The increasing economic burden of DNS hijacking on society has prompted people to reflect on the insufficient strength of their legal norms and promote the improvement of Criminal Law norms in regulating Traffic hijacking.

Starting from the two aspects of the identification of "illegal control" and "Traffic" attributes, this paper uses empirical analysis and comparative research methods to analyze the different convictions that often occur in cases of DNS hijacking in judicial practice. This essay also clarifies the legal attributes of "Traffic Hijacking" and propose solutions. At the same time, this paper makes suggestions on the criminal legal system and application of "Traffic Hijacking" from the legislative and judicial levels. These suggestions can better position it in the legal sense and avoid the phenomenon of confusion in its characterization in judicial practice in the future, which is conducive to maintaining the credibility of judgments.

At present, there is not much theoretical research on the identification of these two attributes. The definition of illegal control of computer information systems is even less involved. According to the Explanation of the Provisions, Legislative Reasons, and Relevant Provisions of the Criminal Law of China, illegal control means the use of various techniques to enable others' computer information systems to be under the control of the perpetrators. Professor Ye Liangfang believed that there was a phenomenon of interleaved coexistence between "illegal control" and "destruction". This view is developed in detail in his article. [1] Meanwhile, he further analysed and classified these two behaviors.

The current academic community is relatively well-researched on the properties of network traffic. However, there is a paucity of research on the website traffic involved in DNS Traffic Hijacking. Most scholars currently only include network traffic in network virtual property such as "How to apply the law to the theft of virtual property such as ‘Traffic packs’" written by Zhao Wensheng, Liang Genlin, Qu Xinjiu. [2] There is also controversy in the academic community as to whether network virtual property is property.

2 THE DISTINCTION BETWEEN "ILLEGAL CONTROL" AND "DESTRUCTION" IS UNCLEAR

The legal provisions of Chinese Criminal and the relevant judicial interpretations do not identify the standard and degree of "illegal control". There has been little discus-

sion in academic circles about the criteria for distinguishing between 'illegal control' and 'destruction', or even the logical relationship between the two. In the case of DNS hijacking, criminals often modify domain name resolution servers or force users to bounce their visits to other web pages. Dose this kind of behavior disable a computer information system and make it unable to function properly? Or does this behavior illegally control a computer information system? The answer to the question is unclear, which leads to different convictions of the act of DNS hijacking in practice. For example, in the case of Shi Shuo et al. [3] and in the case of Li Binglong, [4] the defendants both modified the DNS resolution system to make network users forcibly jump to a designated website when they visited the hijacked website, and finally achieved Traffic hijacking. However, the defendants in the two cases constituted different crimes. In the case of Shi Shuo et al., the defendants modified the configuration files of the DNS to achieve Traffic hijacking. In the judgement, they were deemed to have illegally taken control of a company's computer information system. While in the case of Li Binglong, the defendant obtained the service management rights of the DNS by deception. By registering an account on a web platform providing domain name resolution service, he automatically generated a partial DNS resolution list of the second-level sub-domains of the well-known website. Then he illegally changed the IP pointing of the sub-domains of the website, making the website not operating normally. In the judgement, he was deemed to illegally destroy a computer information system.

The literal meaning of "illegal control" in the crime of illegally controlling computer information systems should be that making other's computer information systems under its control through various technical means, to complete some operational activities. According to Article 286 of the Chinese Criminal Law, the behaviors of "destruction" in the crime of destroying computer information systems include deletion, modification, addition, or interference with the functions of a computer information system, or the deletion, modification or addition of data and applications in a computer information system. In actual cases, the criminals' behaviors of "illegal control" of computer information systems often contain the "destruction" of computer information systems. The lack of clear criteria for distinguishing between the two often leads to ambiguity when it comes to convictions.

3 THE ISSUE OF TRAFFIC ATTRIBUTES IS ILL-DEFINED

There have been no convictions for theft in the current cases relating to DNS hijacking. However, in order to implement the principle of statutory penalties, we must consider the possibility of using theft and fraud to regulate Traffic hijacking. Furthermore, there are still many views in the theoretical community that DNS hijacking will constitutes theft.

On whether DNS hijacking constitutes a property crime such as theft, whether the Traffic belongs to the "belonging" in Criminal Law, there are different views. Both theoretical and judicial circles have different opinions.

Some scholars believed that the Criminal Law does not provide that the "Traffic" in the Traffic hijacking behavior is property. The reason is that the Criminal Law does not provide for Traffic hijacking behavior in the "Traffic" belongs to the property. Theft must be established by the amount of the crime and the direct economic loss caused by the network subject cannot be calculated to the specific amount. [5] In addition, to establish the crime of theft also requires the transfer of possession, and the Traffic is not the reality of the existence, then it cannot talk about the crime of theft. It is difficult to classify it as a property crime, and it should be punished as a computer-related crime. [6]

In the judicial community, in the case of Fu Xuanhao and Huang Zichao [7], the Shanghai Pudong New Area People's Court held that computer-based crimes should be used to regulate them. The objective elements of the crime of damaging computer information systems are present because the hijacking of the DNS domain name system involves the modification, addition and deletion of information and data stored in a person's PC.

Other scholars held that the crime of theft should be applied to regulate the Traffic hijacking behaviour. The intrusion and damage to the computer information system by the wrongdoer is a means of stealing website traffic. Website traffic contains huge property interests that can bring economic value to Internet companies. In many cases, the perpetrators of Traffic hijacking are to obtain Traffic, and not intentional damage, intrusion into the computer information system. So hijacking behaviour causes the most harmful consequences is the loss of economic interests of website operators. [8]

In addition, the wrongdoer hijacked the Traffic and transferred it to the beneficiary website. The beneficiary website obtained the Traffic due to the hijacking, the object of the act has a unified nature, and therefore constitutes the crime of theft.

In conclusion, Traffic hijacking may have been recognized as a computer network crime in judicial practice. However, the legal interest which protected by computer network crime is the security of the computer information system, and Traffic hijacking often brings huge property losses to the victims. So many scholars are trying to use property crime to regulate Traffic hijacking. With the increasing number of DNS hijacking acts, the issue of identifying the properties of the Traffic should become one of the first tasks that needs to be addressed urgently.

4 EXPLORATION OF THE CAUSES OF THE PROBLEM

4.1 An overlap of the elements of the two crimes

There are aspects of "illegal control" and "destruction" that overlap in practice, and sometimes "illegal control" can be used as a means or manner of achieving "destruction". Likewise, "destruction" can be a means or manner of "illegal control". According to Article 286 of the Chinese Criminal Law, there are three main patterns of behavior in the objective act of the crime of destroying computer information systems.

The first main mode of conduct is to severely disrupt the functioning of a computer system to make it not function properly. The second is to severely damage the data and applications in computer information systems. The third is to disrupt the normal functioning of a computer by, for example, implanting a virus into the computer system. Any of these three modes of "destruction" can be used as a precursor or means to illegally control a computer information system. In practice, it is also very common to achieve illegal control of computer information systems by using the above methods.

For example, in the case of Chen Yefan et al. [9], the defendants hacked into the "paperless system" to illegally add medical check-up information of driving test students and illegally delete the blacklist information in the "paperless system". They were deemed to illegally control the computer information system and constitute the crime of illegally controlling the computer information systems. It is easy to find that the offense of "illegal control" by the act of "destruction" is still common in practice. At the same time, the act of "destruction" can also be a subsequent or consequential act of "illegal control". For example, after illegally obtaining the control of the computer information system, the criminal deletes the key data of the operating system, thus causing the computer information system to fail to operate normally and achieving the purpose of destroying the computer information system.

Due to the diversity of computer crimes, there is also a high possibility of overlap and nesting between the objective aspects of each crime elements. So, this has led to difficulties in convictions for DNS hijacking.

4.2 Lack of clarity in judicial interpretation

Some relevant judicial interpretations merely identify the results of "illegal control". There is a lack of provisions on how to constitute "illegal control". This point of view of the word means that "no matter what kind of action is taken, as long as it deviates from the control of the original controller, it can be regarded as illegal control."

According to paragraph 2 of article 285 of the Criminal Law, the crime of illegally controlling a computer information system can only be established if the circumstances are aggravated. The provisions are blank crimes, and the objective aspects of the composition of the crime are simply described as "the implementation of illegal control". Relevant interpretations only explain the "serious circumstances" stipulated in this paragraph. It does not make corresponding determinations and interpretations of the "illegal control" acts. The term "destroy" in the crime of destroying computer information systems is also set out in the legislation as a term with a rather broad connotation, which includes almost all forms of behavior that infringe on the functions, data, and programs of computer information systems. The crime of destroying computer information systems and the crime of illegal control of computer information systems are both broad offenses. The jurisprudence of various courts also lacks clear reasoning and criteria for recognition. There has not yet been a guiding case as a reference standard for the distinction between "destroy" and "illegal control". It has led to a situation where it is often difficult to distinguish between the two crimes in practice.

For example, in the case of Fu Genglin, [10] the defendant was deemed to have damaged the functions of another person's computer information system for illegal gain in the first trail. However, in the second trail, Fu Genglin was not considered to destroy the security of the victim's computer information system. He did not delete or modify the existing data or applications on the victim's computer system. His act of implanting advertisements on the victim's computer system website did not increase the advertising function of the computer website. It rather made use of the advertising function of the website and did not cause serious consequences. In this case, the objective conduct of the two offenses crossed over, thus leading to a competition of offenses. The keyword for the objective conduct under Article 286 is "destroy", but the determination of "destroy" is still relatively ambiguous. While "illegal control" also can be logically interpreted as an "act of destruction".

4.3 Reasons for the controversy over the issue of Traffic attributes

The nature of the Traffic itself.

Traffic itself is a virtual object, rather than a real thing. It is difficult to perceive and observe, difficult to measure in value, but at the same time undeniably valuable. So, the characterization of Traffic has always been controversial. On the Internet, Traffic (website traffic) is used to describe a range of data indicators related to the number of users visiting a website and the number of pages viewed by users. [11] Specifically, it is the total amount of Internet data generated by Internet users during their use of the Internet to experience Internet services. In the form of downloads of software, clicks on news or web pages, and the number of registered users of a website. It is virtual, disposable, economically valuable and transmissible.

The virtual nature of Traffic means that it is expressed and constructed in numerical terms from 0 to 1. [12] Traffic does not have the characteristics of material form. Traffic is incorporeal, does not occupy space, while physical goods must rely on a specific material entity and exist. Website traffic is the number of visits to the site, and the user's visit to the site is an action, and no physical form. Therefore, people cannot perceive and touch it directly. The disposability of Traffic is reflected in the management, control, and disposal of the platform by the platform company. The process by which a platform company "generates" Traffic revenue through the operation of that Traffic is evidence of the platform company's ability to manage and control that Traffic.

The transmissible of Traffic refers to the fact that web links can be redirected to each other. Law breakers can intercept Traffic from websites to their own servers and hijack it through various means. The economic value of Traffic is reflected in the fact that Traffic has become a form of profit for all Internet companies. The number of visitors to a website, the length of time users spends browsing, etc. all affect a company's business reputation and the marketing interests behind it. In today's world, where internet commerce is highly developed, more Traffic means more visibility, and therefore greater business benefits. The "virtual" nature of Traffic distinguishes it from "belonging" in the traditional sense of Criminal Law, but its disposability, trans-

ferability and economic value make it a certain "thing". It is therefore difficult to define the legal attributes of Traffic.

Lack of clear legal regulation.
China's Criminal Law follows the "law of crime and punishment", and the current Criminal Law system in China does not provide for the legal properties of Traffic. It is the root cause of the problem, although Traffic has property value, but the specific belong to what kind of property worth discussing.

China's Criminal Law and related judicial interpretations are vaguer about the identification of Traffic properties, lacking clear and unified regulations. For example, in the Research Office of the Supreme People's Court issued the Research Opinions on How to Qualify the Problem of Using Computer to Steal Others' Game Coins for Illegal Sales and Profits, the network data is protected as electromagnetic data. [13] For the act of using computer to steal others' game coins for illegal sale and profit, it should be recognized as the crime of illegal acquisition of computer information system data. However, in the relevant judicial interpretations in China, it uses network traffic as a criterion for identifying losses. Thus, making the Traffic a kind of legal benefit for protection.

According to the enumerated provisions of the 1998 Interpretation and the 2013 Interpretation on incorporeal objects, the "property" in Criminal Law is based on the principle of corporeal objects. This prevents the expansion of the understanding of incorporeal objects from leading to too broad a strike. Although Traffic has the attribute of "belonging", but because it exists in the virtual space of the network, is a kind of virtual property, it is different from the physical objects. It is also different from electricity, gas, and other inanimate objects, in judicial practice, many people believe that virtual property should not be protected as real property. The legal status of virtual property is not explicitly provided for in mainland China's Criminal Law. However, the bottom provision of "other property" in Article 92 of the Criminal Law provides room for Criminal Law interpretation of the specific existence of property. [14]

5 EXPLORATION OF REGULATORY PATHS FOR DNS HIJACKING

5.1 Clarify the conceptual issues of the two crimes

Distinguish with the help of the theory of the incompletely two-conduct crime.
In order to clearly distinguish between the crime of illegal control of computer information systems and the crime of destroying computer information systems, it is possible in practice to draw on the theory of the incompletely two-conduct crime, to determine in detail whether the perpetrator has a specific subjective purpose. The concept of the incompletely two-conduct crime generally holds that the purpose of a purpose offender can be divided into two categories. One of them can be achieved by the perpetrator committing the act of carrying out. The other one is achieved after the

perpetrator has carried out the act of implementation, but it also requires the perpetrator or a third person to finish other acts.

The main significance of the incompletely two-conduct crime is establishing rules of judgment to identify the particular purpose which was possessed by the perpetrator subjectively. This purpose will have a corresponding effect on the composition of the offense. For example, in the case of Fu Genglin, [10] who committed the crime of destroying the computer information system mentioned in the above reasons, according to the shortened theory of two acts of crime, the court should primarily focus on analyzing whether Fu had the subjective purpose of destroying the computer information system during the trial. In further analysis of the incompletely two-conduct crime, if there is more than one subjective purpose, it should be carefully examined to determine the "stage purpose" and the "final purpose" (the former one is for the latter one).

In conclusion, when judicial institutions distinguish between the crime of illegal control of computer information systems and the crime of destroying computer information systems, if this theory can be accepted, then they should take the subjective purpose of the perpetrator as the key point, usually, three results can be obtained.

First of all, the perpetrator has subjectively no criminal intent and criminal purpose. Then the actor's manipulation of the data cannot be found to constitute an offense even if the objective elements of the offense have been met. The second one is the perpetrator only has the subjective purpose of illegally controlling the computer. The perpetrator only uses the computer information system normally and dose not commit other acts further, constituting the crime of illegally controlling the computer information system. Furthermore, if perpetrator has the subjective purpose of both destroying and illegally controlling the computer, then the "controlling act" can be deemed to serve the "destroying purpose" and constitute the crime of destroying the computer information system.

The computer crime is a type of crime that requires the use of the functions possessed by computers to commit criminal acts and achieve criminal results. The act of computer technology itself has a "subjective and objective" quality that is emphasized in Criminal Law judgments. Judicial institutions can often recognize the subjective purpose of the perpetrator by evaluating the functionality of the program and tools, combined with the way the perpetrator used them.

Distinguish by the actual function of the hijacking means.

In practice, the behavioural patterns and technical means used by criminals for DNS hijacking are often diverse. Therefore, in order to accurately locate the crime of DNS hijacking, it can be distinguished and identified from the main functional aspects of the technical means adopted by the criminals.

Hijacking by "deception".

In practice, some criminals set up mirror servers, i.e., set up a server that can be controlled by themselves and is same with the regular server of the hijacked website (the two can maintain data interoperability). They used the mirror server to impersonate the regular server of the hijacked website and diverted the normal access requests and

eventually diverted the Traffic of the hijacked website to the server set up by the wrongdoers themselves. By this means, they obtained the authentication information sent by the user when surfing the Internet on that server. Then, by capturing the keyword segment of these authentication messages, criminals obtain the user's characteristic code to impersonate the user's identity to log into the regular website and illegally manipulate the user's account.

This type of hijacking is essentially a deceptive act. The function of setting up a mirror server is to impersonate the regular server of the hijacked website in order to achieve the illegal transfer of Traffic. This type of act does not add, delete, or modify the data or functions of the computer information system, nor does it produce any destructive procedures. Therefore, it is not a destruction to the computer information system Meanwhile, the mirror server is set up independently of the hijacked computer information system, and its function is mainly to impersonate and deceive, not to achieve control over the hijacked computer information system. For example, in the case of Chen Zhiyong et al. [15], Chen Zhiyong illegally set up a server in the backbone server room of a communication company. Then he mirrored the GET data on different ports of internet users in the backbone server of the communication company, making users access Baidu through an address with Chen Zhiyong's promotion ID. After that he captured the user's relevant data on the mirror server by the same means, which leads to some internet users were added to the specified group without their knowledge. The defendants' act of setting up a mirror server neither destroy nor control the computer information system of the company and the computer information system of Internet users. So, they could not constitute the crime of destroying computer information systems or the crime of illegally controlling computer information systems. However, their subsequent illegal access to the data of Internet users constituted the crime of illegal access to computer information system data.

Hijacking by "modifying settings.

In judicial practice, there are some criminals who spread malware, or use other means to illegally modify the domain name resolution settings in the computer information system. Then the hijacked Traffic will jump to the beneficiary website or jump to the server set up by the wrongdoers in advance and then jump to the beneficiary website.

This type of hijacking means in essence shows a destructive behavior, that is to destroy the original Domain pointers. This can make the system not operate normally, and finally achieve the illegal transfer of Traffic. The function of hijacking by means of "modifying settings" is mainly to destroy the domain name resolution settings of the normal computer information system, but not to control the hijacked computer information system. Therefore, this type of hijacking should be considered as the crime of destroying computer information system. For example, in the case of Fu Xuanhao and Huang Zichao, [7] the defendants used code to illegally change the DNS settings of Internet users' routers. When users logged on to some specific navigation websites, they just jumped to another navigation website, which was set up by the defendants before. The defendants used this way to force internet users to visit specified websites and achieve Traffic hijacking. But it neither issue other instructions to the computer information system of the users nor control and manipulate the comput-

er information system of the users. Therefore, this type of hijacking should constitute the crime of destroying computer information systems.

Hijacking with "administrator rights".
This type of hijacking refers to the behavior that the administrator of the network service provider (who may be a co-offender or may be used by deception) uses his authority to modify the domain name resolution server of the service provider without authorization in order to achieve Traffic hijacking.

This type of hijacking is essentially an act of "illegal control. In this case, the administrator's authority itself is legal, which means that it enjoys a certain control over the infringed computer information system. The criminals utilized this permission, and make this authority operate without or beyond the original authorization, which constitutes an illegal act. The function of hijacking with "administrator rights" is mainly to illegally obtain the "control" of the infringed computer information system. If actors only use "administrator rights" to hijack the Traffic without destroying the computer, it should constitute the crime of illegally controlling computer information systems. For example, in the case of Shi Shuo et al., [3] Shi Shuo was an employee of the core platform department of a company's network monitoring and maintenance center, and he used the convenience of his position to access the company's DNS system and implement DNS hijacking. As Shi Shuo himself has a certain "control right" over the infringed computer information system, he used his "administrator rights" to enter the relevant system and made certain modifications, making the original legal "control right" into illegal "control right", which should constitute the crime of illegally controlling computer information systems.

5.2 Recognizing ‘Traffic' as belonging to better regulate crime

There is a lack of research on the characterization of Traffic in DNS Traffic hijacking, both in academic and judicial circles. Compared to that, there were many mature discussions and research on whether "network virtual property" is "belongings". If the reasonableness of "Traffic" belonging to "network virtual property" can be argued, then "Traffic" will also be considered as "belongings". This route is described in detail below.

Traffic is network virtual property.
The term "network virtual property" itself is not derived from legal writings or legal texts. So, it is not a strict legal concept, but rather a collection of objects with common characteristics. [16] Virtual property is both intangible and exclusive. Intangibility is the distinction from traditional property and exclusivity is the distinction from intellectual property. [17]

It can also be regarded as a relatively independent and exclusive information resource that exists in digital form. There is not yet a broad consensus among scholars on the concept of network virtual property itself. Most of these definitions are still

descriptive. Because neither electromagnetic record, data resources nor exclusive acts of service directly reveal the legal properties of network virtual property.

In contrast to Criminal Law, which currently has no wording like that of online virtual property, civil law has made a breakthrough, but it is not a complete solution. The Civil Code makes a distinction between data and online virtual property in the chapter on civil rights. What is more, the arrangement of the chapters also shows a certain empowerment of them. Article 127 of the Civil Code formally uses the concept of "network virtual property", which at least serves to reduce disputes in the name. However, the provisions on virtual property in the Civil Code are suggestive and consequential in nature and lack further definition of the concept. The definition of virtual property on the Internet is the characteristic of the times. When defining virtual property on the Internet, the academic community often adopts a non-exhaustive list to avoid heated disputes over the definition.

The mainstream category of network virtual property includes "Traffic", [2] but it should be noted that "Traffic" here refers to network traffic. Broadly speaking, Traffic is divided into website traffic and network traffic. [11] Network traffic is generally defined as Internet Traffic that an Internet user pays a price for from a network operator. Network traffic is the pass to the Internet service that the user receives from the network operator for a price. In simple terms, it is the data experience of a user's mobile device or PC accessing the Internet by paying the operator providing the communication service. The result of Traffic hijacking is that the Internet user is forced to visit another website when they originally wanted to, or to visit a website while accessing other website content. For the owner of the network traffic, i.e., each of us Internet users, Traffic hijacking simply infringes on the user's right to make their own choices about Internet services. No matter which website is visited, the corresponding network traffic will be consumed, but the property value of this network traffic is very small. So, the discussion of the Criminal Law protection of the act of Traffic hijacking with the network traffic as the object of the act does not have obvious practical significance. The social harm is too small to be adjusted by Criminal Law. As a result, the "Traffic" discussed in the act of “Traffic hijacking”, does not refer to network traffic, but the website traffic.

Website traffic is not included in the current mainstream categories of network virtual property. However, the incomplete enumeration approach adopted by the academic community in defining network virtual property means that website traffic is not necessarily virtual property. On the contrary, it can be included in the category of network virtual property through interpretation. As mentioned above, website traffic is virtual, disposable, transitory and economically valuable, and it fits perfectly into the characteristics of network virtual property. [18] This makes it should be considered as belonging to network virtual property. The question "whether website traffic is ‘belongings’" is then transformed into the question "whether network virtual property is ‘belongings’".

The legal interests protected by crime against property allow virtual property to be recognized as belongings.

On whether virtual property belongs to the "belongings" protected by property crimes in Criminal Law, this point has a strong tendency in the current theoretical circles. The discussion is also more in-depth, with most scholars holding the affirmative view. Some scholars argued that virtual property is property from the same characteristics of the two, but this is inappropriate. "Belongings" is a legal concept clearly in the provisions of the Criminal Law. It is not an open concept like network virtual property, the characteristics and constitutive requirements must not be confused. However, it is possible to explore the rationality of this concept in the light of the legal interests to be protected by property crimes.

Traffic hijacking has been recognized as a computer network crime. However, the legal interest protected by computer network crime is the security of the computer information system, Traffic hijacking often brings huge property losses to the parties. The legal interest protected by a property offence is property. The essence of infringing upon the virtual property of network is infringing upon the property legal interests of the property owners behind the virtual property of network. The protection path of crimes against property can fight crime to restore the victim's property losses. It is also in line with the purpose of the Criminal Law to protect the legal interests of the property owner's rights. At the same time, with the formal introduction of the Civil Code, the legal basis for the protection of virtual property has been clarified. Although the role of Criminal Law and civil law in the unified legal system is not the same, after all, there is also overlap and crossover. The civil law has included network virtual property in the scope of protection, Criminal Law is subordinate to civil law. According to the principle of consistent evaluation, Criminal Law protection scope should also include network virtual property. Therefore, it becomes the object of independent protection of legal interests of Criminal Law. It means that the infringement of virtual property is equivalent to the infringement of general property with.

In judicial practice, civil disputes over virtual property and criminal offences are often entangled together. In contrast to Criminal Law circles, civil law circles have conducted more in-depth discussions on how to deal with virtual property in from the properties of property and the properties of rights. According to Chinese civil law scholars, virtual property is different from real material wealth. Because it does not exist in real physical space and cannot be expressed in terms of real-world measurements, weights, and measures. Therefore, it does not belong to physical and tangible things. However, virtual property has the specificity and independence of property, and therefore virtual property should be defined as incorporeal. In our national law community, there is no dispute that virtual property is defined as property, but only the legal attributes of virtual property are in dispute. This controversy is reflected in the handling of cases in judicial practice. However, if the principle of consistency between civil and Criminal Law is adhered to, it is perfectly logical that virtual property is interpreted as property in Criminal Law. What's more, in Chinese law, property itself is a more abstract legal concept. The interpretation of virtual property as belongings does not break the boundary of the possible semantics of belongings.

The legitimate interests of citizens can be better protected if judges apply this perspective in judicial practice. From the perspective of the point of measuring penalty, the point of measuring penalty of computer network crime is high, need to reach "se-

rious consequences" or "serious circumstances". According to the judicial interpretation, the illegal gains need to than 5000 yuan or cause economic losses of more than 10,000 yuan. This will lead to many dangerous acts that cause damage to citizens' property cannot be regulated by Criminal Law. In comparison, the point of measuring penalty for property crimes is lower, when the value of the property is more than 1000 yuan, it can be regulated by the larceny. If the Traffic hijacking can be regulated by property crimes, it will be more conducive to combating crime and protecting the civil rights and interests.

6 CONCLUSION

In recent years, Internet technology has been constantly developing and progressing, and new technological advances bring new issues of rights and interests protection. The virtualized, digital character of the new property of the Internet widely affects all areas. The emergence and continuous improvement of cyberspace has caused changes in the social structure of the real world. Therefore, the study of new types of objects is a common mission of various legal disciplines. The study of these new types of objects is a common mission of various legal disciplines. Many domestic scholars have given their own views on the characterization of DNS hijacking. Among these views, the unclear determination of the attributes of "illegal control" and "website traffic" has led to different convictions in judicial practice regarding DNS hijacking. The author discussed and analyzed the reasons for the lack of a clear distinction between "unlawful control" and "sabotage". The author proposed to be guided by the theory of "completely two-act crime" and to distinguish by the actual function of the hijacking means. In addition, the author analyzed the properties of Traffic by collecting relevant legal literature. The author also organized specific judicial cases and sorted out the theoretical research results of domestic scholars. The author has also proposed the view that website traffic should belong to network virtual property, and then transformed the problem and proposed solutions. The author believes that theft and computer-type crime constitute an imaginative joinder offense. By analyzing DNS hijacking cases in judicial practice, the author clarified the legal attributes of "Traffic hijacking" and proposed measures to solve the problem. Suggestions were also made on the Criminal Law regulation and application of "Traffic hijacking" from the legislative and judicial levels. It can better position the legal meaning and avoid the confusion of its characterization in future judicial practice, which is conducive to maintaining the credibility of the judgment.

It is still a difficult issue to assess the value of website traffic as a network virtual property, and its value is difficult to be judged by representation.

7 REFERENCES

1. L.F. Ye, The nature of Traffic hijacking from the perspective of Criminal Law dogmatics, in: Zhongzhou Academic Journal, vol.08, 2016, pp:45-49.

2. W.S. Zhao, G.L. Liang, X.J.Qu, X.X. Zhang, X.H.Dong, Xin Luo, X.H. Wu, Yang Zhao, How to apply the law to the theft of virtual property such as "traffic packets", in:People's Procuratorial Semimonthly, vol.04, 2014, pp:41-46.
3. Yubei District People's Procuratorate of Chongqing City. v. Shi Shuo and others Crime of Illegal Control of computer information system, Yubei District People's Court of Chongqing City Case No. 00666(2015), November 11, 2015.
4. Xuhui District People's Procuratorate of Shanghai City.v. Li Binglong Crime of Destroying Computer Information System, Supreme People's Procuratorate Guidance Case No. 33, October 12, 2017.
5. Jun Li, Y.L. Bai, Lei Shi, Understanding and Reference to the Case of Fu Xuanhao and Huang Zichao on Damaging Computer Information Systems - Criminal Judicial Determination of DNS Hijacking-type Traffic Hijacking, in: People's Judicature, vol.17, 2021, pp.90-94, DOI: 10.19684/j.cnki.1002-4603.2021.17.021.
6. Y.T. Li, On the Criminal Characterization of Stealing Internet Virtual Property, in: Shanghai Jurisprudence Research, vol. 23, 2021, pp. 203-212. DOI: 10.26914/c.cnkihy.2021.061749.
7. Pudong New Area People's Procuratorate of Shanghai City. v. Fu Xuanhao and Huang Zichao for Damaging Computer Information System, Supreme People's Court Guiding Case No. 102, December 25, 2018.
8. Te Zhang. The Criminal Law regulation of domain name resolution Traffic hijacking, Zhongnan University of Economics and Law, 2020.
9. Dantu District People's Procuratorate of Zhenjiang City, Jiangsu Province v. Chen Yefan, Chai Jianping, etc. Illegal Acquisition of Computer Information System Data and Illegal Control of Computer Information System Crime, Dantu District People's Court of Zhenjiang City, Jiangsu Province Case No.226(2021), November 19, 2021.
10. Danzhou City People's Procuratorate of Hainan Province. v. Fu Genglin for Damaging Computer Information System Crime, Hainan Second Intermediate People's Court Case No.74(2017), April 17, 2014.
11. H.R. Niu, Criminal regulation of Traffic hijacking, Central China Normal University, 2019.
12. J.R. Li, On Legal Protection of Flow Property Righting, Hebei University of Economics and Trade, 2017.
13. Wen Wang, Criminal Law protection path for game gold coins, in: Journal of Changsha Social Work College, vol.25, 2018, pp:51-54.
14. Yong Wang, Study on Criminal Identification of Criminal property of virtual property, in: Criminal Law Review, vol.01,2017, pp:65-95.
15. Shapingba District People's Procuratorate of Chongqing City. V. Chen Zhiyong, Wang Xing, etc. for Illegal Acquisition of Computer Information System Data and Illegal Control of Computer Information System, Chongqing First Intermediate People's Court Case No.575(2016), August 22, 2017.
16. L.B. Xu, The doctrinal unfolding of virtual property crimes, in: Jurist, vol.04, Renmin University of China Law School Press, 2017, pp.44-57+176, DOI: 10.16094/j.cnki.1005-0221.2017.04.004.
17. David Nelmark, Virtual Property: The Challenges of Regulating Intangible Exclusionary Property Interests Such as Domain Names, in: Nw. j. tech. & Intell. prop, vol.3, Chicago, US,2004.
18. Nuo Xu, Qualitative study on the act of stealing online virtual property, East China University of Political Science and Law, 2019.