Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231218

Criminalisation of Traffic Hijacking and the Way Forward for Regulation

Mingxin Xu[1,a,*]

[1] *Faculty of Social Sciences and Law, University of Bristol, Bristol, BS8 1QU, The United Kingdom*
a. ra22623@bristol.ac.uk
**corresponding author*

Abstract: Traffic hijacking is an act of unscrupulous elements using the network chain for profit. From the process of intruding into the system, obtaining information, controlling the computer, damaging the computer system, to helping the information network crime, Internet enterprises have incurred huge economic losses in the traffic hijacking crime. The characterisation of traffic hijacking in current judicial practice is controversial. This paper examines the dilemma of traffic hijacking behaviour identified in criminal law doctrine and judicial practice, analysing the definition of different infringements, the legal interests infringed and the harm caused; Determining the necessity of identifying and regulating acts from the perspective of behavioural science and social harm, considering the prerequisites for identification and identifying the justification of acts; By organising and classifying the offences and cases, distinguishing cyber crimes from traditional criminal law offences, and analysing the judgments, it can provide a consistent characterisation of traffic hijacking in terms of culpability and punishment; Lastly, the system of regulation of traffic hijacking will be constructed in the direction of protecting the legal interests of data, taking domestic and international experience as a guide and combining it with technological governance.

Keywords: traffic hijacking, criminal law, data security

1. Introduction

Traffic hijacking refers to any “Attackers use technical means to illegally intercept, modifies or controls the Internet access of a user by technical means, so as to induce the users to install Trojan horses and obtain user data” [1]. The essence is the technical contact through the technical means or the commercial model, so that the network traffic which should belong to others is forced to traffic into the specific object and has the situation of irregularity. That is to say, the actor deceives the users into the specific target website to increase the number of visits and transactions. Traffic hijacking is not established if the user knowingly and with the permission of the perpetrator makes changes to the network.

Based on the traffic loss link of traffic hijacking, it can be divided into terminal hijacking, link hijacking and server hijacking. Depending on the different effect of traffic hijacking, it can be divided into access hijacking, back hijacking and advertisement hijacking. According to different methods of traffic hijacking, traffic hijacking can be distinguished into mandatory traffic hijacking and non-mandatory traffic hijacking. According to the severity of traffic hijacking, traffic hijacking can be classified as black traffic hijacking and grey traffic hijacking [2].

DOI: 10.54254/2753-7048/17/20231218

Along with the introduction of the Administrative Measures for Data Security in the Field of Industry and Information Technology (for Trial Implementation) in December 2022, the importance attached to network data is evident on the basis of Data Security Law of the People's Republic of China and Data Security Law of the People's Republic of China. As of April 19, 2023, there are a total of 55 cases on traffic hijacking in China Judgments Online. Of these, 10 are criminal cases and 44 are civil cases. Based on the search results in the database, it appears that the case has a wide scope of impact and the amount of damage is substantial. The crime of traffic hijacking has become an important challenge to maintaining cyber security, and due to the limitations of its civil remedies and administrative regulation, criminal definition of traffic hijacking is a necessary step to strengthen cyber regulation. On 1 November 2015, the Shanghai Pudong New Area People's Court decided the first criminal case of traffic hijacking in mainland China, with Fu A and Huang A "DNS hijacking". This was the first case in China in which traffic hijacking was convicted. Previously, such cases were mostly dealt with as unfair competition cases, and similar criminal cases since then often have different sentences for the same case. After that, Chongqing Yubei District People's Court and Shapingba District People's Court also issued two criminal judgments for "traffic hijacking", but the defendants were convicted of illegal control of computer information systems and illegal access to computer information system data. These two cases have caused controversy and extensive discussions in the academic community on the characterization of traffic hijacking. For the regulation of the crime of traffic hijacking, according to the existing adjudication documents and guiding cases, there are crimes of damaging computer information systems, illegal access to computer information system data, illegal control of computer information systems, suspected crime of theft, crime of fraud and so on, and different crimes need to be identified according to the nature of different acts.

2. The Dilemma of Determining Traffic Hijacking

The criminal law dogmatics regards criminal law as the only basis for interpretation and judgment, and the provisions of the current criminal law are both the object of interpretation and the basis for interpretation by scholars of criminal law dogmatics scholars [3]. Most of the current determinations of the crime of traffic hijacking rely on this selective crime. Simply using the legal interests of data property or uniformly adopting the same crime in different situations does not conform to the realistic direction of the adjustment of the criminal law data governance model.

Convictions limited to crimes such as "computer information system data" and "crime of assisting in criminal activities involving information networks "have neither truly effectively protected the legitimate rights and interests of rights holders nor effectively promoted the needs of social and economic development.

From the perspective of risk prevention and control, traffic hijacking also causes harm to many fields such as politics, economy, and military affairs. Taking personal specific information, certificates, mobile phone computer software, etc. as the object of the crime, the legal interests violated include national security, public security, citizens' personal and property safety, social political and economic management order, etc. "Although there is no harm to legal interests, as long as legal interests are threatened through dangerous behavior, the existence of criminal law can be affirmed"[4]. In the epidemic prevention and control, if someone uses traffic hijacking means to use the relevant data to commit a crime, the cost of time and economic cost for the government and citizens will be greatly increased, and public services will be restricted, which may bring serious consequences. Therefore, the refinement and regulation of the crimes of traffic hijacking is conducive to clarifying the boundaries of crimes, making the criminal law consistent with objective reality, and unifying legislative understanding.

DOI: 10.54254/2753-7048/17/20231218

2.1. Differences in the Legal Interests Infringed by Traffic Hijacking

Studying the legal interests violated by traffic hijacking is the prerequisite for confirming its crime. At present, there are mainly three views in the academic circle, which are to regard virtual property, network order, and system security as the legal interests violated by traffic hijacking.

Network virtual property is a kind of intangible property, which is a part of personal property [5]. Virtual property is an asset with economic value. Traffic hijacking violates data traffic, whether data traffic can be regarded as virtual property needs to be classified and discussed. Professor Dong Xiaohua believes that traffic requires telecom operators to invest in the initial cost and bring subsequent economic benefits, and has the corresponding measurement units measured by M and G. In this case, traffic should be regarded as property that can be sold for profit [6]. In addition, the object of traffic hijacking is the will-have traffic, and traffic hijacking cannot be established when the traffic is not in its initial state at the time of distribution. Will-have traffic is the act of a specific target, a website user who has a high degree of clarity of intent to access the services of a specific website, because the traffic hijacker's behavior will be the website should get the traffic for their own benefit. Taking virtual property as the object of traffic hijacking can provide a standard for the court to define the amount of property infringed, but if traffic is simply regarded as the object of crime, it cannot explain traffic hijacking that does not regard traffic as the real object of crime. This approach narrows the scope of criminal law protection and is relatively narrow in terms of criminal law interpretation.

The use of the network order as the object of traffic hijacking infringement is a mapping of the Internet space with as the real social order, which affects the real social order. In the real world, order relies on coercive and non-coercive means such as law, morality, custom and social opinion. In the virtual world of the Internet, the above means are not very useful, and the maintenance of order is more dependent on the guidance and supervision of real policies. The damage caused by traffic hijacking is often more serious than ever in the real world. Under normal network order, users of a website should arrive at the expected URL to obtain a specific network service in a normal functioning or good looking condition. If the system does not function properly, it also fits the description of" causing the computer information system to fail to operate normally" in the crime of destroy a computer information systems. The flaw in this doctrine is that it is impossible to measure the damage to legal interests caused by traffic hijacking. According to the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems, The penalty for serious consequences is "if the proceeds of the offence are more than RMB 5,000 or if the economic loss caused is more than ¥10,000" [7]. In judicial practice, especially in the case of transnational cybercrime activities, sentencing standards are not consistent according to the different characteristics of different regions, creating certain obstacles to the final trial and compensation [8].

Taking system security as the legal interest violated by traffic hijacking, the crimes related to computer crimes in the criminal law are mostly related to system security. Regardless of the crime, the purpose is to protect the stable and safe operation of the computer information system, and ensuring safe operation is a prerequisite for system operation. From this point of view, the act of intruding into a computer system itself creates a loophole in the computer defense system, and the biggest legal interest it infringes is the system security of the computer. But on the other hand, the act of hijacking traffic itself is an act of unfair competition. To a certain extent, it did not cause economic losses to Internet companies, which is one of the decisive conditions for measuring whether the perpetrator is subject to criminal punishment. However, the computer information system cannot operate normally, including not only making the computer information system

DOI: 10.54254/2753-7048/17/20231218

unable to operate, but also including failing to operate according to the original design requirements [9]. From this point of view, even if no economic loss is caused, data theft and other behaviors have brought serious security threats to users. Therefore, traffic hijacking will inevitably cause damage to the system to a certain extent.

2.2. Confusion Between Traffic Hijacking and Other Definitions

2.2.1. The Difference Between Traffic Hijacking and Data Traffic Theft

The early confusion was due to the fact that the term "traffic" has different meanings in different contexts, resulting in ambiguity between traffic hijacking and traffic or data theft. Generally speaking, stealing data traffic refers to stealing the amount of data purchased by individuals or companies from traditional operators for Internet access, that is, the number of bytes consumed by a web page on a terminal. For example, stealing the traffic of the operator or rubbing the Internet between network users. When the act of stealing data traffic reaches a certain amount, it can be characterized as the crime of theft. For example, in the 2013 case of "lawyer sued China Mobile for clearing traffic", the court of first instance held that "traffic is not a 'thing' but the measurement of services". Although the court of second instance upheld the original judgment, the judgment pointed out that "the Network data in units of bytes has the characteristics of objects and can become the object of infringement in this case" [10]. In this case, "flow" is more of a property in the legal sense, that is, a "thing".

2.2.2. The Difference Between Traffic Hijacking and the Use of Malware and Rogue Software

By definition, rogue software is forcibly installed and run on the user's computer or other terminal without explicitly prompting the user or obtaining the user's permission, and is used to track the user's online behavior and report the user's personal behavior to relevant Interest Groups [11]. These software can pop up advertisements to the user, modify the computer browser work bar and so on. Rogue software is forced to install and uninstall leftovers. This kind of behavior is for the purpose of advertising, and often does not affect the normal use of users and the safe use of computers. Malware, on the other hand, is designed to damage or destroy computers, servers, clients, etc. without the knowledge of the user. These two kinds of software can be roughly divided into adware, spyware, ransomware, Trojan horse virus and so on. Traffic hijacking is a technical means of controlling computers, and its behavior of intruding and hijacking browsers without the consent of users is intersecting with traffic hijacking.

3. Analysis of Legal Issues Related to Traffic Hijacking

3.1. Legal Characterization of Traffic Hijacking: Criminal Offences

3.1.1. Behavioural Perspective

Aiming at the boundary of the criminal law of traffic hijacking, some scholars believe that the type of link hijacking should not be criminalized. This type of traffic hijacking is an act of unfair competition and should be resolved by civil law or administrative law. However, the link hijacking actor also changes or destroys the data of the expected website or application program of the network user, and then guides the network user to enter the tab made by him. This behavior actually meets the requirements of the crime of destroy a computer information system.

DOI: 10.54254/2753-7048/17/20231218

3.1.2. Social Harm Perspective

According to the theory of the separation of binary subjects of cybercrime victims, the object of traffic hijacking should be "unspecified network users + specific Internet content providers" [12]. From the perspective of unspecified network users, the perpetrator changed the number of network users' background data or the number of computers to implement control behavior is the appearance of the impact of its behavior is established crime. Traffic is the element that connects network users and Internet content providers. Although the traffic is a benefit that will be obtained, it is still possible to determine the social harmfulness of the behavior by calculating the traffic obtained by the actor. That is to classify the degree of social harm through traffic statistics.

3.2. Factors to Be Considered

3.2.1. "Will-have Traffic" Is the Prerequisite for Determining Traffic Hijacking

When determining "will-have traffic", factors such as user's habits, psychological expectations, and Internet industry practices should be taken into account. "Will-have traffic" refers to the use of user habits and Internet business practices, Internet products or services providers for their products or services will be provided by the behavior of the prospective traffic [13]. Traffic hijacking is to divert other people's "will-have traffic" to the hijacker's name through technical means or business models, and the diversion behavior is improper.

3.2.2. Objectively Analyze Whether the Traffic Guiding Behavior Is Improper

Only traffic guidance behaviors that exceed the legitimate boundary are improper. Traffic competition is essential. When determining whether traffic guiding behavior is improper, the reasonable boundary of legitimate technical contact behavior should be considered. If it exceeds the reasonable boundary, it will be improper. The essence of judging by comparing the business models of other similar products, is to evaluate the behavior with reference to industry practices and general knowledge of the industry.

3.3. Analysis of the Criminalization of Traffic Hijacking

The current dilemma of traffic hijacking identification includes many aspects. The premise of conviction and sentencing in criminal cases is to accurately understand the subjective and objective facts of the case. In practice, on the one hand, electronic evidence is easily lost. In order to cover up the truth and avoid judicial investigation, criminals will destroy relevant documents and procedures, chat records and other key evidence [14]. On the other hand, there are various means of Internet hijacking, and the different means at different stages lead to different ideas of criminal law regulation for different cases.

4. Cases Illustrated

4.1. The Crime of Destroy a Computer Information System

Traffic hijacking is a highly typified criminal behavior that destroys computer information systems, and is mainly realized by modifying computer systems or data and applications in computer systems [15]. In 2014, the executives of Chengdu Gisu Technology Co., Ltd. violated state regulations and used hijacking codes to force network users to visit designated websites and modify, add, or delete data stored and processed in computer information systems; In 2017, Qingye Technology (Beijing) Co., Ltd. Mo A provided technical support and destructive programs. After the user executes the

DOI: 10.54254/2753-7048/17/20231218

bundled application, the user's Chrome kernel browser is hijacked and modified, and the user is prevented from changing it by himself. The company also developed traffic monetization software without authorization, and gave the company a share based on the number of advertisement clicks. In this case, the source code program involved in the case ran after the silent download and installation of a browser plug-in without the user's authorization, which is illegal control of the computer information system; However, a browser plug-in modifies the user's browser start-up page without the user's permission, against the user's will, which damages the original function of the user's computer information system [16]. The relationship between the two is the implication of means and ends, but the crime of illegal control a computer information system to evaluate the above-mentioned acts of the defendant unit is incomplete and incomplete.

In Guiding Case No. 102 of the Supreme Court, the two defendants leased multiple servers and used malicious code to modify the mutual DNS settings so that users would be redirected to other configured websites when logging in to a specific navigation website. Then sell the obtained Internet user traffic to the owners of the navigation websites that have been set up to obtain illegal income. All of these cases were ultimately convicted of the crime of destroy a computer information system. However, only relying on guiding cases to guide practice cannot fully evaluate traffic hijacking.

Therefore, traffic hijacking is carried out regardless of implanting software, malicious code, modifying browser configuration, installing browser plug-ins, or any other means. Therefore, traffic hijacking is carried out no matter by implanting software, malicious code, modifying browser configuration, installing browser plug-ins or any other means. As long as serious damage is caused to the computer system or the data and application programs in the computer system in other forms, it constitutes the crime of destroying the computer information system. Regarding the "unable to operate normally" in the clause, it shall be interpreted according to the purpose of legislation. It should not only be understood as extreme situations such as the inability of the computer information system to start or the inability to enter the operating system, but a state in which the collection, processing, storage, transmission, retrieval, and other functions of the computer information system cannot function normally [17]. In addition, the appropriate expansion of the interpretation of computer information systems and the expansion of the scope of criminal punishment may be based on the requirements of the development of the times, which does not substantially violate the basic principle of modesty in criminal law [18]. The damage to the data and application programs of the computer's external network access business is regarded as the damage to the computer system, in line with the trend of computer protection.

In judicial practice, the interpretation of case facts focuses on the analysis of "serious consequences". "Serious consequences" are the necessary conditions for incriminating the three behaviors listed in the crime of destroying computer information systems. For the consideration of "consequences", at this stage, the calculation is still based on the confirmation of property rights, that is, the illegal income used to sell Internet user traffic after hijacking is calculated.

4.2. The Crime of Assisting in Criminal Activities Involving Information Networks

Article 287b is of the Criminal Law limits the object of knowing, that is, "knowing that others use the information network to commit crimes", which is a general understanding. It is not necessary for the perpetrator to know the nature and type of crime being committed by the person being assisted, as long as he or she knows that the other person is using the information network to commit a criminal act.

In 2016, Dianzhuda Company, together with Shaanxi Xipu Company, obtained relevant telecom operators through the business channel of Xipu Company to use this authority to deploy a DPI program with relocation function on relevant servers. The redirection function of the

DOI: 10.54254/2753-7048/17/20231218

aforementioned DPI program was used by Chen A of Point Touch to parse and modify the packets received in the aforementioned server for the purpose of traffic hijacking for profit, which constitutes helping information network criminal activities.

In 2018, Li A, Liang A and others distributed advertisements with content such as "DNS domain name hijacking" and "traffic hijacking" in Baidu Tieba and QQ groups to attract customers of gambling websites. Then use the "Flowbot" website to increase traffic for the customer's gambling website, use redirection software to transfer the click users of the purchased empty shell gambling website to the gambling website designated by the customer. And hire others to manually register accounts, recharge and gamble on the customer's gambling website, implement the crime of increasing traffic to the gambling website, and make illegal profits, which constitutes the crime of assisting in criminal activities involving information networks.

In these two cases, the defendant acted with knowledge that another person had committed an information network crime and provided him with assistance in the settlement of the payment. The defendant and the hijacker paid each other in accordance with the statistical results, and therefore should have been guilty of facilitating the trust

4.3. The Crime of Illegally Controlling a Computer Information System

In traffic hijacking cases, if the perpetrator implants software and modifies the settings of the DNS server privately in the DNS server.

Its modification act does not delete, modify or add operations to the data and applications stored, processed or transmitted in the computer information system, nor does it affect the use function and normal operation of the computer information system. This approach causes less damage to the security of the computer system, and highlights the control factor, then it does not constitute damage to the computer information system [19].

From 2013 to 2014, Gao A and Li A sent Shi A the domain name of the website to be hijacked and the IP address of the website to be pointed to. Relying on the convenience of working in Chongqing Telecom Company, Shi A used the DNS system to modify the domain name resolution configuration file, hijacked the domain name of a private server game, and obtained website promotion fees. In this case, Shi's behavior focused on gaining control of the computer information system as an internal staff member. The "destroying" of the computer system is an act of "change" to achieve "control", so it was finally convicted and sentenced for the crime of illegally controlling a computer information system.

The crime of illegally controlling a computer information system is a crime of circumstances. Obtaining a certain amount of online financial service identity authentication information, online financial services information outside the identity authentication information, illegally controlling a certain number of computer information systems, obtaining a certain amount of illegal income or causing economic losses are "serious circumstances." The crime of illegally controlling a computer information system must also have a certain causal relationship with the control behavior. When the perpetrator uses his authority to modify the DNS server settings without authorization to achieve traffic hijacking, if the "serious circumstances" standard is met, it constitutes the crime of illegally controlling the computer information system.

4.4. The Crime of Illegally Obtaining Computer Information System Data

This crime and the crime of illegally controlling computer information systems belong to different aspects of the same crime. This crime refers to the data stored, processed or transmitted in ordinary computer information systems, and does not involve the functions and actual operation of computer information systems.

DOI: 10.54254/2753-7048/17/20231218

In the second half of 2014, Chen A and other seven people implanted Internet data in violation of regulations, changed the ID of Internet users when accessing Baidu to the Baidu promotion ID set by the defendant, and illegally obtained Baidu promotion profits. They used the servers deployed by them to capture and purchase the Cookies data of QQ users and obtain illegal income. The defendant was convicted and sentenced for the crime of illegally obtaining computer information system data. At this time, "damage" is the determination of the result of the act. Although the crime of destroying the computer information system has not been convicted, it cannot be considered that the overall behavior has not caused damage to the security of the computer system. On the whole, although the method itself is less destructive, it may cause great harm in the future.

4.5. Other Related Crimes

In practice, there are also traffic hijacking as a technical means to implement traditional crimes. For example, traffic hijacking is to prepare for subsequent fraud, theft, and so on. At this time, the process of traffic hijacking essentially belongs to the network of traditional crimes, constituting an accomplice, and therefore should be recognized as a traditional criminal law crime.

Article 287 of the Criminal Law provides that "Anyone who uses a computer to commit financial fraud, theft, embezzlement, misappropriation of public funds, theft of state secrets or other crimes shall be convicted and punished in accordance with the relevant provisions of this Law." This article provides new ideas for the criminal law to deal with traditional crimes that are mediated by traffic hijacking.

From a criminal law doctrinal perspective, the argument that traffic hijacking constitutes the crime of theft is not well-founded; for the user, although the purchased traffic is introduced to a website that he or she does not want to visit, it is still actually the actual amount of traffic used to calculate the traffic, without the characteristic of excluding the domination of others over things [20]; However, for the use of traffic hijacking to steal network users' bank accounts, passwords to carry out theft, should be convicted and punished in accordance with Article 64 of the Criminal Law for theft.

2014 Defendants Shen A and Liu A committed the crime of damaging computer information systems by means of traffic hijacking.

With the purpose of defrauding advertising companies of promotion fees, the crime of fraud was committed. According to the principle of punishment from one felony, it was finally determined as a crime of fraud. In addition, the behavior of swiping traffic is to deliberately obtain settlement fees by creating false data, which also meets the constituent elements of the crime of fraud [10].

For traffic hijacking infringement of other personal information of network users, it may constitute t the crime of selling the personal information of citizens under Article 253 of the Criminal Law. And if the means of traffic hijacking is used to exercise the convenience of the position. For example, the defendants Chi A, Yuan A and others by making a mirror on the server with advertisements on it. To collect advertising fees to profit, and together the unit's property illegally for their own behavior, this belongs to constitute the crime of money laundering.

Traffic hijacking constitutes a crime of sabotage of production or other business operation under certain circumstances. In other words, the object of the crime of disrupting production and business operations should be interpreted in an expanded manner, from the original physical production and operation order to the production and operation order including the Internet operation order.

As traffic hijacking is characterised by unfair competition, the offence of sabotage could be expanded to include the use of misleading advertisements, drop-down boxes, menus or keywords to induce potential users to access a particular website on their own. Even if not carried out in a hard way, such as by damaging computer information systems, traffic hijacking may still be suspected of

DOI: 10.54254/2753-7048/17/20231218

sabotage of production or other business operation, rather than necessarily being subject to civil remedies [20].

5. Analysis of the Regulation of Traffic Hijacking under the Perspective of the Application of Criminal Law

For a long time, traffic hijacking has mostly been adjusted by means of civil and commercial means. Among them, the main ways of civil relief are compensation and application for pre-litigation injunction. However, with the operation of criminals' industrialization model, simple civil remedies are likely to create a vacuum in the application of law. At this stage, the crimes of traffic hijacking are mainly computer-related crimes, and criminal regulation can improve the applicability of criminal law to deal with new types of crimes. In addition, the behavior of traffic hijacking is highly concealed, and most traffic hijacking actors set up their sites outside the country, and civil relief will increase the difficulty of the party's burden of proof [21]. And the use of criminal means to intervene in multi-department joint investigations can eliminate technical obstacles to collect and preserve evidence to safeguard public interests.

5.1. Constructing a Criminal Law Protection System That Typifies the Legal Interests of Data

In the absence of pre-administrative regulations, the appropriate expansion of the criminal law will help maintain the order of network security, but the expansion of the network crime circle must be based on the basic principle of clear protection of legal interests [22].

Arbitrary data carries two different types of legal interests from the beginning of its generation: the first type of legal interest is the independent legal interest of data as a form of carrying, that is, data security; The second type of legal interest is the legal interest contained in the information content carried by the data, which may involve personal information, property rights, privacy, etc. At the same time, it must be realized that whether it is to change the state of awareness or controllability of data, or to obtain control over computer information systems, or to affect the normal operation of computer information systems, it is necessary to operate on data at an objective level. This is the core feature of computer crimes, and it is also the key to distinguish the crimes related to endangering the security of computer information systems from other traditional crimes. Since the legal interests for the protection of traffic hijacking are identified as the security of the computer information system, the legal interests for the protection of the criminal law should also cover it. Narrowly protecting the legal interests of data property does not conform to the essence of traffic hijacking, nor is it conducive to the healthy development of the computer network system as a whole.

5.2. Classification of Convictions Based on Behavioural Characteristics

There are four main modes of traffic hijacking, namely: DNS hijacking, CDN hijacking, gateway hijacking, and client hijacking. The characteristics of these behaviors include: a wide range of crimes, based on the high-speed transmission of the network, can launch attacks on multiple systems at the same time, causing damage to the security of the entire network system; The criminal behavior is concealed, using hidden network channels to attack, and even imitating formal information to carry out "phishing" attacks; The social harm is serious. Considering that traffic hijacking mostly uses indiscriminate attacks, the number of attacks on the target processor during peak hours may reach tens of thousands per day.

At the same time, the crime of sabotaging computer information systems is generally characterized by a wide range of crime areas, hidden criminal acts, and serious social harm. These

DOI: 10.54254/2753-7048/17/20231218

characteristics are also consistent with the characteristics of traffic hijacking crimes. Only by classifying traffic hijacking behaviors, strictly abiding by the principle of legally prescribed crimes and punishments, and scientifically dealing with the competition and cooperation relationship between this crime and the other crime can it be correctly characterized by the criminal law

5.3. Countermeasures Against Traffic Hijacking in Practice

Firstly, the guiding case is used as a guide. Guiding Case No. 102 adopted the offence of destroy a computer information system for DNS traffic hijacking. From this level, in the subsequent trial process, judges will be more inclined to use the guiding case as a reference for adjudication, and accumulate corresponding trial experience, then use the experience accumulated in the guiding case to supplement the judicial interpretation and other content.

Secondly, the interpretation of the law should precede the legislation. Some scholars have summarised the entire legal interest of cybercrime as the public information order, and this view has a certain degree of reasonableness. European and American countries have enacted the EU–US Privacy Shield to protect the privacy data security of individual users; The main crime involved in the regulation of traffic hijacking by Japanese criminal law is the crime of obstructing business such as damaging electronic computers under Article 234 of the Japanese Criminal Code [23, 24]. This public character reflects the importance of that order and the need to emphasise preventive efficacy in both legislation and justice. Through the trend of amendments to criminal law in recent years, the state's fight against cybercrime has also undergone a preventive transformation. It is proposed to treat critical computer information systems carrying data transmission services as special objects of protection, to separate them from the general objects of computer crime and to lower the criteria for incrimination of violations of critical information infrastructures. The act of infringing on computer critical information infrastructure will be independently incriminated. The concept of critical information infrastructure is proposed in the Cybersecurity Law, and the criminal law should respond to this from the perspective of the interface between the execution and punishment. Cybercrime depends on the rapid development of the network, frequent creation of new crimes for cybercrime will affect the stability of criminal law, but this trend can not become the norm of China's criminal legislation on cybercrime.

Finally, the boundaries of existing offences should be clarified, while the focus of legislative work should be shifted from the quantitative problem of lack of compliance to the qualitative problem of achieving good law and good governance.

6. Conclusion

In today's computer data security is highly valued, in the face of traffic hijacking behavior to bring a variety of challenges to network security, the intervention of criminal law is inevitable. To criminal law means to regulate the traffic hijacking behavior has the essential and advantageous. In the criminal law of various countries, there are relevant legal provisions involved. European and American countries have enacted the EU–US Privacy Shield to protect the privacy data security of individual users; The main crime involved in the regulation of traffic hijacking by Japanese criminal law is the crime of obstructing business such as damaging electronic computers under Article 234 of the Japanese Criminal Code. The legal interest protected is the smooth conduct of business carried out by the electronic computer, which itself can be seen as a continuation of the protection of the security of the computer system; There is also a special criminal law, the Prohibition of Illegal Network Connections Act, which promotes the healthy development of a high information and communication society by maintaining the order of electrical communication through storage control functions. When criminalising traffic hijacking, the specific act should be limited to the

principle of criminality. The crime of destroy a computer information system should not be treated as a pocket crime, and the relevant offences should be interpreted in an expanded manner, and traffic hijacking should be treated with specific classification in order to correctly characterise the criminal law.

References

[1] *Guo, Q. (2020) A Compilation of Interpretations of Technical and Legal Terms for Cybercrime Cases by the First Office of the Supreme People's Procuratorate, Post & Telecom Press, Beijing.*
[2] *Chen, Y. H. (2019) Thoughts on the Criminal Law Regulation of Traffic Hijacking——From the Perspectiveof Guiding Case No. 102, in: Journal of Southwest Petroleum University (Social Science Edition), 6, 76-83.*
[3] *Feng, J. (2014) The Standpoint and Method of Criminal Law Dogmatics, in: Peking University Law Journal, 1, 172-197, DOI: CNKI:SUN:WFXZ.0.2014-01-010.*
[4] *Zhang, M. K. (2017) Protection of Legal Interests and the Principle of Proportionality, in: Social Sciences in China, 7, 88-108+205-206, DOI: CNKI:SUN:ZSHK.0.2017-07-005.*
[5] *Ji, J. (2016) The Legal Construction of the New Internet Property Interest Form——From the Perspective of Proposing the Traffic Right Confirmation Rules, in: Science of Law(Journal of Northwest University of Political Science and Law), 3, 182-191, DOI:10.16290/j.cnki.1674-5205.2016.03.018.*
[6] *Zhao, W. S. (2014) How the law applies to the theft of virtual property such as "traffic packages", in: People's Procuratorial Semimonthly, 4, 41-46, DOI: CNKI:SUN:RMJC.0.2014-04-012.*
[7] *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems, Article 4, Retrieved from: http://www.chinalabs.com/.*
[8] *Chen, Y. H. (2019) "Control", "Acquisition" or "Destruction"——Analysis of the crime of traffic hijacking, in: Journal of Northwest Minzu University (Philosophy and Social Sciences), 6, 95-103, DOI: 10.14084/j.cnki.cn62-1185/c.2019.06.012.*
[9] *Wang, X. M. (2019) How to determine the crime behind "crazy traffic", in: Beijing Daily, 6, 014.*
[10] *Wang, J. (2017) Let's talk about the legal matters of traffic, in: Beijing Arbitration Quarterly, 1, 122-129, DOI: 10.13611/b.cnki.978-7-5093-3452-2.2017.01.008.*
[11] *Chinalabs :Research Report on Rogue Software and Countermeasures in China, (2016) , Retrieved from: http://www.chinalabs.com/.*
[12] *Jing, M., Feng, Y. G. (2021) Criminal law characterization and governance countermeasures of traffic hijacking, in: The South China Sea Law Journal, 2, 11-21, DOI: CNKI:SUN:NHFX.0.2021-03-003.*
[13] *Wang, S. Y. (2021) Criteria for identifying "will get traffic" in traffic hijacking cases, in: Journal of Information Security Research, 7, 1077-1083, DOI: CNKI:SUN:XAQY.0.2021-11-012.*
[14] *Wu, F. Y. (2019) Research on criminal law evaluation and criminalization of traffic hijacking, in: Shanghai Legal Studies, 3, 358-360.*
[15] *Yu, X. H. (2015) Judicial Practice Analysis and Normative Meaning Reconstruction of the Crime of Destroying Computer Information System, in: SJTU Law Review, 3, 140-154, DOI: 10.19375/j.cnki.31-2075/d.2015.03.013.*
[16] *Li, T. (2022) Distinguish technical background and accurately punish traffic hijacking behavior, in: Prosecutor's Daily, 5, 17-19.*
[17] *Xiao, Y. (2020) Qualitative research on traffic hijacking behavior in computer crime, in: Journal of Capital Normal University (Social Sciences Edition), 1, 37-44, dol: CNKI:SUN:SDSD.0.2020-01-009.*
[18] *Chu, H. Z. (2016) Discrimination and Analysis of Modesty and Practical Rationality in Criminal Law, in: Journal of Soochow University (Philosophy & Social Science Edition), 3, 59-67+191, DOI: 10.19563/j.cnki.sdzs.2016.03. 009.*
[19] *Gao, S. Y. (2021) "Economic loss" in crimes against computer information system security, in: Journal of Southwest University of Political Science & Law, 4, 04-0093-14, DOI: 10.3969/j.issn.1008-4355. 2021.04.*
[20] *Li, J., Bai, X. W. (2017) Judicial determination of traffic hijacking, in: People's Court Daily, 1, 7.*
[21] *Song, Z. Y. (2021) Rethinking on the Criminal Law Regulation of Traffic Hijacking, in: Journal of Shanghai Police College, 4, 58-66+89, DOI: 10.13643/j.cnki.issn2096-7039.2021.04.009.*
[22] *Wu, S. K., Li, T. (2020) Criminal Law Response to Traffic Hijacking, in: People's Procuratorial Semimonthly, 8, 30-33, DOI: CNKI:SUN: RMJC.0.2022-08-008.*
[23] *Zheng, Y. M., Zheng, H. F. (2018) Research on Cross-border Personal Data Protection and Relief Mechanism in the Internet Era——Taking " EU–US Privacy Shield " as an Example, in: Journal of Guangxi University(Philosophy and Social Science), vol.02.2018, pp.42-48, DOI:10.13624/j.cnki.jgupss. 2, 6.*
[24] *Sun, L. (2015) "Research on Criminal Omission in Joint Offenses." Renmin Chinese L. Rev. 3, 164.*