Asian Social Science; Vol. 19, No. 6; 2023
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

The Research on the Production and Sale of Online Game Hacks Behavior Conviction

Jiachun Du[1], & Jun Lin[2]

[1] ICBC Changchun Municipal Branch, Changchun, China

[2] Economic Law School, Southwest University of Political Science & Law, Chongqing, China

Correspondence: Jiachun Du, ICBC Changchun Municipal Branch, Changchun, 130000, China. E-mail: 13141103900@163.com.

Co-first authors, the authors contributed equally.

Received: September 27, 2023 Accepted: October 7, 2023 Online Published: October 22, 2023

doi:10.5539/ass.v19n6p34 URL: https://doi.org/10.5539/ass.v19n6p34

Abstract

The endless emergence of online game hacks affects the development environment of the entire online games, damaging the interests of the developers and operators while also hitting the enthusiasm of social innovation. This paper will adopt empirical research method and comparative research method based on the data of previous court judgements and combined with the current relevant legal regulations. The objective of this research is to expose the problems in judicial practice by analysing the existing case judgments on the criminal law system of making and selling online game hacks, distinguishing different crimes according to the legal benefits, and providing corresponding suggestions. The results of the study reveal that there are different definitions of online game plug-ins, mismatches between legal and technical knowledge, unclear thresholds of offence, and confusing identification of crimes in the current judicial practice. To sum up, firstly, we can learn from the way of dealing with this problem in other countries. Secondly, the offence should be identified more accurately by making an accurate distinction between specific legal interests in practice. Finally, the above problems can be solved by analysing the nature of infringement from a technical perspective and combining it with the law in depth.

Keywords: Production and sales of online game hacks, Criminal law regulation, Judicial practice, Crime analysis

1. Introduction of Online Game Hacks

1.1 Definition and Classification of Online Game Hacks

1.1.1 Definition of Online Game Hacks

The earliest definition of plug-ins in China derived from the 2003 *Notice on the Launching of Special Control on "Private Services" and "Plug-ins"*. However, over the last dozen years, game plug-ins have also evolved. It is difficult for the definition to meet the current evaluation. Definition of game hacks need to be combined with its own characteristics and legal thinking. On one hand, plug-ins using computer technology, the development of a variety of built-in peripheral programs to manipulate and modify the game data in the view of the characteristics of plug-ins. On the other hand, subject to criminal penalties for game hacks have a greater degree of harmfulness, the production of the seller has the subjective intent and profit-making behaviour from the perspective of the criminal law system. In conclusion, this paper considers that the online game hacks which should be subject to the criminal law system refers to the intentional use of computer technology to crack the protected game programme, which is harmful to the online game information system, and thus is used as a tool to change the game programme for profit-making.

1.1.2 Classification of Online Game Hacks

The Chinese National Standard GB/T32413-2015 *"Prevention and Control of Online Game Plug-ins"* divides online game plug-ins into six categories from a technical point of view. However, not all online game plug-ins are subject to criminal law. Mixing different types of plug-ins with different degrees of harm is likely to cause disputes over criminalisation and the problem of adapting to crime and punishment. For example, the function of simulation plug-ins is "to assist the user to complete some simple and repetitive operation process, to reduce the

use of a large number of repetitive operations, typical software such as 'keystroke smurf[1]". Although this type of game plug-ins affects the fairness of the game to a certain extent, the criminal law emphasizes on the social harm and the severity of the situation, so this type of behaviour is often not regulated by the criminal law. Instead, the game company will seek civil damages for the production and sale of such online game plug-ins, and penalise players who use such plug-ins.

The online game plug-ins discussed in this article are mainly destructive hacks, and here we can refer to Article 3.2 of the "*Code of Practice for Destructive Programming Tests"* issued by the Forensic Authority for the definition of destructive programming, that is to say, unauthorised and intentional acquisition, deletion, addition, modification, disruption, and destruction of the functions of the computer information system or the data stored, processed, or transmitted by the program.

1.2 The Dangers of Online Game Hacks

1.2.1 Harmful Effects of Online Game Hacks on Game Development and Operation Companies and Game Players

The emergence and high incidence of online game hacks have greatly undermined the fairness of games, leading to player withdrawal, shortening the life of the game, causing losses to development companies, leaking game data, and discouraging innovation, etc. Game companies have been deeply troubled by this problem, while the cost of combating violations has been increasing day by day. In 2018, about 30 game manufacturers in Europe and the United States jointly formed the "Fair Gaming Alliance", aiming to find the best strategy to deal with the malicious gaming behaviours of game hacks. In China, as of September 2020, "Tencent Guardian Programme security experts said the actual sales scale of game hacks in China exceeds 2 billion yuan per year, which had a significant impact on the healthy development of China's game industry.[2]"

1.2.2 Online Game Hacks Prone to Derivative Offences

Online game hacks involve many derivative offences and have a wide range of negative impacts on society. Convictions for the production and sale of game hacks as a whole showed a diversified pattern, and the following is a brief description of a few more representative crimes.

Firstly, fraud cases ranked second with a conviction rate of 21.7%. In such cases, the perpetrators usually use the sale of game hacks as a gimmick to publish false advertisements to attract buyers and charge various fees, or use part-time recruitment to lure young people into joining the gang and trick them into paying a large amount of "start-up funds". Theft with 41.6% of the joint and several judgement rate and fraud closely linked, and to a certain extent, showing the dependence on fraud, weakening and deviation, the symbiotic form of the two crimes illustrates the game as a surface bait on the threat to the citizens' personal property.

Secondly, the crime of helping cybercriminal activities and the crime of disguising and concealing the proceeds of crime as downstream crimes, show a strong homologous correlation with the crime of illegally using information networks. However, cases in this area often involve a large number of defendants, and the courts of jurisdiction are scattered, so there is the problem of "different judgments for the same case" in the judicial practice[3]. The tendency towards fragmentation fully reflects the limitations of the judicial authorities in terms of the breadth and depth of their knowledge of new Internet crimes.

Finally, in the crime of infringing on citizens' personal information, the perpetrator will virus implanted in the plug-ins so as to steal the real information of the player's illegal behaviour and the crime of theft there is the possibility of competition, the proliferation of game hacks for the network security, personal privacy and property security have brought certain potential risks. The rapid development of Internet technology provides a breeding ground for new types of crime, and the form of crime triggered by online game plug-ins is showing an expanding trend of dispersion.

[1] An Chaojie, "On the Criminal Laws and Regulations of Mobile Terminal Plug-in Software", in Beijing Politics and Law Vocational College Journal[2019]Issue 4

[2] Chen Yuxi, 'Tencent: game plug-in black production scale reaches 2 billion yuan per year, calls for crackdown on the manufacture and sale of plug-ins'(2020)<https://www.thepaper.cn/newsDetail_forward_8978328> accessed1 September 2020

[3] Wang Jianwei illegal use of information network first instance criminal judgment (2019)

Luo Cheng Luo Jiaxing illegal use of information network first instance criminal judgment (2019)

Liu Yimin helped information network criminals in the first instance of criminal judgment (2020)

Yin Zhenya help information network crime first instance criminal judgment (2019)

2. Current Practice of the Determination of the Offence of Making and Selling Online Game Hacks

2.1 Status of Judicial Practice on the Offence of Making and Selling Online Game Hacks

This article uses the Wolters Kluwerw Priority Legal Information Database to count a total of 469 criminal cases related to game plug-ins from 2001-2023, and draws the following conclusions:

2.1.1 The Identification of Offences Is Confusing, But Generally More Focused

According to data from the Wolters Kluwerw Priority Legal Information Database form 2001-2023, approximately 29 per cent of criminal cases concerning online game hacks were found to be crimes of providing programmes and tools for invading or illegally controlling a computer information system, as set out in article 285, paragraph 3, of the Criminal Law. The crime of illegal business operation accounted for 14%, and the crimes of damaging computer systems, copyright infringement, illegally obtaining computer information system data, and illegally controlling computer information systems accounted for roughly the same amount, with none of them exceeding 10%. In addition, cases of fraud in the name of selling game hacks accounted for about 22%, and other kinds of offences accounted for a total of 20%, with more cases of crimes derived from online game hacks, of which fraud was the main one. In practice, the courts have been confused in determining offences, but in recent years there has been a greater focus on the determination of offences.

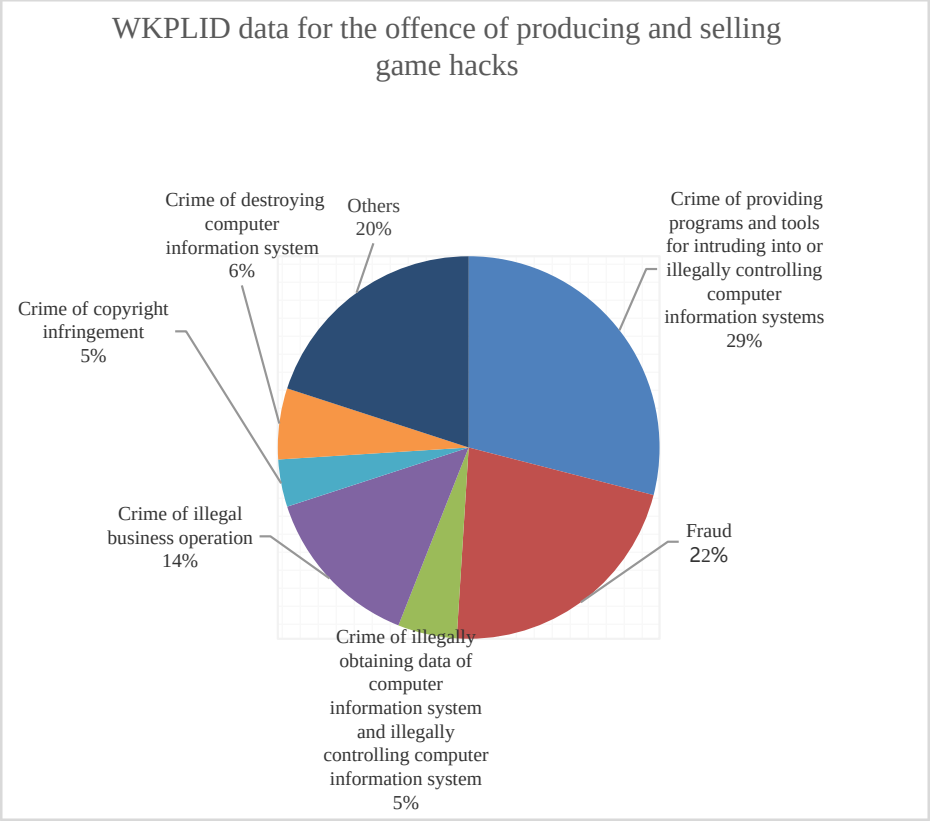

Figure 1. WK Priority Legal Information Database (WKPLID) data for the offence of producing and selling game hacks

2.1.2 Changes in the Types of Offences Identified

According to Wolters Kluwerw data, during the period 2001-2018, about 31% of cases were characterised as illegal business operation offences. In 2009, Article 9 of the *Criminal Law Amendment (VII)* added the new offence of providing the offence of invading and illegally controlling computer information system programs and tools. But only after 2014 did the application of this crime gradually begin to increase, and only about 10% of cases were found guilty of this offence before 2018. In recent years, the differentiation of the found offences has become significantly smaller, and in 2017, for the first time, the number of convictions for the offence of providing programs and tools for invading and illegally controlling computer information systems exceeded the number of convictions for the offence of illegal business operation. After 2019, there were fewer cases in which such acts were found to constitute the crime of copyright infringement.

It can be seen that with the in-depth understanding of the way of operation of game plug-ins, there has been a

shift in the determination of criminal law offences for the production and sale of online game hacks in judicial practice . In the past, most judgements directly identified online game plug-ins as illegal publications, and the practice of identifying such crimes as illegal business crimes was clearly unreasonable.

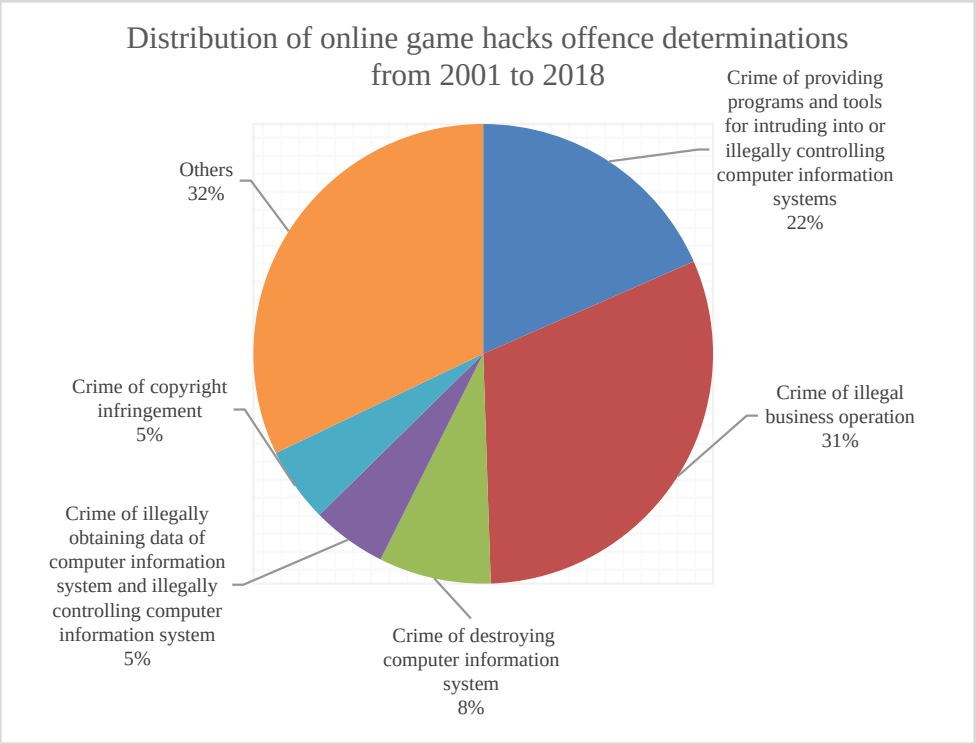

Figure 2. Distribution of online game hacks offence determinations from 2001 to 2018

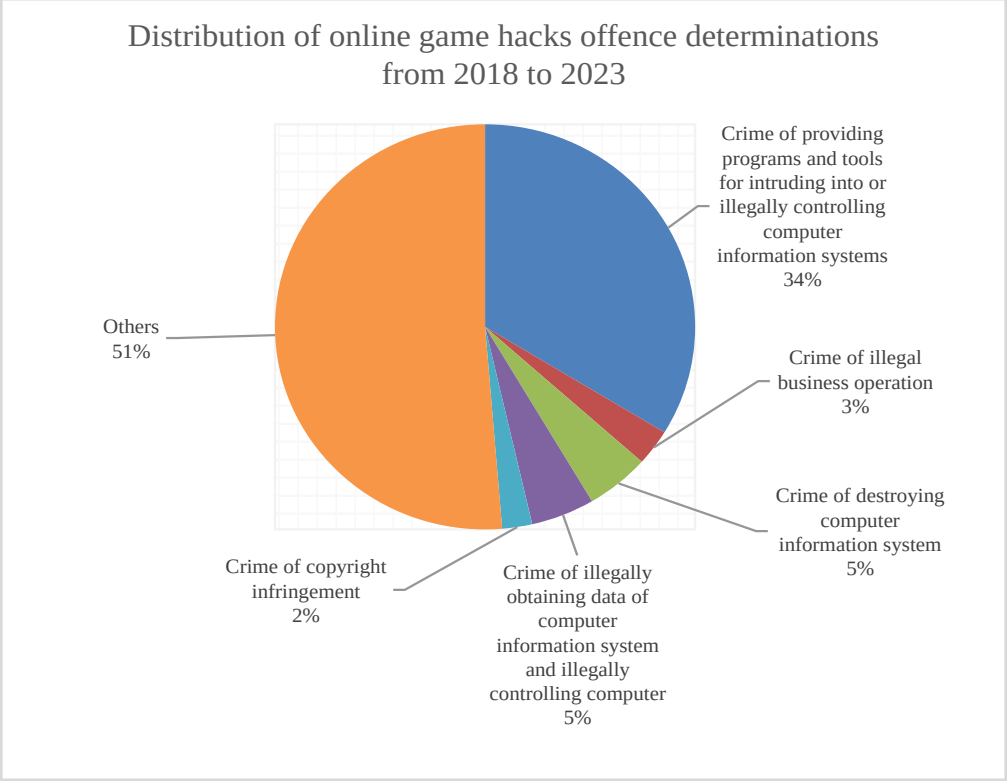

Figure 3. Distribution of online game hacks offence determinations from 2018 to 2023

2.1.3 The Crackdown Against Online Game Hacks Has Been Strengthened and Regulatory Penalties Have Intensified in Recent Years

The types of online games tended to diversify after 2018, with online games showing a prosperous development trend against the backdrop of e-sports being selected for the Asian Games and Chinese team IG winning the League of Legends S8 World Championship. According to the *2018 China Game Industry Report*, "China accounted for about 23.6% of the global game market in 2018, and the scale of game players reached 626 million people, up 7.3% year-on-year[4]". As a result, China has strengthened its criminal supervision and crackdown on online game hacks since 2018, with about 89.6% of related cases being criminal penalties. The number of penalties has been higher year after year, with a total of 73 cases closed within one year in 2018, which is a significant increase compared to previous years.

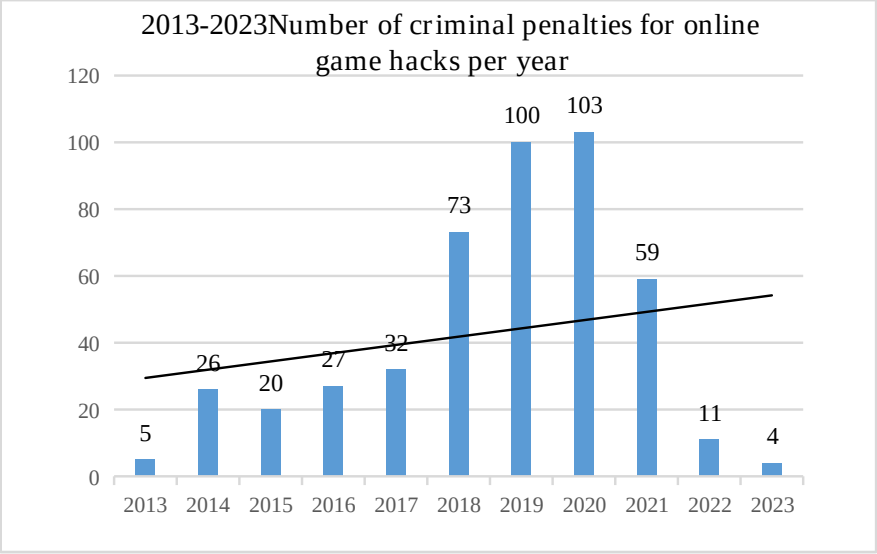

Figure 4. 2013-2023 Number of criminal penalties for online game hacks per year

2.2 Existing Problems in the Determination of the Offense of Making and Selling Online Game Hacks

Due to the lack of uniformity in the definition of online game plug-ins, the courts have varied in their determination of the crime. At present, the determination of the crime has shifted from the crime of illegal business operation to the crime of providing programs and tools for invading and illegally controlling the computer information system, and the object of legal protection has shifted from the market economic order and intellectual property rights to the computer information system. Judicial practice has been more cautious in the use of the underpinning provisions of the crime of illegal business operation to prevent overly expansive interpretations. However, controversial issues such as unclear thresholds for criminalization and vague types of applicable crimes still exist. In cases where profits are made from the sale of online game hacks, there are cases with different penalties. For example, in cases where the amount of the crime is around 100-600 RMB, some courts choose to impose a single fine, while some choose to impose a sentence of punishment above criminal detention and to impose a fine. In cases where the amount of the crime was different, there were cases with similar penalties, for example, where the amount of the crime was 104 yuan and the amount of the crime was 70,000 yuan, both of which were sentenced to one year's imprisonment.

Prior to 2018, there were many cases in which the offenses were similar but the courts found different charges and the sentences lacked detailed reasoning and did not differentiate between the different charges. At the same time, in the past five years, many courts have given priority to the application of Article 285(3) when finding cases involving online game hacks, cases involving hacks are often complex, and consideration should also be given to whether or not there is a problem of competing crimes, which should be analyzed in a specific manner to prevent blind convergence in the determination of crimes.

3. Analysis of the Problem of the Offence of Making and Selling Online Game Hacks

In China's criminal law system, for the production and sale of online game hacks acts of incrimination and

[4] GPC, CNG: '2018 China Game Industry Report' in China Economic Net(2018) <http://www.ce.cn/culture/gd/201812/24/t20181224_31097900.shtml>, accessed 24 December 2018

conviction due to its relevant legislative lag, qualitative ambiguity and judicial interpretation of the vagueness, which makes this crime related to the application of the offence and conviction and sentence in the actual trial practice of the larger differences, and more controversial. The following article through the literature combined with specific cases to analyse China's production and sale of online game hacks behaviour of the crime.

3.1 Crime of Providing Programmes and Tools for Intruding into or Illegally Controlling Computer Information Systems

According to article 285, paragraph 3 of the Criminal Code, the legal interest protected by this offence is the security of computer information systems. One of the circumstances constituting this offence is that the perpetrator provides tools and programmes dedicated to the criminal act of unlawfully controlling and intruding into a computer information system. The word "provision" includes providing the tools and programmes to a specific or non-specified object in a gratuitous, direct or indirect, online or offline manner, and the programmes and tools in this case are mostly illegal. Another situation requires the perpetrator to knowingly provide them, placing more emphasis on the subjective malice of the perpetrator, which may constitute the offence even if the programmed tools provided are themselves lawful.

With regard to "programmes and tools specially used to invade or illegally control computer information systems", the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Endangering the Security of Computer Information Systems (hereinafter referred to as the "Interpretation") defines them into three main categories[5] according to Article 2 of the Interpretation. In practice, when the crime is identified, the game plug-in is generally judged whether the destructive, according to the definition of destructive program mentioned above and the judicial interpretation of the three situations to be compared. It is not difficult to find that in the protection of data on the judicial interpretation of the provisions of the requirements of "access and control", and the destructive program concept covers a broader and more comprehensive behaviour. The concept of disruptive procedures covers a broader and more comprehensive range of behaviours. With regard to the definition of "aggravating circumstances", the Interpretation also contains clear provisions[6]. However, it should be noted that whether or not the perpetrator's purpose of providing the programme or tool is for profit is only one of the criteria for determining the seriousness of the circumstances, and does not affect whether or not the crime is established.

According to the analysis of the above data and crimes, most of the seriousness of the production and sale of online game hacks is determined to be this crime, precisely because the plug-in program has the role of circumventing or breaking the security protection measures of the computer information system, copying and controlling the data of the computer information system without or beyond the authorisation as mentioned in the Judicial Interpretation. In other words, as long as the game hack has enough destructive properties, it will

[5] According to Article 2 of the Interpretation, a program or tool with one of the following circumstances shall be deemed to be a "program or tool specially designed to invade or illegally control a computer information system" as stipulated in the third paragraph of Article 285 of the Criminal Law: (1) a program or tool that has the function of circumventing or breaking through security protection measures of a computer information system, and obtaining data of a computer information system without authorisation or beyond the authorisation.(a) with the function of bypassing or breaking through the computer information system security protection measures, unauthorised or exceeding the authorisation to obtain computer information system data; (b) with the function of bypassing or breaking through the computer information system security protection measures, unauthorised or exceeding the authorisation to implement the function of controlling the computer information system; (c) other programs and tools specially designed to invade, illegally control computer information systems and illegally obtain computer information system data

[6] According to Article 3 of the Interpretation, providing programmes and tools for invading or illegally controlling computer information systems shall be deemed to be aggravating circumstances as stipulated in Paragraph 3 of Article 285 of the Criminal Law if one of the following circumstances exists: (1) providing programmes and tools that can be used for illegally obtaining payment and settlement, securities trading, futures trading, and so on, or for the purpose of illegally obtaining payment and settlement, securities trading, and futures trading. (a) providing a special programme or tool that can be used to illegally obtain authentication information for payment and settlement, securities trading, futures trading and other network financial services for more than five times; (b) providing a programme or tool other than those in item (a) that is specifically used to invade or illegally control a computer information system for more than 20 times; (c) knowing that another person has committed the offence of illegally obtaining authentication information for payment and settlement, securities trading, futures trading and other network financial services (c) knowing that others have committed illegal payment and settlement, securities trading, futures trading and other network financial services identity authentication information and provide programs and tools for more than 5 times; (d) knowing that others have committed illegal acts other than (c) of intrusion into, illegal control of computer information systems and provide programs and tools for more than 20 times; (e) more than 5,000 yuan of illegal proceeds or cause economic losses of more than 10,000 yuan; (f) other serious circumstances. If the perpetrator of the acts stipulated in the preceding paragraph has one of the following circumstances, he or she shall be deemed to have committed a particularly serious offence of providing programmes or tools for invading or illegally controlling computer information systems: (a) the number or amount of such programmes or tools reaches more than five times the standard stipulated in subparagraphs (a) to (e) of the preceding paragraph; and (b) other circumstances of a particularly serious offence

certainly constitute this crime. Judicial interpretation of the seriousness of the circumstances of the standard for the provision of the number of times and the illegal income, the amount of damage caused by the low threshold of criminalisation, strong punishment, which is conducive to preventing the plug-in layers of resale, limiting the downward influence. Judicial appraisal of the destructiveness of a wide range of content, strict requirements. In fact, some auxiliary plug-ins will also be involved to a certain extent in the unauthorised reading of data and information, but its social harm is less, whether the crime and punishment are compatible is also one of the controversial points of the long term.

3.2 Crime of Illegally Obtaining Data from Computer Information Systems

According to article 285(2) of the Criminal Code of the People's Republic of China, the interests protected by this provision are the security of data in computer systems, which mainly refers to the confidentiality and control of information. In this provision, the perpetrator must have the intention of illegally obtaining the data and controlling the computer system to meet the requirement of subjective side.

Paragraph 2 and Paragraph 3 of Article 285 both deal with the situation of unlawful acquisition of data, overlap to some extent. To distinguish them, we should determine the juridical attributes of the data information based on its specific content, which is also an effective guide to determining the type of specific legal interest infringed upon. Using technology to analyse the characteristics of the operation of game hacks and the internal logic of the protection of legal interests can be a good way to find differing aspects of the two articles. Moreover, a case-by-case strategy would be the icing on the cake.

The subject of the crime of illegally obtaining data from computer information systems and the crime of illegally controlling computer information systems mainly corresponds to the game hack maker mentioned in this article. In carrying out the conviction, it is necessary to combine the Data Security Law and the Network Security Law to comprehensively realize the legal interests protected by this crime, and to understand the word "obtain" in this provision. It is also the key to distinguishing this crime from Article 285 (3) and Article 286. The interests protected by Article 286 tend to be the integrity of data use and the operability of the system, whereas Article 285 (3) tends to prevent the illegal obtaining of data and the modification of the use of the data, focusing on the protection of data confidentiality.

3.3 Crime of Damaging Computer Information Systems

The crime of damaging computer information systems emphasizes the damage caused to the data in the computer information system and requires that this damage should be able to cause serious consequences that affect the normal operation of the computer system.

Generally speaking, the data in the computer information system can be divided into two categories, the first is the functional data as part of the computer function to support the operation of the information system, and the second is the processing data generated in the process of system operation and stored in the database, which needs to be protected. The type of data involved in game hacks is mainly processing data.

The "damage" in this Article mainly includes two main ways, the first is destroying the functions, data and procedures of the computer information system, and the second is causing the system to be unable to operate normally. Compared to other crimes with the same object, this crime carries the heaviest statutory penalties and leads to the most serious consequences. Furthermore, there is also a difference in the subject matter of this crime, which can distinguish Article 286 from 285(3). Although game hacks are destructive, the degree of destructiveness of the two crimes cannot be equated, so this crime should be applied with caution.

3.4 Crime of Copyright Infringement

The crime of copyright infringement is stipulated in Article 217 of the Criminal Law, which contains six situations. The judicial practice mainly identifies this crime with the first situation, which requires knowing and for profit subjectively, and objectively without the permission of the copyright owner, copying and distributing, and disseminating computer software to the public via the information network. Whether online game hacks constitute this crime, there are very different views in the academic sector and judicial practice.

In 2007, the People's Court of Haidian District, Beijing City, clarified the scope of legal interpretation of "copying and distribution". In this viewpoint, "copying and distribution" in paragraph 3 of Article 11 of the Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Specific Application of Laws in Handling Criminal Cases of Infringement of Intellectual Property Rights is mainly applicable to the issue of pirated software in the network environment, and should not be overly expanded to include the interpretation that online game hacks are equivalent to pirated software. This is because the only way to run the game hacks is to attach it to the game itself, in other words, the behaviour of

modifying the game's own data to achieve hacking by external procedures belongs to "secondary processing".

In 2014, the People's Court of Longquanyi District, Chengdu City, Sichuan Province, found that the behaviour of the Li Shoubin, Xiang Renda and two others is an infringement of copyright. The court held the view that hacks could add features , which were not in the original game. Only through copying the source code of the game program can this behaviour accomplish. With a high degree of similarity to the original game program, the hack intercepts and modifies the data sent from the client to the server, which meets the legal requirement of "copying and distribution".

By comparing the two cases mentioned, it is not difficult to find that the main point of contention lies in whether some online game hacks can be regarded as "copying and distributing" when they are involved in modifying data. According to the Copyright Law, copyright includes the right of modification, and the modification of data mainly involves the right of modification. A few scholars believe that "the unauthorised production of online game hacks for profit infringes on the modification right rather than the copying and distribution right of the online game right holder's copyright, and does not constitute the crime of copyright infringement. ". In addition, some people convict the behaviour from the perspective of the subjective and objective combination of the commission of the crime and the focus on the protection of different legal interests, believing that such acts mainly violate the security of the computer information system, rather than the reproduction and distribution rights of game works. For those who affirm that the hack constitutes "copying and distribution", they hold the view that the modification of data often requires the use of existing data, in which the copying of data is a necessary process, and involves the use of communication protocols of online games without the permission of the online game operator. What's more, some scholars also qualify the matter from the degree of independence of the operation of the hack, whether the copied content touches the core of the game's operation mode, the proportion of copied content, as well as the form and substance of the copy. According to judicial guiding cases, the types of game hacks that have been found guilty of copyright infringement are mainly offline hacks.

This paper believes that the interpretation of the meaning of "copying and distribution" should not be confined to the mere concept of words, nor should it be over-expanded. At present, the infringement of copyright on the rights covered by the content is not exactly the same between the Copyright Law and the Criminal Law. What's more, civil and criminal norms in this area do not yet bridge the gap, lacking of complete articulation. To solve the problem of determining the crime of producing and selling game hacks, judicial authorities should analyse the rights and interests of different hacks based on the specific protection, giving full consideration to the operating characteristics of different hacks, the similarity between the programs, the substantiality of the copy, and the magnitude of the impact of the copied data content on the originality and overall operation of the game. Copyright law should, on the one hand, be harmonised with the rights provisions of criminal law and, on the other hand, take into account the emphasis placed by copyright on originality and other characteristics. Although the Amendment (XI) to the Criminal Law has expanded the coverage of copyright protection, it has not been used as a basic crime to regulate the production and sale of hacks in judicial practice. Except for the "clich éd" interpretation of "copying and distribution", Prosecutor Liu Tao of the Supreme People's Procuratorate believes that " technologies and devices that intrude into the computer information system, illegally obtain computer data and interfere with the normal operation of games cannot simply be regarded as "technological measures" in copyright law, as stipulated in article 217 (6) of the Criminal Law. The conceptual scope of the two is not the same, and they cannot be directly equated. "

4. Suggestions for Improving the Use of Criminal Law to Regulate the Production and Sale of Online Game hacks

4.1 Comparison of the Way to Deal with the Production and Sale of Online Game Plug-ins at Home and Abroad

The regulatory schemes for the production and sale of online game plug-ins outside of China presents a diversified pattern with different combat strengths and across multiple sectoral laws.The following is a comparative analysis of the Chinese and foreign governance modes of combating the production and sale of online game hacks and bots.

4.1.1 South Korea: Special Legislative Protection Needs to Be Viewed Dialectically

As early as 2017, South Korea has begun to regulate online game hacking by special legislation. The Act on Promotion of Information and Communication Network Use and Information Protection and the Game Industry Promotion Act provide effective policy protection and legislative support for e-sports and the game industry. In this context, the cost of defending the rights of game operators in South Korea is relatively low and the efficiency is relatively high. To a certain extent, the practice of "criminalisation of hacks" in China is similar to that of South Korea, which provides stable public power protection for game operators and users to a large extent,

and plays an important role in purifying the network information space. However, the "unrecognised program" standard used in the existing Korean law to determine hacks relies too much on prior regulation and ignores the diversity of realities and potential possibilities for development, which has been criticised by many in their own country. In this regard, China needs to learn a lesson and take a path that is in line with its own unique national conditions. While encouraging and fostering new industries to promote economic development, the Government and the courts should also pay attention to the ultimate complementary nature of the criminal law and avoid overly pursuing a comprehensive crackdown on related crimes.

4.1.2 Japan: Macro-regulation Mode Provides a Reference Path

In response to the behaviour of archive modification in games with both single and online play, Japan has adopted a regulatory approach similar to that of hacks to legally restrain such behaviour in the Unfair Competition Prevention Act (2018 vision).The adoption of anti-unfair competition law to regulate this behaviour essentially shows that game hacks or bots fall under the jurisdiction of economic law in Japan, with an emphasis on the property rights and interests of game producers and operators and fair competition among players. At the same time, Japan uses multi-disciplinary sectoral laws to attribute responsibility and punish the relevant behaviours, almost achieving an effective link between civil and criminal law. China has also used the anti-unfair competition law on the production and sale of hacks, but current judicial overall bias in favour of the criminal law level, lacking of a mature civil, commercial and economic law linkage system. This paper believes that, for the less harmful auxiliary plug-ins, referring to Japan's appropriate use of national macroeconomic regulation and management is also a complementary program.

4.1.3 The United States: Intellectual Property Protection System Worth a Reference

The United States has now formed a relatively perfect copyright Legal Normative Framework for the production and sale of online game plug-ins. However, existing judicial practice in the United States would classify similar conduct as an intellectual property crime, the conviction of which shows a centralised and extensive trend. In contrast, China's official awareness of intellectual property protection and action is still insufficient, but the identification, categorisation and analysis of specific interests is more precise than in the US to some degrees. In this regard, China should make up for the shortcomings mentioned above and refer to the U.S. copyright law system reasonably, forming a comprehensive process for the protection of auxiliary operation hacks by means of intellectual property rights. Meanwhile, it is crucial to clarify the boundaries and criteria for regulating illegal publications in order to achieve precise conviction. Only in this way can abuse of copyright-based crimes and the lack of reasoning in judgements be minimised.

In a nutshell, the various ways of determining the same act in different countries reflect the reality and value orientation of each country at a deeper level. Using comparative law perspective to penetrate the political, economic and cultural kernel contributes to adequate reference to advanced rule of law practices around the world, which provides a optional path for the Chinese domestic reality.

4.2 Proposals on the Conviction of the Producing and Selling Online Game Hacks

4.2.1 Integration of Multiple Channels for Accurate Criminalisation with Due Regard to Specific Legal Interests

In the criminal regulation, for the judgement of the lack of theoretical foundation, the case of unclear statement of facts, the interpretation of the problem of changeable random and other realities, the judiciary should strictly observe the principle of proportionality between crime and punishment, and endeavour to achieve clear identification of crimes and precise application of crimes in the light of specific legal interests. At the same time, in the process of transforming of criminalising the production and sale of online game hacks, attention should also be paid to circumventing the over-reliance on the crime of providing procedures and tools. For auxiliary hacks, civil law or economic law can be appropriately used to regulate to maintain the final complementarity of the criminal law. In conclusion, for the production and sale of game hacks as a specific crime, various laws and methods should be comprehensively applied to make specific judgments, and effective integration of different sectoral laws should be formed in the tone of criminal regulation.

4.2.2 Focusing on Emerging Crimes in the Context of Cyber-Information and Bridging the Legal and Technological Divide

Nowadays, the judicial practice of cybercrime is facing an insurmountable technical barrier in terms of updating speed, appraisal effectiveness and conceptual understanding. In response to that, this paper puts forward the following suggestions. Above all, the appraisal authority should be urged to analyse the source code of the hack, point out the difference between the plug-in and the original client-side, what kind of influence it brings to the normal game and other specific operation principles and mechanisms, and investigate whether the hack has the

risk of increasing and modifying memory data as well as deleting and destroying the built-in game procedures, so as to provide the court with reasonable and reliable technical support. In the second place, the professional and technical training of judicial staff should be vigorously promoted and the information mastery and legislative efficiency of the public prosecutors and law enforcement teams should be enhanced, so as to minimise the intergenerational gap between the statutory law and the realities of the situation. In the end, if the courts are able to progressively shy away from the forensic organ and to identify the social hazards of the crime itself through the technological mists, the source of the justice system may return to its true essence. In that case, the contradiction in the appropriateness between the law and the technology can be resolved at the fundamental level.

4.2.3 Advocating the Culture of Knowing and Abiding by the Law and Creating a Healthy Cyberspace Together

The research found that due to the diversified forms, changing circumstances and false publicity of the production and sale of online game hacks, their social hazards and criminal illegality are often overlooked and misunderstood by the public. Although the post-90s and post-00s generation are the main audience of online games, most of them know little about the fact that the production and sale of hacks has been criminalised. Therefore, it is necessary for all kinds of subjects to take into full consideration the realistic obstacles to compliance with the law and take action from the following perspectives. Firstly, the public, especially social youths, should seriously study basic legal knowledge and take the initiative to understand the criminalisation, conviction and sentencing standards of cybercrime and other new forms of crime. Secondly, judicial organs at all levels should set up new types of crime information counters, hotlines and websites to provide comprehensive online consultation services on cybercrime, and set up volunteer teams to carry out door-to-door legal literacy services regularly. Finally, law enforcement organs, mainly governmental ones, should actively cooperate with colleges and universities, communities and public welfare organisations to continually organise public welfare legal literacy activities, and expand the scope of publicity by posters, leaflets, new media and other forms, in order to promote the long-term development of legal literacy on cybercrime.

5. Conclusion

This paper has discussed the reasons for the inconsistent convictions for the production and sale of online game hacks, with the aim of using a comparative vision and empirical research to effectively sort out existing cases. The investigation has shown that China's determination of the offence of making and selling online game hacks has been transformed from the offence of illegal business operation to the offence of providing programs and tools for invading and illegally controlling computer information systems, and the object of legal protection has also shifted from the market economic order and intellectual property rights to the computer information system. However, there are still such problems as blind convergence in the selection of offences, unclear thresholds for entry into the offence, and ambiguities in the types of offences to be applied that have yet to be resolved. In a global perspective, the precedents of the use of special legislation, economic law and intellectual property law for protection around the world have provided effective references for Chinese judicial practice.

The suggestions put forward in this study cover a wide range of legislative, judicial and legal literacy levels. With regard to the production and sale of online game hacks, Chinese courts should be based on a wide range of strengths and weaknesses, follow the principle of appropriateness of crime and punishment, combined with the specific interests of the law and other targeted analysis. At the same time, the legislative and judicial organs should also pay attention to the popularisation of the law, and improve the technical level to provide solid scientific and technological support for the legal practice in the professional field. Only by taking the above measures can the rights and interests of gamers and producers be fully protected by the law, and the cyberspace become a clear and righteous place. More broadly, research is also needed to fully integrate the fight against online game hacks within the judicial protection system, which still has a long way to go.

References

An, C. J. (2019). On the criminal law system of mobile terminal hack software. *Journal of Beijing Politics and Law Vocational College*, (4), 80-86.

Brown, A. (2020, September 29). *Cheats and Hacks That are Commonly Used in Online Games.* Retrieved from https://ugtechmag.com/cheats-and-hacks-that-are-commonly-used-in-online-games/

Chu, Y. C. (2019). Discussion on the judicial determination of online game hack behaviour--analysis based on 134 case samples. *Rule of law forum*, (4), 83-95.

Duh, H. B.-L., & Chen, V. H. H. (2009). Cheating Behaviors in Online Gaming. In A. A. Ozok, & P. Zaphiris (Eds.), Online Communities (LNCS 5621, pp. 567-573). https://doi.org/10.1007/978-3-642-02774-1_61

Feng, C. (2023). *Research on Criminal Laws and Regulations of Scripting-type Hangers*. South China University of Technology.

He, B. W., & Hu, L. Y. (2022). On the Admissibility of Network Electronic Data Identification Opinions-Analysis of Judicial Decisions on Game Hanging Class Cases as a Sample. *Journal of Henan University of Finance and Law, 37*(4), 101-111.

Huang, S. J. (2021). The criminal law system of game plug-in behaviour. *Journal of Hubei University of Economics (Humanities and Social Sciences Edition), 18*(2), 94-98.

Liu, S. T. (2022). *A case study on the illegal production and sale of online game hacks.* Hunan University.

Luo, P. F. (2008). The legal application of unauthorised production of online game hacks for sale for profit. *People's justice*, (12), 57-61.

Petro, D. (2020, October 29). *Cheating at Online Video Games and What It Can Teach Us About AppSec*. Retrieved from https://bishopfox.com/blog/cheating-at-online-video-games-part-1

Qian, Q. Q. (2022). *Qualitative research on the criminal law of making and selling hack software.* East China University of Politics and Law.

Ran, J. P. (2020). Research on the criminal law system of making and selling online game hacks. Southwest University of Political Science and Law.

Shi, J. P., & You, T. (2009). On the Criminal Laws and Regulations of Online Game Hangers. *Politics and Law*, (10), 52-58.

Wang, Y. L. (2015). *Research on criminal law issues of online game hangers.* Graduate School of Chinese Academy of Social Sciences.

Wang, Y. Y. (2022). Criminal Laws and Regulations on the Production and Sale of Online Game Hangers. *Journal of Jiangxi University of Technology, 43*(2), 89-97.

Williams, K. (2021, September 12). *Is it illegal to cheat in online video games? We have the answer.* Retrieved from https://win.gg/news/is-it-illegal-to-cheat-in-online-video-games-we-have-the-answer/

Wu, S. X. (2021). Application of criminal law to the production and sale of online game plug-in software. *Crime Research*, (4), 24-36.

Xia, C. H. (2023). Characterisation of the criminal case of "external hack" and "private service". *Procuratorial winds and clouds*, (11), 60-62.

Yang, X. X. (2023). *Criminal law system of making and selling online game hacks.* East China University of Politics and Law.

Acknowledgments

Not applicable.

Authors contributions

Authors contributed equally to the study.

Funding

Not applicable.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal’s policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.