Cyber Black and Gray Industries: Status, Types and Legal Regulations

Zhang Junqi*
Guanghua Law School, Zhejiang University, Hangzhou, Zhejiang, China
**Corresponding Author*

Abstract: Cyber black industries not only directly infringe upon individuals' property and privacy but also pose severe threats to the socio-economic order, cybersecurity, and even national security. The paper analyses the status, types and legal regulations of cyber black and gray industries. Also challenges that the governance of cyber black and gray industries faces involve in terms of technology, law, and regulation. In response to these issues, the paper further proposes comprehensive countermeasures and suggestions in multiple dimensions. International judicial cooperation will increasingly work together to combat cross-border crimes of cyber black and gray industries.

Keywords: Cyber; Black and Gray Industries; Status; Types; Legal Regulations

1. Introduction

In today's digital era, the rapid development of the internet has profoundly transformed people's lifestyles and work methods, becoming a significant force driving social progress. However, as the "dark side" of the internet, cyber black and gray industries have also emerged and spread rapidly.

During the 2019 National Cyber security Week, Ren Yan, Director of the National Internet Emergency Center, stated: Currently, the development of the cyber black industry chain is severe, harming public economic interests, disrupting normal market operations, threatening the stable operation of critical information infrastructure, endangering personal information security, and seriously affecting the healthy development of the internet industry [1].

According to research and statistics by Threat Hunter security researchers, the number of people engaged in cyber black and gray industries continued to rise in 2023, reaching 5.871 million, a 141% increase compared to 2022.[2] Their "2024 Mid-Year Report on Cyber Black and Gray Industries" pointed out that in the first half of 2024, the number of people engaged in black and gray industries exceeded 4.27 million, the number of malicious mobile phone numbers in China reached 3.23 million, the number of daily active risky IPs was 11.36 million, and the number of bank cards involved in money laundering was 195,000. In recent years, as the integration of digital technology and the real economy deepens, the disruption of corporate business security by black and gray industries has become more prominent in large-scale cyber business scenarios. Malicious brushing, financial fraud, and other black industry incidents are continuously coming out, and the increasingly intelligent and chained operation of cyber black industries has caused significant financial losses to enterprises, affecting their normal operations and long-term development. Cyber black and gray industries have shown a diversified and complex development trend, covering areas such as telecom fraud, cyber gambling, data theft, false advertising, and malicious brushing, posing serious threats to individuals, enterprises, and the stability and development of society as a whole [3].

The study searched for journal articles from 2015 to 2024 on CNKI using "cyber black and gray industries" as the keywords and found only 55 articles discussing this topic, with only 14 related masters' and doctoral theses. The research on cyber black and gray industries by industry professionals and scholars is obviously far from enough, and in-depth research and timely crack-down of cyber black and gray industries are urgently needed. This study aims to objectively present intelligence data on black and gray industries, give a heavy blow to cyber black and gray industries, and strengthen effective defense as the goal and consensus across various industries, helping more ordinary people and numerous enterprises know better about black and gray industries and effectively prevent various risks.

2. Analysis of Cyber Black and Gray Industries

2.1 Definition and Characteristics of Cyber Black and Gray Industries

Cyber black and gray industry is an unconventional name without any clear definition at the legal level. Generally speaking, it refers to a series of illegal and criminal activities carried out with the purpose of illegal profit and relying on network technology, covering many fields such as cyber fraud, cyber pornography, cyber gambling, cyber theft, and the production and dissemination of malicious software. It includes the "Three Blacks of Content" which is composed of reprinting or distorting others' manuscripts, malicious marketing, and illegal manuscripts; and the "Three Blacks of Operation" which is composed of hackering others' accounts, fans and traffic brushing, and marketing cheating and etc. [1]. These activities not only pose a serious threat to personal property security and privacy rights, but also greatly disrupt social and economic order, and even have a negative impact on national security [4].

Cyber black industries have significant characteristics. Firstly, it is highly covert. With the help of complex network architecture, encryption technology, and anonymous communication tools, black industry practitioners can conceal their identities and criminal traces, making it difficult for regulatory authorities to trace and trace them. The second is the organized and industrialized operation, from upstream technology research and development and resource provision, to midstream tool production and platform construction, and then to downstream behaviors and money laundering, forming a finely divided and closely coordinated industrial chain, with each link interlocked, greatly improving behaviors efficiency. The third is the severity of the harm, which has a wide range of impacts. It not only directly causes personal economic losses and mental harm, but also indirectly triggers business difficulties, industry trust crises, and further erodes social order and good customs, causing a huge impact on the stability of the entire cyber ecosystem and even the real–world society [2].

On the other hand, cyber gray industry refers to a series of activities to seek economic benefits by some ambiguous means of network technologies. Compared with the cyber black industry, its behavior has not been clearly defined as illegal behaviors, but with behaviors risks that cannot be ignored. Cyber gray industry has the following characteristics. First, it is highly hidden. Practitioners often use complex network, encryption technology and virtual identity to hide their intentions and operation tracks, making it difficult for regulators to detect. Second, it is marginal. It is good at taking advantage of the ambiguity of legal provisions and loopholes in industry rules to play a "marginal ball" to cover up its improper profit purpose in a seemingly legal form. The third is its diversity, which covers a wide range of fields, from e-commerce, social networking, content creation and many other Internet scenes [1].

2.2 Major Types of Cyber Criminal Industries

According to documents issued by the Cyberspace Administration of China and the Office of the Central Cyberspace Affairs Commission, cyber black industrial chain can be divided into three sections: upstream, midstream and downstream, including cyber fraud, pornography, gambling, theft, software-related behaviors, etc. (shown in Figure 1) [4].

2.2.1 Cyber fraud

Cyber fraud manifests in diverse forms, with dating fraud being particularly representative. Fraudsters typically meticulously construct false personas on social platforms, swiftly establishing emotional connections with victims through flattery and sweet talks. Once trust is gained, they induce the victims to transfer funds under the pretext of investment, entrepreneurship, emergencies, or the like. For instance, according to reports by Xin'an Evening News, Anhui News, and Dawan News, the Criminal Investigation Brigade of the Traffic Police Branch of Bengbu Public Security Bureau cracked a behaviors in which a male fraudster posed as a beautiful woman cyber to carry out fraudulent activities. The police finally arrested the suspect, Mr. Yang, who had registered over 20 WeChat accounts by multiple mobile phones and employed location-spoofing software to impersonate a young "beautiful woman" on social apps, defrauding dozens of male victims out of a great sum of money [5].

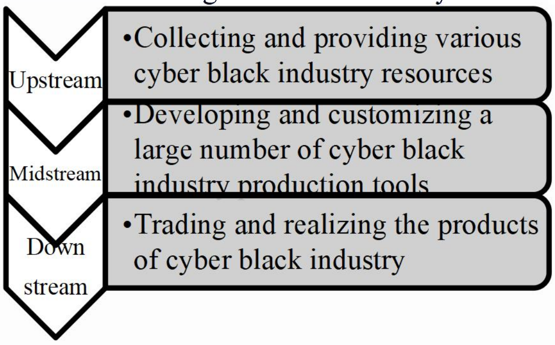
Upstream
•Collecting and providing various cyber black industry resources
Midstream
•Developing and customizing a large number of cyber black industry production tools
Down stream
•Trading and realizing the products of cyber black industry

Figure 1. Streams of Cyber Black Industry

Part-time "click farming" (fake transaction-based rating manipulation) fraud is equally rampant. Under the guise of "easily earning", lawbreakers first deceive victims into trusting them through small-sum rebates, and subsequently lure them into investing large sums of money to execute the fraud scheme. According to Chang'an Cyber (the official news portal of China's Central Political and Legal Affairs Commission), in July 2022, the Public Security Sub-bureau of the High-tech Zone in Daqing City, Heilongjiang Province, in collaboration with the Cyber Police Sub-bureau, cracked a behaviors involving the illegal use of information networks, apprehending 23 suspects. To the public’s surprise, the case involved over RMB 50 million in illicit funds and over 3 million pieces of click-farming transaction data [6]. Fraudulent notifications of false lottery winnings are also a common occurrence. Criminals, masquerading as well-known enterprises or institutions, send out winning notifications, demanding that victims pay fees, taxes, or other charges before they can claim their prizes. Many victims fall prey to such scams out of greed for the alleged rewards.

2.2.2 Cyber pornographic cases

The propaganda channels of the cyber pornographic behaviors have always been so covert to evade crackdowns. On the one hand, they use euphemistic terms, suggestive images or videos through live-streaming platforms and social groups to attract users’ attention. On the other hand, they upload illegal content in short-video platforms too, attracting users to illegal platforms for paid viewing or offline transactions. In terms of profit models, they also generate revenue by collaborating with membership fees, viewing charges, advertisements and even personal information leakage fee, forming a complete black industrial chain. According to a report on the WeChat of the Tongliao Municipal Public Security Bureau on January 13, 2024, the Horbin Sub-bureau of the Tongliao Municipal Public Security Bureau in the Inner Mongolia Autonomous Region cracked a severe behaviors of cyber obscene performances. The pornographic APP involved over 100,000 registered users and 4,000 female anchors, with a cumulative transaction sum of nearly RMB 100 million [7].

2.2.3 Cyber gambling behaviors

Cyber gambling behaviors expanded rapidly on the internet with gambling websites and apps proliferating. These platforms typically use virtual currency recharges and point exchanges to conceal the flow of gambling funds and control gambling outcomes. In addition to traditional card games and lottery-based gambling, new forms of gambling, such as betting on sports events and e-sports competitions, also emerged. According to a report on China Chang'an Cyber, on the evening of December 10, 2022, police successfully cracking Yibin's first soccer gambling behaviors since the start of the Qatar World Cup. They apprehended 22 suspects, with an involved amount exceeding RMB 140 million [8]. More seriously, a large sum of gambling funds is illegally transferred across borders through underground banks, virtual currencies and other channels, posing a significant challenge to the government financial supervision.

2.2.4 Cyber theft behaviors

Cyber theft behaviors primarily rely on hacking techniques. Hackers exploit software vulnerabilities, phishing and malicious programs to steal valuable assets such as users' accounts, passwords, bank information and even virtual currencies. In addition, the sale of personal information is also an indispensable part of the cyber theft behaviors. Hackers collect and aggregate various types of users' information, including names, ID numbers and contact details and sell them in bulk on the illegal web or trading platforms. The information is then used for illegal activities, such as targeted fraud and advertising harassment, which causes great distress and damage to the public.

2.2.5 Malicious software behaviors

The malicious software behaviors include behaviors committed to Trojans, viruses, and other ransomware. Trojan programs are often hidden in seemingly normal software, email attachments, or website links. Once downloaded or clicked by users, they run furtively in the back ends, stealing users' data and remotely controlling the devices. Moreover, viruses have the characteristics of self-replication and propagation, capable of rapidly infecting a large number of computers, damaging system files, tampering with the registry, and causing system crashes. Ransomware even encrypts user files as a threat, demanding victims should pay a high ransom for decryption. Take the "WannaCry" ransomware as an example. The Colonial Pipeline incident is one of the poorest victims that ransomware attacked in recent years. In May 2021, Colonial Pipeline, a major refined oil pipeline operator in the United States, was forced to shut down for five days due to a ransomware attack. Ultimately, Colonial paid nearly 5 million US dollars in ransom to cyber hackers to restore the attacked system [9].

2.3 Main Types of Cyber Gray Industries

2.3.1 Fake network traffic Industry

The fake network traffic industry includes activities such as traffic inflation, fan inflation, and review inflation, all aimed at creating a false impression of popularity or reputation, thereby misleading users and the market. In the realm of e-commerce, merchants, in an effort to enhance their store rankings and boost product sales, would hire people to engage in fake transactions, fabricating an illusion of soaring sales. On social media platforms, internet celebrities, stars, or self-media practitioners purchase followers, likes, and comments to forge an image of high popularity, thereby attracting more commercial collaboration opportunities. On content platforms, such as video-sharing websites and cyber literature platforms, creators or operators inflate play counts and reading volumes to deceive platforms into allocating recommended resources and sharing advertising revenue. According to the relevant data, on a popular short-video platform, the proportion of fake accounts among the followers of certain internet celebrity accounts is as high as 30%-50%. This phenomenon severely disrupts the platform system of fair competition, placing high-quality content creators in a predicament akin to "bad money driving out good," where subpar content creators may outperform those producing superior work due to fraudulent practices.

2.3.2 Personal information trading industry

The personal information trading industry has evolved into a clandestine industrial chain that spans from information collection, organization, to transaction. Information collectors, employing methods such as web crawling, hacking attacks, and insider leaks, illegally acquire a vast amount of personal information, and sensitive details like names, ID numbers, phone numbers, home addresses and bank information. They then engage in transactions on the dark web, illegal forums, or instant messaging groups. The buyers are predominantly telecommunications fraud perpetrators, marketing companies, and some PR teams.

2.3.3 Cyber advertising fraud industry

Cyber advertising fraud industry primarily encompasses forms such as ad view inflation, click fraud, and false promotion. Ad view inflation involves manipulating automated scripts or hiring manual view inflation teams to artificially inflate ad impressions and click-through rates, misleading advertisers into believing that their ad placements are highly effective. Click fraud utilizes technological means to simulate user click behaviors, defrauding advertisers of click fees. In some cases, ad networks even collude with fraudsters to share the ill-gotten gains. False promotion manifests as promoting products or services through false advertising and exaggerated claims, misleading consumers into making purchases.

2.3.4 Cyber black public relations industry

Cyber black PR industry often manipulates public opinion through means such as publishing negative information, deleting posts, and orchestrating cyber comments by paid commentators, serving the interests of specific groups. Black PR firms, hired by corporate competitors or individuals with self-serving interests, excavate negative materials about target companies, exaggerate or distort the reporting, and rapidly disseminate it cyber to damage the companies' reputations. If the targeted companies attempt to address the situation through public relations efforts, black PR firms may demand exorbitant fees for deleting the negative posts. Simultaneously, they organize paid commentators to post false remarks on major social media platforms, forums, and news comment sections, steering public opinion in a desired direction.

3. Current Legal Regulations of Cyber Black and Gray Industries

3.1 Laws and Regulations of Cyber Black Industries

Criminal Law: As the core legal instrument for combating cyber black industries, *Criminal Law* has established corresponding criminal charges and stringent sentencing standards for various types of cyber black industry activities. It regulates behaviors related to cyber black industries from multiple perspectives, such as hacking attacks and the creation and dissemination of malicious software, constructing a comprehensive criminal law defense line against cyber black industries.

Cybersecurity Law of the People's Republic of China: As a foundational law in the cyber domain, Cybersecurity Law plays a pivotal role in governing cyber black industries. It clarifies the security obligations of network operators, requiring them to adopt technical and other necessary measures to ensure cybersecurity, stable operation, effective response to cybersecurity incidents, and the protection of personal information security. For platform operators involved in cyber black industries, once they fail to fulfill their responsibilities in security protection, information review, etc., leading to the proliferation of black industry activities, they will have to bear corresponding administrative liabilities under this law, including orders for correction, warnings, and fines.

Public Security Administration Punishment Law of the People's Republic of China|: The Public Security Administration Punishment Law imposes public security administrative penalties on cyber black industry activities that do not constitute behaviors, thus playing a supplementary role in combating such activities.

3.2 Laws and Regulations of Cyber Gray Industries

Anti-Unfair Competition Law: The law provides a solid legal basis for regulating unfair competition behaviors within cyber gray industries.

Law on the Protection of Consumer Rights and Interests: This law emphasizes the protection of consumers' legitimate rights and interests in cyber consumption, thereby imposing constraints on cyber gray industries. In the context of the cyber advertising fraud industry, advertisements featuring false promotion and exaggerated efficacy mislead consumers into making purchases, infringing upon their rights to information and choice.

Interim Measures for the Administration of Internet Advertising: These measures further refine the norms in the field of internet advertising, explicitly stipulating that internet advertisements shall be truthful, lawful, and shall not contain false content or deceive or mislead consumers. With regard to behaviors such as ad view inflation and click fraud within the cyber advertising fraud industry, these measures prescribe corresponding regulatory measures and penalty standards. Advertisers, advertising operators, and advertising publishers who violate the provisions will face penalties such as orders for correction, fines, and suspension of advertising publishing operations. This serves to combat cyber gray industries from the perspective of advertising industry norms and purify the cyber advertising market environment.

4. Discussion

4.1 Governance Challenges for Cyber Black and Gray Industries

4.1.1 Technological difficulties

Cyber black and gray industries continually innovate their criminal methods by leveraging cutting-edge technologies, posing significant challenges to regulation and suppression. On the one hand, practitioners of black and gray industries are adept at utilizing emerging technologies such as blockchain, artificial intelligence, and encrypted communications to conceal their identities and obfuscate transaction paths, making traceability extremely difficult. For instance, in virtual currency money laundering cases, criminals exploit the anonymity of blockchain technology to rapidly transfer illicit funds across multiple virtual currency wallets, creating a convoluted flow of funds that traditional investigative methods struggle to penetrate and track. On the other hand, the tools used for criminal activities are becoming increasingly intelligent and sophisticated. For example, automated scripts and group control software are employed to carry out large-scale creation of false traffic and batch registration of accounts. The operational logic of these tools is so highly precise that makes detection and decryption a formidable task. Thus regulatory authorities often find themselves at a disadvantage in technological confrontations, struggling to promptly detect and effectively curb black and gray industry activities.

4.1.2 Legal dilemmas

With the rapid evolution of cyber black and gray industries, existing laws and regulations struggle to comprehensively cover new types of illegal and criminal activities. Some black and gray industry operations fall into legal vacuums, leaving law enforcement agencies without clear legal grounds to take timely and forceful measures. There exist numerous lags and ambiguities in the legal regulatory framework, which hinder the precise strikes against cyber black and gray industries. For instance, the legal provisions fail to precisely define covert data theft behaviors carried out using novel algorithms, making it difficult to determine their illegality. Moreover, issues such as poor coordination among different laws and regulations, and ambiguous scopes of application, give rise to jurisdictional disputes and divergences in legal application, which results in inconsistent judgments in similar cases within judicial practice and undermining the authority and deterrence of the law.

4.1.3 Regulatory challenges

The cross-regional and cross-departmental nature of cyber black and gray industries poses significant difficulties in regulatory coordination. From a geographical perspective, leveraging the internet, black and gray industries can instantaneously commit behaviors across national and provincial borders. Variations in regulatory policies and enforcement standards across regions, coupled with an imperfect information-sharing and collaborative linkage mechanism, create regulatory loopholes. Criminals exploit these gaps to evade detection by moving around and committing behaviors. In cross-border cyber gambling cases, for example, the operational teams of gambling websites are distributed across multiple countries and regions abroad, collaborating remotely with domestic agents and technical support personnel through encrypted communications. Due to issues related to jurisdiction and legal procedures, domestic and foreign law enforcement agencies face difficulties in synchronizing information and conducting joint operations in a timely manner.

From a departmental perspective, cyber black and gray industries involve the functional scopes of multiple departments, including cyberspace administration, public security, market supervision, and finance. However, the division of responsibilities among these departments is not clearly defined, leading to overlaps and regulatory gaps. This often results in buck-passing and a lack of regulatory synergy, making it difficult to implement effective control over the entire chain of cyber black and gray industries.

Meanwhile, as crucial carriers of cyber black and gray industries, network platforms often fall short in fulfilling their responsibilities in user verification, content supervision, and data protection, providing fertile ground for the proliferation of black and gray industries. Some platforms, in pursuit of traffic and commercial interests, turn a blind eye to fake accounts and non-compliant information. Even when aware of black and gray industry activities, they adopt a passive attitude, failing to take necessary measures such as banning or reporting, thereby indirectly condoning the widespread prevalence of cyber black and gray industries.

4.2 Countermeasures and Suggestions for Cyber Black and Gray Industries

4.2.1 Technological responses

Investing in technological research and constructing an all-encompassing and multi-layered technological prevention and control system are a must. On the one hand, the government may encourage research institutions and enterprises to develop monitoring, early warning and traceability technologies tailored to cyber black and gray industries. For instance, the police may leverage big data analytics technology to conduct real-time monitoring of network traffic and user behavior patterns, accurately identifying abnormal traffic and suspicious transactions. Artificial intelligence algorithms may be utilized to deeply mine vast amounts of data, discovering potential leads related to black and gray industries in advance. The immutable nature of blockchain technology can also be applied to store and certify critical data, ensuring the authenticity and integrity of electronic evidence and providing strong support for traceability and accountability. On the other hand, the government should establish cross-departmental and cross-industry technology sharing and collaborative response mechanisms to achieve technological interconnection and data exchange among regulatory authorities, internet enterprises, financial institutions, etc., breaking down information silos. Once signs of cyber black and gray industries are detected, all parties can swiftly collaborate and act in unison to sever the technological support chains of black and gray industries at the source, thereby enhancing the efficiency of suppression efforts.

4.2.2 Legal improvements

The existing laws and regulations needs to be revised promptly to fill legal gaps, refine legal provisions, and enhance the pertinence and operability of the law. Legislative bodies should closely monitor the development trends of cyber black and gray industries and, in light of emerging cases and technological characteristics, timely revise relevant laws such as *Criminal Law, Cybersecurity Law* and *Anti-Unfair Competition Law,* incorporating emerging black and gray industry into the scope of legal regulation and clarifying their elements of illegality and sentencing standards. Meanwhile, the Supreme People's Court and the Supreme People's Procuratorate should also issue judicial interpretations to unify the standards for legal application, resolve disputes over legal application, and provide clear guidance for judicial practice. In addition, given the transnational nature of cyber black and gray industries, actively strengthen international judicial cooperation, sign bilateral or multilateral judicial assistance agreements with other countries, and establish regular cooperation mechanisms in evidence exchange, extradition of criminals, joint law enforcement, etc., to jointly combat transnational cyber black and gray industry behaviors and safeguard international cybersecurity order.

4.2.3 Strengthen regulations

The government needs to further clarify the responsibilities and authorities of regulatory departments, optimize regulatory processes, and construct a regulatory landscape characterized by unified powers and responsibilities as well as efficient coordination. Through legislative or administrative provisions, the division of labor among departments such as cyberspace administration, public security, market supervision, and finance in the governance of cyber black and gray industries can be refined, thus avoiding functional overlaps and regulatory gaps. Establishment of a regular joint law and enforcement mechanism are also necessary on a regular basis to comprehensively combat cyber black and gray industries across the entire chain.

At the same time, we need to strengthen the main responsibilities of network platforms, urge platforms to improve their internal governance mechanisms, and enhance the review and supervision of key links such as user registration, content publication, and transaction behaviors. Technological means can be utilized to conduct real-time monitoring of platform data, promptly discovering and disposing of information and accounts related to black and gray industries. Moreover, we may try to establish a reporting and reward system for black and gray industries on platforms, encouraging users to actively participate in supervision, and providing material rewards and credit incentives to users whose reports are verified, fostering a favorable atmosphere of governance by people.

5. Conclusion and Prospects

Cyber black industries not only directly infringe upon individuals' property and privacy but also pose severe threats to the socio-economic order, cybersecurity, and even national security. Although they have not yet been explicitly defined as criminal by law, they significantly disrupt the fair competition environment in the market, infringed upon consumers' rights and interests, and undermine the healthy development of the cyber ecosystem. Both individuals' self-protection awareness in cyber socializing, consumption, and investment, and enterprises' fulfillment of responsibilities in platform operation, user management, and data protection, urgently need to be strengthened and improved.

Although China has established a legal framework including *Criminal Law*, *Cybersecurity Law*, *Anti-Unfair Competition Law*, etc., to combat cyber black and gray industries, issues such as legal lags, ambiguities, and poor coordination have become increasingly prominent with the rapid development of cyber technologies and the continuous evolution of black and gray industry forms, posing numerous challenges to law enforcement and judicial practice.

The governance of cyber black and gray industries faces multiple challenges in terms of technology, law, and regulation. At the technological level, practitioners of black and gray industries leverage emerging technologies to conceal their tracks and innovate their methods, often leaving regulatory authorities in a passive position in technological confrontations. At the legal level, legislative lags and uncertainties in legal provisions result in a lack of precise basis for law enforcement and inconsistent judicial adjudication standards. At the regulatory level, the cross-regional and cross-departmental nature of black and gray industries makes collaborative governance difficult, and the inadequate implementation of responsibilities by network platforms provides a breeding ground for black and gray industries.

In response to these issues, we have proposed comprehensive countermeasure suggestions covering multiple dimensions such as technology, law, and regulation. Technologically, we should increase R&D investment, construct an intelligent monitoring, early warning, and traceability system, and strengthen cross-departmental technological collaboration. Legally, we should promptly revise laws and regulations, refine legal provisions, unify judicial interpretations, and strengthen international judicial cooperation. In terms of regulation, we should clarify departmental responsibilities, optimize collaborative mechanisms, strengthen platform responsibilities, promote industry self-regulation, and construct a co-governance pattern involving the government, enterprises, and society.

In the future, the governance measures for attacking cyber black and gray industries will continue to evolve in the dynamic digital era. The legal regulations will be further optimized and improved and continue to refine and supplement the legal provisions. The judicial interpretation will also provide precise, clear and strong guidance for judicial practice, and ensure the unity and authority of the application of law. International judicial cooperation will increasingly work together to deal with and combat cross-border crimes of cyber black and gray industries.

References

[1]Anonymous. Five Typical Forms of Cyber Black and Gray Industries and Three Governance Suggestions.[EB/OL].http://www.whwx.gov.cn/wlzl/zljg/202201/t20220118_1908413.shtml. 2025-02-12.

[2]Anonymous. Data of Cyber Black Industry: Annual Research Report on Cyber Black Industry in 2023. [EB/OL].https://www.thepaper.cn/newsDetail_forward_26200441.2025-02-25.

[3]Threat Hunter. Research Report on Cyber Black and Gray Industries in the First Half Year of 2024.https://max.book118.com/html/2024/1013/7036144116006161.shtm. 2024-12-25.

[4]Anonymous. How to Prevent Cyber Black Industry Chain? [EB/OL].https://www.cac.gov.cn/2019-10/08/c_1572062776375154.htm.2025-01-27.

[5]Anonymous. Bengbu: Man, disguised as a lady, registered more than 20 WeChat messages and cheated dozens of male victims. [EB/OL].https://society.huanqiu.com/article/46Sl6a0asQH. 2025-02-26.

[6]Anonymous. Three million bills swiping with 50 million yuan involved! Heilongjiang police arrested tens of thousands of "Bill brushing" criminal gangs. [EB/OL]. http://www.chinapeace.gov.cn/chinapeace/c100044/2022-07/25/content_12651866.shtml. 2025-01-25.

[7]Anonymous. Cyber pornographic performances was uncovered: 4000 female anchors and more than 100000 registered users were involved [EB/OL].https://www.thepaper.cn/newsDetail_forward_26004604.2025-01-25.

[8]Anonymous. Sichuan Yibin Police cracked a 140million cross-border gambling case during the World Cup. [EB/OL].http://www.chinapeace.gov.cn/chinapeace/c100059/2022-12/14/content_12698996.shtml. 2024-12-25.

[9]Anonymous. Blackmail software is rampant: One more enterprise victim involved every four hours with the manufacturing industry as the greatest victim. [EB/OL].https://baijiahao.baidu.com/s?id=1766191971669481466&wfr=spider&for=pc.2025-03-01.

[10]Anonymous. Top Ten Cases of The People's Court in 2023. [EB/OL].https://www.court.gov.cn/zixun/xiangqing/422622.html.2024-12-30.

[11] Criminal Law of The People's Republic of China

[12] Cybersecurity Law of The People's Republic of China

[13] E-commerce Law of The People's Republic of China

[14] Anti-Unfair Competition Law of The People's Republic of China

[15] Law of The People's Republic of China on The Protection of Consumer Rights and Interests

[16] Interim Measures for The Administration of Internet Advertising

[17] Interpretation on Several Issues Concerning The Specific Application of Laws in Handling Criminal Cases of Gambling