Proceedings of the 2nd International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2024.BO17965

Multi-governance Model of New Cybercrime under the Risk of New Technologies Risks and Responses

Jiabao Li[1,a,*]

[1]*Media college, Shanghai Lida College, Shanghai, 201608, China*
a. lijiabao1111@outlook.com
**corresponding author*

Abstract: With the rapid development of science and technology, cyberspace has become the main position for new types of criminal activities, and new types of cybercrime, with its non-contact, inter-temporal and covert characteristics, have posed a serious challenge to the traditional mode of crime governance. The purpose of this paper is to analyse the specific manifestations of new technology risks and the characteristics of new cybercrime under new technology risks, explore the ways of coping with new cybercrime under the traditional governance model, summarise the transformation paths of the new cybercrime governance model of the public force model, the private force model, and the multi-dimensional common governance model, and analyse in depth its potential risks and coping strategies. This paper summarises three apparent risks, including privacy leakage risk, system security risk and fraud risk, as well as three potential risks caused by the diversity of governance subjects, the coordination difficulties, the balance between data sharing and privacy protection, and the rapid changes in new cybercrime and the lagging behind of governance means, and puts forward three potential risks accordingly, namely, strengthening the principle of openness and standardisation, cultivating highly skilled and complex talents, and perfecting governmental governance. Accordingly, three measures are proposed to strengthen the principle of openness and standardisation, cultivate high-tech talents and improve the governmental governance mechanism, providing theoretical support and practical guidance for the construction of an efficient and coordinated new cybercrime governance system.

Keywords: new technology risks, new types of cybercrime, diversified governance model.

1. Introduction

1.1. Selected Background

With the rapid development of science and technology, new technologies such as artificial intelligence, big data, cloud computing, and the Internet of Things have significantly enhanced people's lives. However, these technologies have also created new opportunities for cybercrime. Such crimes have repeatedly undermined the lawful rights and interests of citizens. In some cases, they even pose a threat to social stability and public security.

In China, for example, the 54th Statistical Report on the Development of the Internet in China, published by the China Internet Network Information Committee (CNNIC) on 29 August 2024, validates the increasing informatisation of society. This report reveals the new dynamics of China's

DOI: 10.54254/2753-7048/2024.BO17965

Internet development, with nearly 1.1 billion Internet users (1,099.67 million people) and an Internet penetration rate of 78.0 per cent as of 29 August 2024 [1]. At the same time, the acceptance rate of new technologies is increasing year by year. With such a large network base, it is not difficult to find that people are becoming more and more accustomed to accepting new technologies as well as information-based lifestyles. However, this has also led to the emergence of new types of cybercrime under the risk of new technologies.

On December 13, 2019, Baidu and the Third Institute for Legal Research of the Ministry of Public Security jointly released the "2019 White Paper on Cybercrime Governance and Prevention", which shows that the economic losses suffered by the world due to Internet crime are as high as $2.9 million, and the economic losses are as high as $1.5 trillion per year, and present a new state of upstream and downstream crime precision bundling, and intricate and complex crime patterns [2]. Moreover, with the development of new technologies, the means, subjects and modes of crime have also evolved. For example, blockchain technology provides greater security for financial transactions but is used by criminals for money laundering and fraud; the Internet of Things and remote control technology have brought about the popularity of smart homes but have also made it easy for hackers to break into home devices to conduct illegal surveillance or steal data. This "double-edged sword effect" has led to new complexities in social governance.

1.2. Literature Review

1.2.1. Review of National Literature

Zhang Jiahua believes that the perpetrators of crimes constantly update technology, resulting in a new type of cybercrime showing a trend of hybridisation and mutation, resulting in harmful consequences of seriousness, diversity and complexity [3]. In this regard, Zhang Jiahua points out that, in the face of an endless stream of new types of cybercrime offences, it is necessary to carry out purposeful prevention and control in accordance with their typical characteristics and outstanding problems [3].

Pi Yong proposes that the new type of cybercrime is an independent offence of disrupting the management order of information network security, and that it is a justifiable piece of legislation with the characteristics of a "cumulative offence", and that the application of its legislation should adhere to the principles of independent application and compliance with the principle of substantive justification [4].

1.2.2. Review of Foreign Literature

For new types of cybercrime, Germany and Japan limit the definition of constituent elements to qualitative aspects only, without quantification, and adopt a "legislative qualification, judicial quantification" approach [5]. Foreign scholars on the regulation of cybercrime pay more attention to the importance of government-led governance, for example, the American scholar Sunstein advocates strengthening the government's efforts to regulate network information, stressing that the government should proactively take measures to respond to bad information [6].The theory of regulation is elaborated by the British scholar Anthony in his work, who argues that the role of government regulation can correct market imperfections [7].

In the increasingly open Internet era, in order to curb new cybercrime, it is necessary first to adhere to the rule of law and strengthen all kinds of supervision; on this basis, it is necessary to intensify the fight against new cybercrime and establish a good interactive relationship with the public in order to better control new cybercrime.

DOI: 10.54254/2753-7048/2024.BO17965

1.3. Research Significance

This study aims to analyze the specific manifestations of new technological risks and the characteristics of emerging cybercrime under these risks. It explores methods of addressing new cybercrime within the traditional governance framework, summarizes the evolution of cybercrime governance from the public force model to the private force model, and ultimately to a multidimensional governance model. It also provides an in-depth analysis of potential risks and coping strategies, offering strong support for the study of "new cybercrime governance."

2. Specific Manifestations of New Technology Risks

2.1. Privacy Leaks Risk

The popularity of new technologies has made the collection and transmission of personal information more convenient, however, the concentration and sharing of big data have also increased the risk of data leakage, which will inevitably lead to the loss of personal property and damage to personal rights and interests once criminals make use of the new technological means to steal personal information and make illegal use of it. For example, people's mobile phones are loaded with a variety of applications, and when people download and use them, they often require a series of authorisations, such as access to photo albums, location information, etc. Often, in order to be able to successfully use these applications, people do not think about clicking on the "agree" without realising that this may lead to the leakage of personal privacy, and unscrupulous application developers Unscrupulous app developers may sell the information they receive to third parties, resulting in damage to personal rights and interests; In addition, people often connect to free WIFI, hackers may set up fake WIFI hotspots to lure people to connect, thus stealing the user's personal information in the network transmission, such as account passwords, bank card information, etc. Once this information is stolen, it will bring huge economic losses to the user.

2.2. System Security Risks

The complexity of new technologies can lead to security gaps in systems, providing opportunities for criminals to intrude. For example, the Internet of Things connects a wide range of devices, from smartphones to household appliances and even industrial equipment, yet the security of these devices is often overlooked and vulnerable to hacking; in addition, hackers can use AI algorithms to carry out phishing attacks, mislead users into clicking on malicious links or providing sensitive personal information, and also use AI technology to crack encryption algorithms and thus access encrypted data. This is a great threat to financial institutions, enterprises and personal privacy [8].

2.3. Fraud Risk

New forms of cybercrime often take advantage of the application of new technologies to commit various forms of fraud, such as financial fraud and phishing, bringing economic losses to individuals and society. Taking the data on cybercrime handled by Shanghai procuratorial authorities from January 2017 to October 2022 as a sample, the four major crimes of fraud, theft, casino crimes, and the crime of disseminating obscene materials (for profit) accounted for more than 55% of the total number of cyberfrauds accounted for the highest percentage of cyberfrauds and the rate of growth was obvious, with an average rate of growth of more than 20% over the past three years [9].

DOI: 10.54254/2753-7048/2024.BO17965

3. Characteristics of New Types of Cybercrime in the Light of New Technological Risks

3.1. Diversification and Rejuvenation of Criminal Subjects

As a result of the popularity of computer technology and network applications, the criminal subjects of new cybercrime have shown a trend of diversification. People of all professions, ages and statuses may be involved in cybercrime activities, and increasingly young people are becoming the main subjects of cybercrime. Taking minors' cybercrime as an example, with the network skills of criminal behaviour, the degree of physical dependence on natural crime decreases significantly, enhancing minors' ability to commit crimes; at the same time, the non-direct sensibility of the virtual society leads to a decrease in the sense of shame of minors' crimes, and the role of moral indoctrination in inhibiting the generation of crimes is relatively diluted, with minors' cybercrime appearing to be precocious and diversified.

3.2. Diversification and Concealment of the Means of Committing Offences

With the popularity of new technologies, new cybercrime methods are emerging, and criminals are constantly researching new technical loopholes and attack methods to evade security systems and surveillance. The combination of emerging technologies and traditional criminal means has also escalated into more sophisticated and covert cybercrime. For example, traditional telephone fraud has evolved into "voice imitation fraud" using artificial intelligence-generated voice synthesis technology, or anonymised money laundering through blockchain, while criminals have also used viruses, hacker attacks, phishing scams and other means to commit crimes such as information theft and fund transfers. Not only are these tactics difficult to detect, they also tend to be cross-border and cross-platform in nature, and modern cybercrime often involves the legal systems and law enforcement authorities of multiple countries or regions: criminals may manipulate devices in one country and commit fraud in another, while the stolen money is laundered in a third country through virtual currency. This transnational character makes existing single-country means of governance often inadequate, and highlights the importance of international cooperation.

3.3. High Impactrange of the Offence and Serious Harm

In China, the real danger of crimes against citizens' personal information is also growing due to the increasing degree of informatisation in China. Due to the openness of the Internet, objectively making the vast majority of crimes against citizens' personal information crime space has been greatly expanded, and the number of victims has also increased rapidly, which has resulted in a new type of cybercrime involved in a large range of cases, the social hazards, and the traditional "non-contact" is different. The behaviour is usually unnoticed after the victim has suffered harm, and it is not possible to find out in time that one's privacy has been illegally purchased and used, and thus not be able to report the crime in time. Normally, a downstream offence can only be found guilty after a more serious offence has been committed. Offences against citizens' personal information cause great damage to the normal order of life of the victim, the safety of his or her person and property and the security of national information. The resulting large number of downstream offences have had a huge impact on social stability and are potentially extremely harmful to society [10].

4. Exploration of New Cybercrime under the Traditional Governance Model

4.1. Ex Post Facto Responsiveness Type

In the traditional governance model, ex post facto responsiveness dominates. This model focuses on the pursuit of responsibility and punishment through legislative and judicial means after a crime has

DOI: 10.54254/2753-7048/2024.BO17965

been committed, and China's criminal policy for the punishment of crime is mainly set up on the basis of traditional crime, while the response to cybercrime along the lines of the traditional crime countermeasures does not fully take into account the characteristics of cybercrime itself [11].

Legislative embodiment: China through the enactment of relevant laws and regulations, has clarified the definition of cybercrime, sentencing standards and penalties, providing a legal basis for judicial practice. However, in the face of rapidly changing new forms of cybercrime, the problem of the lagging nature of the law is becoming more and more prominent.

Judicial manifestation: the judicial authorities investigate, prosecute and try cases of new types of cybercrime in accordance with the provisions of the law. However, due to problems such as difficulties in evidence collection and long crime chains, judicial practice often faces many challenges.

4.2. Ex-ante Intervention Type

To address the shortcomings of the reactive response model, the preventive intervention model has gradually gained attention. This model emphasizes the use of technical means and regulatory measures to detect and prevent cybercrime in advance. However, in practice, the preventive intervention model still faces challenges such as inadequate early warning mechanisms and the lack of targeted intervention measures. In order to compensate for the shortcomings of the ex-post response model, the ex-ante intervention model of governance has gradually gained importance. The model emphasises the early detection and prevention of cybercrime through technical means, regulatory measures and other means. However, in practice, the ex-ante model still suffers from problems such as inadequate early warning mechanisms, lack of targeted intervention measures and lagging legislation.

5. Transformation of the Governance Model for New Cybercrime

5.1. Public Power Model

The public force model, i.e. the government-led cybercrime governance model, stresses the decisive role of the government in the entire process of regulating cyber behaviour. A comprehensive, multi-level cybercrime prevention and control system is constructed by strengthening legislative, law enforcement and judicial forces. Specific measures include: improving cybercrime-related laws and regulations and enhancing the timeliness and accuracy of the application of laws; strengthening the construction of cyberlaw enforcement teams to enhance the effectiveness and level of law enforcement; and optimising the allocation of judicial resources to ensure that new types of cybercrime cases are dealt with in a timely and fair manner. Due to the leading role of the government, the public force model has stability and certainty in the process of combating cybercrime [12].

5.2. Private Force Model

The private force model refers to the model of free cooperation among private subjects in the governance of cybercrime, focusing mainly on the role of social forces and the self-purification and governance of cyberspace by means of industry self-regulation and technological protection. Enterprises, social organisations and individual netizens should actively take advantage of their inter-industry strengths, make use of their own technological advantages and resource conditions, and establish solid data sharing and exchange channels and platforms with each other, so as to build a cybersecurity line of defence and enhance the efficiency of combating cybercrime. At the same time, education on cybersecurity awareness should be strengthened to enhance the public's cybersecurity literacy and self-protection ability.

DOI: 10.54254/2753-7048/2024.BO17965

5.3. Multi-dimensional Governance Model

The multifaceted governance model, in which the public sector and the private sector, especially large Internet enterprises, work together to combat cybercrime, stresses the synergy of multiple actors, including the Government, enterprises, social organisations and the general public, in order to jointly address the challenges of new types of cybercrime. The model achieves effective integration and optimal allocation of governance resources through the establishment of a sound information-sharing mechanism, a mechanism for coordinated action and a mechanism for accountability. At the same time, it focuses on giving full play to the role of scientific and technological support, and applies advanced technological means such as big data and artificial intelligence to enhance the effectiveness and level of governance [13].

6. Potential Risks of a New Model of Multifaceted Cybercrime Governance

From the viewpoint of legislative content and specific practice, the new model of multiple governance of cybercrime has been an important model of cybercrime governance at present. However, in practice, the new model of multiple governance of cybercrime still has the following problems. When multiple subjects such as the government, enterprises, and social organisations participate in the governance of cybercrime, due to the differences in their respective goals, resources, and means, inconsistencies in coordination are prone to occur, thus affecting the effectiveness of the governance. Under the multifaceted governance model, all parties need to share a large amount of data in order to improve the efficiency of governance, but this may also lead to the risk of personal privacy leakage, triggering a crisis of public trust; as cybercrime techniques are constantly being updated, the speed of traditional laws and regulations tends to lag behind that of technological advances, and the technical capabilities of law enforcement agencies are difficult to keep pace with the rapid development of criminal technology. It is often difficult for the means of governance to keep up with this pace, leading to potential risks such as limited effectiveness of governance.

6.1. Risk Response to the New Cybercrime Multifaceted Governance Model

6.1.1. Adherence to Both Openness and Regulation

In the journey of constructing a new model of multifaceted cybercrime governance, it is particularly important to uphold the cornerstone principle of both openness and regulation. This principle requires breaking down traditional sectoral barriers and geographical shackles, realising cross-domain flow and efficient integration of governance resources, and promoting information-sharing and collaborative operations among various governance bodies. At the same time, it is necessary to strengthen the construction of a system of laws, regulations and standards, so as to ensure that every step of governance activities is on the track of legality and norms. This is not only about the legitimacy of governance activities, but also the cornerstone of maintaining order and security in cyberspace. Therefore, relevant laws and regulations should be continuously explored and improved, so that they can adapt to the rapid changes in cybercrime, but also effectively guide governance practices, and provide a solid guarantee of the rule of law for the construction of a pluralistic governance model.

6.1.2. Constructing the Cultivation of Highly Skilled and Complex Human Resources

The governance of new types of cybercrime cannot be separated from a team of composite talents with profound knowledge of cybersecurity, proficiency in legal provisions and proficiency in information technology. Such talents are a key force in promoting innovation in governance models and the application of technology. For this reason, it is necessary to actively build a high ground for

DOI: 10.54254/2753-7048/2024.BO17965

the training and introduction of talents, and to continue to inject fresh blood and wisdom into the cause of cybercrime governance by optimising the education and training system, expanding the channels for the introduction of talents, and formulating more attractive talent policies. At the same time, attention should be paid to upgrading the professional skills and comprehensive quality of existing governance personnel, so that they can adapt to the needs of governance in a new technological environment and become the backbone of a diversified governance model.

6.1.3. Deepening the Government's Governance Mechanisms

The government plays a pivotal role in the governance of new cybercrime, and the degree of improvement of its governance mechanism directly affects the effectiveness and direction of governance. Therefore, it is necessary to deepen the innovation and improvement of the government's own governance mechanism, and continuously improve the government's ability to deal with new cybercrime by promoting the optimisation of its internal governance structure, coordinating with the data management bureau as the competent authority, and introducing advanced governance concepts and technical means. At the same time, emphasis should be placed on the formation of a pool of experts as a third-party assessment and monitoring body to ensure the fairness and transparency of governmental governance activities and to enhance the public's trust in and support for governmental governance. This series of innovation and improvement measures will provide solid government support and guarantee for the construction of a diversified governance model.

7. Conclusion

The governance of new cybercrime is a complex and arduous task; the public force model is stable but has technological, data and efficiency disadvantages; the private force model can make use of industry resources but may bring about abuse of power and inequality; the public-private partnership model faces many conflicts and needs to seek a balance between the government and the private sector. Therefore, in order to deal with new types of cybercrime, it is necessary to construct an all-round and comprehensive governance system at the national level. The national level needs to build an all-round comprehensive management system, emphasising the integration of prevention, punishment and suppression, regulating the handling of electronic evidence, promoting uniformity in the application of the law and upgrading the use of technology; the social level needs to strengthen the leading role of governmental departments, with technical support from the private sector, and at the same time pay attention to the protection of and participation by all special groups; and the international level needs to strengthen the international cooperation known to the United Nations, insist on national sovereignty and actively participate in international rule-making. Only through the joint efforts and cooperation of the government, enterprises, social organisations and the public can people effectively safeguard the security and stability of cyberspace under the challenges of new cybercrime under new technology risks. Only by building a governance model of pluralistic governance and adopting corresponding risk response measures can people effectively respond to the challenges of new types of cybercrime under the risk of new technologies and maintain the security and stability of cyberspace. In the future, with the continuous development of science and technology and the continuous improvement of social governance system, people have reason to believe that the governance of new cybercrime will achieve more significant results and breakthroughs.

References

[1] *China internet network information center, The 54th Statistical Report on the Development Status of the Chinese Internet published ,2024.08, cnnic.net.cn.*

[2] *Baidu and the Legal Research Centre of the Third Institute of the Ministry of Public Security, White Paper on Cybercrime Governance and Prevention, 2019.*

DOI: 10.54254/2753-7048/2024.BO17965

[3] Zhang Jiahua. (2022) The Dilemma of Punishing New Cybercrime in the Era of Big Data and the Way Forward [J] Study and Practice, 05.006
[4] Pi Yong. (2018) On new cybercrime legislation and its application [J]. China Social Science, (10):126-150+207.
[5] Li Xiang. (2006) Study on Circumstances Offences, Shanghai: Shanghai Jiao Tong University Press, 73-74
[6] Cass R. (2009) Sunstein. On Rumors. America: Allen Lane,136.
[7] [English] Anthony Ogles, (2008) translated by Luo Meiying. Regulation: Legal Forms and Economic Theory. Beijing: Renmin University of China Press,15.
[8] He Zhe. (2020) Social Risk and Governance of Artificial Intelligence Technology [J]. E-Government, (09):2-14.
[9] Chinese Society of Criminology, Overview of the 2020 Annual Meeting of the Chinese Society of Criminology, 2020, zgfzxxh.com.
[10] Zhentian Zhang. (2015) Research on the characteristics of new cybercrime in the context of network era--Taking the crime of infringing citizens' personal information as an example [J]. Law and Society. (07).
[11] Shan Y. (2022) Sociological Research, School of Law, Nanjing University, Issue 4.
[12] Su Jiang.Associate Professor, School of Law, Peking University "Politics and Law", Issue 8, 2020.
[13] Duan Beiling. (2024) The Construction of Multi-dimensional Governance Model of New Cybercrime under the Risk of New Technology[J]. Network Security Technology and Application, (05):145-148.swsss