Trends in Social Sciences and Humanities Research
ISSN: 2959-9938
DOI: 10.61784/tsshr3032

REFLECTION ON STRENGTHENING THE GOVERNANCE OF NEW CYBERCRIME IN THE CONTEXT OF DIGITAL SOCIETY

Zhu Wen, LiNing Yuan*
School of Information Technology, Guangxi Police College, Nanning 530028, Guangxi Province, China.
Corresponding Author: LiNing Yuan, Email: yuanlining@gcjcxy.edu.cn

Abstract: In the context of the digital society, new types of cybercrime continue to breed and spread rapidly. The proportion of cybercrime cases in the total number of criminal cases is increasing year by year, making strengthening the governance of new types of cybercrime a key task for the development and stability of the current digital society. At present, research on new types of cybercrime mainly focuses on laws, regulations, and investigation techniques, lacking research on diverse integration mechanisms. Therefore, it is necessary to explore new ways to strengthen the governance of new types of cybercrime from the aspects of improving the legal system for the governance of new types of cybercrime, constructing cooperation mechanisms for the governance of new types of cybercrime, and innovating technological means for the governance of new types of cybercrime. The digital society is composed of a system of institutional guarantees at the upper level, an organizational management system at the middle level, and a technical system at the basic level. The governance of new types of cybercrime in the digital society also requires the joint efforts of three systems: a sound legal system guarantee, an active multi-party cooperation system, and effective governance technology support.
Keywords: New type of cybercrime; Governance; Digital society; Electronic data

1 INTRODUCTION

With the development of the information technology revolution, today's society is gradually moving into the era of a digital society, where digital technology has fully penetrated socio-economic life and become a new driving force for economic growth and social evolution. However, the rapid development of digital technology has also provided a unique breeding ground for cybercrime. The structural change of cybercrime is almost synchronized with the change of the status of the Internet in social development [1]. In the digitalized society, new types of cybercrime are constantly breeding and rapidly spreading, and the number of cybercrime cases in the total number of criminal cases is increasing year by year [2]. Unlike traditional crimes, cybercrime has moved from "face to face crime" to "digital crime", which is mainly manifested in the non-contact type of precise crimes, cross-border concealment with the support of science and technology, continuous renovation of deception techniques, industrial chain of criminal organizations and the trend of youthfulness of the subjects and victims of crimes. Victims show a trend of youthfulness, greatly increasing the difficulty of solving cases and making the social harm more and more serious. Therefore, strengthening the governance of new cybercrime has become an important factor affecting the transformation, development and stability of the digital society, and the governance of new cybercrime has a certain legal, technical and research basis. Based on the perspective of digital society, this paper puts forward the following thoughts on strengthening the governance of new cybercrime.

2 ANALYSIS OF NEW TYPES OF CYBERCRIME

Maintaining social security and stability requires making "severe punishment of cybercrime" an important task. This includes severely punishing crimes of stealing and trafficking personal information through fraudulent use of malicious programs, illegal intrusion into monitoring systems, and pursuing criminal liability for infringement of personal information and incitement to cyberviolence, insults, and defamation. This will create a clear cyberspace. New cybercrime is a prominent problem of the digital society, forming a "black and grey industrial chain" and criminal interest association in its development. Its manifestations are not limited to infringing property rights and personal safety, such as telecommunication fraud and gambling, but also include new economic and computer crimes. These pose a great threat to social order and stability.

2.1 Overview of New Types of Crime

The term "new cybercrime" has become a common phrase in media reports, especially in those related to the public security industry, in recent years. At present, there is no standard definition of "new type of cybercrime" in legal norms, but there are concepts such as "information network" and "information network crime" in the criminal law and network security law. The term "cybercrime" has become an important concept in legal norms. Additionally, there are numerous scholars researching and discussing new network crimes from perspectives such as judicial application, crime management, and development trends. Many police authorities have also established special new network crime investigation teams to conduct electronic forensics and crime management. Overall, cybercrime continues to evolve

alongside the development of network technology and changes in scholars' and the public security industry's understanding.

Early cybercrime referred only to the use of networks to commit crimes against the security of computer information systems, while with the development of Internet technology, new types of cybercrime emerged based on traditional cybercrime [3], manifesting in the use of information networks to commit a large number of hazardous behaviors [4], with cumulative hazardous consequences reaching the severity level of penalties imposed [5]. Entering the digital society, new cybercrime presents obvious features of grouping, industrialization, and intelligence, forming a black industrial chain of cybercrime with intertwined links [6] . At the level of judicial practice, cybercrime refers to crimes committed against information networks, crimes committed using information networks, and other upstream and downstream related crimes [7]. Based on the characteristics of cybercrime in the digital society, this paper generally describes new cybercrime as: a general term for actors or industrial chains using digital technology and digital devices to attack or destroy systems or information, or to commit other non-contact crimes, including mainly: new types of online fraud and gambling, new types of economic crimes and data theft crimes.

2.2 Dilemmas in the Governance of New Types of Crime

China Judicial Big Data Research Institute released a special report on "Characteristics and Trends of Information Network-related Crimes," mentioning that the total number of information network-related crime cases from 2017 to 2021 was more than 282,000, with the volume of cases showing a year-on-year increase. In 2022, the national police authorities continued to organize cluster battles and carry out intensive and concentrated operations, and successively carried out special operations such as "Cloud Sword", "Broken Card" and "Broken Flow". That year, a total of 464,000 cases of telecommunication network fraud were cracked. The Ministry of Foreign Affairs, the Supreme Court, the Supreme Prosecutor's Office, and the Ministry of Public Security jointly deployed the "Pulling Out the Nails" operation, and 240 leaders and backbones of wire fraud syndicates were successfully apprehended. The Supreme Prosecutor's Office released the "Work of Procuratorial Organs in Combating and Managing Telecommunications Network Fraud and Its Related Crimes (2023)," mentioning that from January to October 2023, procuratorial organs nationwide prosecuted more than 34,000 people for crimes of telecom network fraud, a year-on-year increase of nearly 52%. It can be seen that in a digitalized society, new types of cybercrime are developing rapidly and growing at an extremely fast rate. Although obvious results have been achieved in the fight against new cybercrime, the form of crime is severe and complex, and the fight against new cybercrime continues to be long-term, complex, and arduous.

New cybercrime has become a mainstream crime, with accelerated iterative changes in fraudulent techniques, intensified and upgraded offensive and defensive confrontations, and increasingly obvious transnational organized features. From the perspective of combating and governance practice, new cybercrime is a complex social governance problem. Due to its non-contact characteristics, new cybercrime is fundamentally different from traditional contact cases and has now developed into black and gray industry chains, terrorist activity crime networking, fourth-party payment problems, major public events, transnational cybercrime, which makes governance of new cybercrime face heavy challenges.

First, cybercrime is difficult to prevent. In many cybercrime cases, the education, knowledge, and social experience of perpetrators appear inferior to victims, but victims are actually facing a vast black and gray industry chain possessing broad knowledge and technology including psychology, economics, and new network technologies. As long as certain knowledge or technology exceeds victim cognition, criminals can defraud victims. Second, combating cybercrime is technically challenging. Some scholars analyzing authoritative data summarized cybercrime situations in various countries as "quadruple" - high-end technology, behavioral grouping, industrialized division of labor, and cross-border activities [8]. New cybercriminals leverage latest network communication technologies, black and gray industry chain support, and systematic division of labor and cooperation to set obstacles for tracking and conviction through cross-border, making timely, accurate governance harder. Third, cybercrime is hard to tackle. In actual case handling, criminals are organized, intelligent teams, and crime subjects are digital products, data systems, and other virtual objects, requiring inter-departmental public security cooperation and external carrier, bank, etc. data. Work barriers and procedural conflicts between units hinder efficient collaboration. In contrast, criminal gangs quickly accomplish goals via simple internet division of labor with no rules. Thus, case teams and criminal gangs exhibit stark efficiency and execution contrasts.

2.3 Significance of Cybercrime Governance

In a digitalized society, the network has evolved from an object and tool of crime to a space for crime, inevitably involving traditional crime in the network and increasing cybercrime frequency. The frequent occurrence of new types of cybercrime violates the legitimate rights of citizens, brings adverse effects to society, and induces other associated crimes, seriously jeopardizing social stability. Telecommunication network fraud and cross-border gambling account for a high proportion of new cybercrime. In October 2020, the Kunming Public Security Bureau in Yunnan Province successfully cracked a case supervised by the Ministry of Public Security, where Ms. Li's online dating partner, Wang Mou, introduced an investment app, initially promising high returns and inducing her to invest all savings, then losing her job and swindling her cash. The case is a typical example of online fraud in the name of love, where gambling sites and "investment platforms" promise "sweeteners" to lure victims into investing large sums and transferring funds. In

February 2020, police in Guangming District, Shenzhen City, Guangdong Province, cracked a burglary case leading to major cross-border online gambling criminal activities behind it. Burglar Li Mou was caught in a live game gambling scam, purchased coins to enter online gambling, owed high debt, and resorted to burglary unable to repay. The case shows internet gambling triggering associated criminal loan sharks and home invasion robbery, with great harm from cross-border gambling. According to police, offshore casinos and gambling sites increase recruitment of gamblers within countries, some criminals implementing telecommunication network fraud, the two criminal types colluding, even inducing kidnapping, detention, violence, and debt collection, with more prominent harm.

New cybercrime has brought many adverse effects to citizens and society, and its governance is of great practical significance. First, strengthening the governance of new cybercrime is an important guarantee of digital social stability. A large number of new types of cybercrime wandering in the gray zone and the edge of the law impact social governance and seriously threaten social stability. Some telecommunication fraud and illegal fund-raising on the Internet involve huge amounts of money and many people. Therefore, the governance of new network crime is not only related to the rights and interests of individual citizens but also closely related to social stability. Second, strengthening the governance of new cybercrime is an important foundation for developing a digital society. The development of a digital society involves the economy, culture, education, and other aspects, all moving forward on the road of digital transformation. Amid digital transformation, big data has become the main target of new cybercrime. Criminals steal, destroy, and misappropriate commercial data and citizen information, cheating money and controlling public opinion, seriously affecting social development.

3 NEW CYBERCRIME GOVERNANCE TECHNOLOGY

The techniques in the governance of network crimes refer to the application of cutting-edge technologies such as artificial intelligence, big data, and blockchain, combined with legal, social, and management approaches, to construct a comprehensive network security protection system. The aim is to prevent, detect, respond to, and recover from network criminal activities.

3.1 Big Data Analysis Technology

In today's digital age, big data analytics [9] stands out as a powerful and revolutionary tool, enabling precise and rigorous analysis of a vast ocean of diverse network data. This sophisticated technology has the capacity to uncover subtle hints of potential network crimes, deepening our understanding of the potential risks and characteristics of cyber attackers. For instance, we can harness the power of advanced machine learning algorithms and artificial intelligence technologies to conduct comprehensive and in-depth analyses of user behavior patterns. This helps us trace the origins of suspicious events and identify possible warning signs of criminal activity in a timely and efficient manner. Furthermore, Big Data Analytics can seamlessly integrate data from an array of sources and formats, constructing sophisticated crime prediction models. These models can forecast potential network crimes and provide invaluable insights for effective prevention strategies. The utilization of this cutting-edge technology significantly enhances our cybersecurity protection capabilities, safeguarding our digital assets and infrastructure.

3.2 Blockchain Technology

Blockchain [10], a unique technology with features such as decentralization, immutability, and traceability, is highly suitable for investigating and tracing network crimes. Its application can to some extent change the current situation of network security. By leveraging blockchain technology, network events can be recorded in real-time, accurately reconstructing the course of a case and providing law enforcement agencies with strong evidence. This also provides new possibilities for investigating network crimes. Furthermore, blockchain has applications beyond just this, such as in digital asset management and identity authentication. This "one stone, two birds" approach undoubtedly enhances network security protection capabilities and raises security levels in the network environment. Overall, blockchain's diversified applications bring more possibilities and expectations to our work in network security.

3.3 Internet of Things Security Technology

The widespread application of Internet of Things (IoT) security devices brings great convenience to our work and daily life [11], but also poses a novel and severe challenge to the field of cybercrime governance. Due to the relatively weak security protection capabilities of IoT devices, they are vulnerable to cyber attacks such as data theft or remote control. In this context, research and application of new network crime governance technologies has become essential and urgent. By establishing a comprehensive and efficient IoT security framework, these technologies aim to significantly enhance the security protection capabilities of IoT devices, thereby creating a more secure IoT environment. These technologies employ a series of innovative methods and measures to strengthen the security of IoT devices. For instance, by introducing advanced device authentication mechanisms, they ensure that only authorized devices can access the network, effectively blocking unauthorized access. Simultaneously, they adopt powerful data encryption techniques to ensure that the communication between IoT devices is not intercepted or tampered with during transmission, guaranteeing the integrity and security of the data. Furthermore, by utilizing edge computing technology, these

governance techniques can process and analyze data locally on IoT devices, not only reducing potential security risks during data transmission, but also enhancing the speed and efficiency of data processing.

3.4 Network Situational Awareness Technology

Network situational awareness technology [12] acts as a vigilant eye, constantly monitoring the rapidly changing network environment and promptly identifying abnormalities. It provides solid support for security alerts and emergency response execution, enabling effective network environment maintenance and protection. For example, leveraging artificial intelligence's powerful analytical capabilities for deep interpretation of various complex network traffic information, subtle access patterns not easily detectable can be identified. This allows for prompt warnings and blocking potential network attacks with decisiveness - a sharp sword, swiftly cutting through network crime threats. Additionally, network situational awareness technology can be deeply integrated and shared with cutting-edge technologies like big data and geographical information, constructing a comprehensive, three-dimensional network situational awareness system. This system, like a sturdy defense line, significantly enhances prevention and response to network crimes, making the network environment more secure and better protecting user information.

3.5 Intelligent Threat Perception

Intelligent threat detection technology [13], a core component of novel cybercrime governance technologies, harnesses advanced machine learning and deep learning algorithms to enable real-time analysis of massive network traffic and user behavior data. This enables identification of anomalous activities and potential threats. Compared to traditional methods primarily relying on preset rules, this technology demonstrates significantly higher accuracy and flexibility. For instance, APTs often conceal themselves in normal network traffic, making traditional detection methods difficult to detect their presence. However, by leveraging the capabilities of pattern recognition and behavior analysis offered by Intelligent Threat Detection technology, these concealed threats can be detected and pre-warned. This not only underscores the significant value of Intelligent Threat Detection technology in the field of cybersecurity, but also highlights its critical role in combating increasingly sophisticated cybercrimes. By deeply mining subtle features and behavior patterns of network activities, Intelligent Threat Detection technology provides a more efficient, intelligent solution for cybersecurity defense, significantly enhancing the security and stability of the network environment.

4 EFFECTIVE MEASURES TO PREVENT NEW CYBERCRIME IN DIGITAL SOCIETY

The digital society comprises an upper-level institutional safeguard system, an intermediate-level organizational and management system, and a basic-level technological system. Governance of new types of cybercrime in the digital society requires combined efforts of all three systems: a sound rule of law institutional safeguard, an active multi-party collaborative system, and effective governance technology support.

4.1 Strengthening Legislation and Improving the Legal System

Many countries have made many efforts to combat cybercrime by introducing targeted laws and regulations for corresponding cases. These laws and regulations, ranging from the security protection of information systems and the management of Internet security to the high incidence of telecommunication network fraud in recent years, as well as the recently introduced comprehensive legislation on cyber-protection for minors, have laid the legal foundation for cybercrime governance. In order to adapt to the development of a digitalized society and safeguard the rights and interests of citizens and social order, it is necessary to continuously improve the legal system for cybercrime governance in accordance with the development trend and characteristic laws of new types of cybercrime. However, although countries have been gradually improving laws and regulations involving cybercrime, the virtualization of cybercrime subjects, the cross-border of criminal groups, and the protection of information and conflicts of interest remain the greatest obstacles to combating and managing cybercrime and e-discovery, and the use of the inadequacy of the foreign-related legal system and the use of virtual IPs and cross-border crimes to carry out cybercrime in an organized manner and transfer assets abroad have become the focus of cybercrime governance. Therefore, it is necessary to strengthen the development and improvement of international cybercrime legislation in order to combat cross-border cybercrime and safeguard the rights and interests of citizens in accordance with the law.

4.2 Pluralistic Integration and Cooperative Mechanisms for Governance

The governance of new cybercrime in a digitized society is not limited to real space or cyberspace, but requires facing a "double-layer society" formed by the real and network societies, making cybercrime governance diversified and requiring joint cooperation from all parties. First, supervision should be combined and strengthened across networks, finance, and other industries, with strict control of capital flow and real-time monitoring of network information to create a clean network environment. At the same time, publicity on network security prevention should be increased, and the ability of the masses to prevent cybercrime improved. Public opinion media should be mobilized to remind network users of potential traps in online transactions, dating, and voice/video calls, which may involve AI-altered voices and faces. Users should always remain vigilant. The source of the criminal subject and victim should be killed.

Second, prevention and control should progress together, combining combative and defensive measures to maintain a severe stance on cybercrime punishment, especially for high-incidence, new types of cybercrime. Full-chain and specialized punishment should be adhered to, and typical cybercrime case reviews strengthened, optimizing wind control strategies in a timely manner through individual case investigations and forensics technology. Third, social co-rule requires regulatory authorities and enterprises to form linkages. Police internal network security and technical investigation departments should cooperate externally with operators, banks, third-party payers, network service providers, etc. on cases, building a mechanism for information interoperability and providing effective electronic data evidence. Intelligence on black and gray production, personnel, and technical databases should be shared.

4.3 Data Empowerment and Innovative Governance Technology Methods

New types of cybercrime in a digitalized society are characterized by digital technologies such as big data and artificial intelligence, so detection and governance means should be cut from their characteristics to empower the digital transformation of new cybercrime governance with data. First, strengthen the construction of technical capacity for investigation and forensics. New cybercrime is characterized by high intelligence, high technology, and high concealment, necessitating increased forensic capacity for new media and case-related software/APPs and expanded development of research and judgment application models for forensic data. Second, focus on innovating governance means ahead of time. Given the complexity of new cybercrime, governance means often lag behind crime technology, so strengthen forward innovation in governance means using data analysis to prejudge cybercrime means. Third, build a digital ecosystem. Realize intelligent networking of laboratory and forensic equipment networks, build a forensic knowledge ecosystem, upload existing forensic methods to the data center as reference methods for subsequent forensics, and realize the combination of individual ability and collective wisdom to improve crime governance efficiency. Finally, increase cultivation of high-level professional talents in network attack-defense and electronic forensics through targeted internal training and external introduction to expand the professional level of cybersecurity and technical investigation, combating new types of cybercrime from the source of technology.

5 CONCLUSION

In the rapidly evolving digital landscape, the emergence of new cybercrime has brought about a plethora of adverse effects on citizens and society at large. The governance of this new wave of cybercrime assumes immense practical significance. In the context of digital transformation, big data has emerged as the principal target of new cybercrime, exerting a profound impact on social development. The governance of this novel form of cybercrime encompasses not merely individual rights and interests but bears a direct correlation to social stability. Consequently, the fortification of new cybercrime governance assumes a pivotal role in the stability of the digital society, necessitating a perfect rule of law, active multi-party collaboration, effective technical support, and extensive media and public opinion propaganda, thereby instituting a transparent cyberspace.

FUNDING

This work was supported in part by the Social Science Fund of Guangxi under Grant 23FTQ005 and the Key Research and Development Program of Guangxi under Grant AB22035034.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Gottfredson M R, Hirschi T. A general theory of crime. Stanford University Press. 1990.
[2] Zhang Jiahua. The dilemma and approach of punishing new cybercrimes in the era of big data. Study and Practice. 2022(05): 85-95.
[3] Xue Tiecheng. The way to explain the crime of helping information network crime: the theory of accomplice and non-accomplice. Shandong Social Sciences. 2023(10): 175-184.
[4] Pi Yong. On the Localization and Internationalization of Chinese Legislation of Crimes in Cyberspace. Journal of Comparative Law. 2020(01): 135-154.
[5] Pi Yong. Legislation on the New Types of Cybercrime and Its Application. Social Sciences in China. 2019, 40(03): 152-173.
[6] Liu Yanhong. Intergenerational characteristics of Internet crime in Web3.0 era and criminal law response. Global Law Review. 2020, 42(05): 100-116.
[7] Yang Shuhan, Chen Zhijuan. Research on the path of law education of network security for college students in the new era. Legality Vision. 2023(23): 19-21.
[8] Zhao Liang. On the development trend of information network crime and the perfection of criminal policy. 2022(01): 122-134.

[9] Kumar Ravi, Nagpal Bharti. Analysis and prediction of crime patterns using big data. International Journal of Information Technology. 2019, 11(4): 799-805.
[10] Zheng Zibin, Xie Shaoan, Dai Hongning, et al. Blockchain challenges and opportunities: A survey. International journal of web and grid services. 2018, 14(4): 352-375.
[11] Alaba Fadele Alaba, Othman Mazliza, Hashem Ibrahim Abaker Targio, et al. Internet of Things security: A survey. Journal of Network and Computer Applications. 2017, 88: 10-28.
[12] Li Yan, Huang Guangqiu, Wang Chunzi, et al. Analysis framework of network security situational awareness and comparison of implementation methods. EURASIP Journal on Wireless Communications and Networking. 2019: 1-32.
[13] Rangaraju Sakthiswaran. Ai sentry: Reinventing cybersecurity through intelligent threat detection. EPH-International Journal of Science And Engineering. 2023, 9(3): 30-35.