Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/53/20240076

Adapting Law Enforcement Strategies: Correlating Traditional Crimes with Emerging Cybercrimes in the Internet Era

Yutong Ma[1,a,*]

[1]*Shandong University of Political Science and Law, Jiefang East Road, Lixia District, Jinan City, Shandong Province, China*
a. 1121087889@qq.com
**corresponding author*

Abstract: With the development of the Internet era, various new forms of cybercrime have frequently appeared, the current study aimed to clarify the correlation between traditional crimes and new cybercrimes, and to make feasible suggestions for law enforcement agencies in adjusting their law enforcement programmers' previous research has demonstrated the characteristics of new cybercrime and its various controversies in investigation, legislation and justice. The previous research has demonstrated the characteristics of the new cybercrime and its various controversies in investigation and legislation and justice. The enforcement process of law enforcement agencies is based on these previous controversial exploration programmers, and the governance of new types of cybercrime is much more difficult and controversial. Therefore, it is important to distil the commonalities between the governance model and judicial experience of traditional crime and apply them to new cybercrime.

Keywords: New cybercrime, Cybernation of traditional crime, dilemmas, governance

1. Introduction

Since 2018, the three Internet courts in Beijing, Hangzhou and Guangzhou have received a total of 217,256 new cases of first instance and other types of Internet cases, and concluded 208,920 cases, of which 15,327 cases were received in 2018, and 12,792 cases were concluded; 104,714 cases were received in 2019, and 99,405 cases were concluded; and 97,215 cases were received in 2020, and 96,723 cases were concluded. Some other courts have also heard a large number of Internet cases. Overall, the number of Internet cases is growing year by year, involving new, complex and difficult legal issues, and the people's courts are facing more and more new challenges and difficulties. With the rapid development of the Internet society in China, there are many changes in the forms of cybercrime and numerous means of committing cybercrime, which also creates difficulties in governance for law enforcement authorities. The impact of new cybercrime on the legislative and judicial fields has always been a hot issue in the cyber era, and there has been a large amount of literature [1][2][3] that has studied the characteristics of new cybercrime, the challenges it poses, and the measures of governance. These studies have achieved refinement in various areas of new cybercrime, however, they lack a transition between traditional and new cybercrime. In this

DOI: 10.54254/2753-7048/53/20240076

regard, this paper will develop this transition. As the new cybercrime is an altered form of cyber-mediated traditional crime, this paper builds on the differences and transitions between traditional and new cybercrime to show how law enforcement can proactively adapt a response and the positive value of that response for the future in the area of cybercrime governance.

2. Literature Review

2.1. Research on new cybercrime techniques

2.1.1. Current context of new forms of cybercrime

There are many different starting points for the definition of new cybercrime, which from a literal point of view, is a newly emerging form of crime. From the perspective of Chinese criminal law, a new type of cybercrime is a form of crime that undermines the order and security of cyberspace. The first division by old and new is too broad, which affects the normal induction and the proposal of corresponding strategies, and the second from the criminal law, the offences in the amendment of the criminal law do not cover all its features well. To sum up, the new type of cybercrime should be a product of the stage of development of the socialization of cyberspace, and is a general term for behaviors such as destroying the security of information and data and obstructing the order of the network with the help of the black and grey industrial chain of the network as a tool.[1]According to Chen Longxin, new types of offences committed against networks and offences committed using networks are classified according to whether or not the information directly contributes to the network. In terms of the area of specialization of the offence, it is further divided into the categories of material supply, reliance on technical support and financial settlement. [1]

2.1.2. Characteristics of new types of cybercrime

According to author Jiang, the characteristics of new cybercrime arise from the influence of its new social environment, which, compared with traditional types of crime under the influence of the traditional social environment, is free from the restrictions of geography and identity, and has a stronger sense of concealment, confusion and convenience, but, leaving aside its external modifications, the essence of its crime is not different from that of traditional crime.[4] Essentially, the new cybercrime is characterized by a blend of digital-age features and a new form of traditional crime. From a law enforcement investigation, new cybercrime is different from the investigation of traditional crime in that, after a case is filed, the investigating authorities investigate and restore the scene; cybercrime is non-contact, and a large number of cases cannot be restored to the scene and involve many areas of the Internet that are not covered by the law. At the same time, new types of cybercrime are mostly committed by gangs, with a long criminal industry chain[1] and dispersed personnel, making it difficult to capture evidence in a timely manner for key links and to completely destroy the industry chain, thus affecting the efficiency of law enforcement agencies.[5] [6]

2.2. Links between traditional and new forms of cybercrime

2.2.1. Intergenerational renewal from traditional to new forms of cybercrime

In the past, the focus of criminology was mainly on the articulation of traditional crime; with the emergence of the digital age, real and virtual societies are intertwined, closely interacting with each other, and causing each other. The dominant criminological theory of urban attraction to criminals has gradually shifted to cyber-attraction to crime. [7]

DOI: 10.54254/2753-7048/53/20240076

The Internet attracts crime, and a quality Internet fosters excellence, but the breadth of the Internet also provides opportunities for criminals to take advantage of it. China has the world's largest Internet population, an Internet infrastructure that spans multiple geographic regions, and Internet patterns and technologies that are in sync with the world's advanced Internet technologies. The evolution of new types of cybercrime in China is highly compatible with generational differences in the Internet. [8]Starting from the position of the network in cybercrime, traditional crime has gone through three stages of development after its intergenerational update to cybercrime: cybercrime as object, cybercrime as tool and cybercrime as space.

2.2.2. Differences and similarities between responses to traditional crime and new forms of cybercrime

Both are similar in that they are guided by the general provisions of the criminal law and are convicted and sentenced with the help of the provisions in the sub-principles of the criminal law. The difference lies in the characteristics of the two, with new cybercrime being a more digitally-enabled form of crime, which has special characteristics in terms of response. Amendment to the Criminal Law responds to the trajectory of cybercrime practice, based on the "3+1" counterattack model. In the macro aspect, the criminal legislation realizes three modes of responsibility: the criminalization of complicity, the implementation of preparatory acts, and the platform responsibility of network service providers, so that new cybercrimes can be accurately cracked down on in accordance with the characteristics of new cybercrimes, and criminal responsibility and punishment can be realized. At the macro level, criminal legislation has realized three modes of liability, namely, the formalization of complicity and the implementation of preparatory acts and the platform liability of network service providers, so as to combat new types of cybercrime with precision and achieve a balance between crime and responsibility. [8]Additionally, in terms of the construction of offences, cybercrime is different from traditional crime in that it has the characteristic of "accumulating quantities to constitute an offence", and the application of the relevant provisions of the Criminal Law has encountered difficulties, and it is difficult to achieve theoretical self-consistency in accordance with the interpretation of the relevant theories of substantive preparatory offences and helping offenders.[9]

2.3. Law Enforcement Adapts Measures to Address Emergence of New Types of Cybercrime

2.3.1. Difficulties in the governance of new cybercrimes

Du Wenhui pointed out that firstly, cyberspace is divided into three levels, namely, the surface level and the deep level, with the deepest level being the dark web, which has a hidden carrier due to the fact that the network transmission software used is different from that used at other levels. Under the protection of concealment, the dark web breeds more opportunities for crime and makes it more difficult for law enforcement agencies to investigate. At the same time, the darknet also involves cross-field and transnational types of cybercrime, which involves jurisdictional issues and differences in ideology and values between countries, all of which increase the difficulty of implementing regulatory measures. Secondly, the information and network age are rapidly developing and changing. However, the legislation, formulation, modification and implementation of laws require a lot of time and procedures to ensure their rigor, which makes the two cannot be synchronized, and the law has a lag in applying new types of cybercrime. Finally, cybercrime subjects are diversified, offenders are involved in many cases, evidence is difficult to collect, and the randomness and variability of their cyberspace is too great.[3]Author Li Yajie and Guo Qi further indicated that on the issue of evidence collection, compared with traditional crime, most of the evidence collection for cybercrime is the collection, extraction and fixation of electronic data,

DOI: 10.54254/2753-7048/53/20240076

but because of the special characteristics of cyberspace, evidence also has a changeable nature, making it difficult to retain a timely and complete chain of evidence.[10] Author Chen Longxin and Shasha also have supplementary to the investigation and evidence collection process of the new network of hidden, dispersed and intelligent, increasing the difficulty of evidence detection also for the subsequent recovery of stolen goods, how to identify the stolen money and other issues to pave the way. In terms of the application of the law, new types of cybercrime face difficulties in identifying the subjective aspect, as well as a longer criminal chain and communication through the medium of the Internet, leading to a blurred sense of criminality between upstream and downstream. The nature of the act is also difficult to qualify because of the variability of the information network, and many crimes that were previously thought not to occur through the network have also appeared, such as indecent assault through the network, for which there is no precedent of judicial practice for law enforcement agencies to follow, but the rights of citizens cannot be unprotected. In terms of judicial application, the new cybercrime offences themselves are relatively low in social harm, the plot elements are highly elastic, and the relevant judicial application standards are unclear, leading to a low rate of application and undue expansion of the criminal circle; in order to maximise the effectiveness of the legislation, it is necessary to formulate relevant and reasonable judicial rules based on the unique structure of the offences themselves, reasonably limiting the constituent elements of the offences and providing a typological and qualitative interpretation of the plot elements. [9]At the same time, the issue of conviction for offences is also controversial; some cybercrimes are in fact just traditional crimes in a cyber-shell, but because of the novelty of the form of the case and the high level of public attention, their conviction is also facing controversy. [10][11]

2.3.2. Existing governance programmers and innovations for new forms of cybercrime

Author Li Yajie and Author Guo Qi pointed out that it is imperative to improve the laws and regulations, applying first and foremost administrative regulations and using criminal means with caution. A distinction should also be made between the application of offences and traditional crimes, which, although similar in nature, also require special attention to the determination of offences, as there are no precedents in judicial precedents.[12] In the construction of the evidence system should focus on public-private cooperation, professional things to the professional field of technical personnel to join, open up the technical experts to participate in the case of evidence collection, to improve the objectivity of evidence collection. And constantly resort to the technology of outside professional companies to improve the ability of law enforcement agencies to obtain evidence. While ensuring efficiency, it is also necessary to ensure the standardization of forensics, the preservation of original evidence and the timely extraction and fixing of evidence. [13]At the legal level, law enforcement agencies are more concerned with controlling and rationally dividing the work of investigation, justice and trial. However, the Internet also requires the intervention of law enforcement agencies to control and improve it. Author Jing Honghao pointed out that improvements should be made to the network so that it conforms to the laws of the information network, is logically self-consistent and operable, and the network will be more orderly with legal intervention. It is also necessary to carry out typological research on networks, make positive connections between types of cybercrime and types of legal protection, and explore a new model of cybercrime governance with Chinese characteristics. He also pointed out that in the 21st century, researchers of cyber-criminal law theory need to fulfil their mission of the times by understanding cybercrime on the basis of scientific rationality, responding to cybercrime on the basis of social rationality, and integrating systematic thinking with problematic thinking, so as to provide systematic protection for the entire cyber social system at the level of criminal substantive law.[14][15] The dilemma of law enforcement authorities, whose governance is based on the

DOI: 10.54254/2753-7048/53/20240076

investigation, prosecution and trial phases, also lies in the fact that legislative and judicial issues have not been adequately addressed and that the application of penalties for offences and punishments has not been proportional to the speed of the emergence of cybercrime. This has led to the work of law enforcement authorities lagging behind the emergence of new forms of cybercrime to a certain extent. In this context, the cybercrime of traditional crime is of great interest and relevance. Law enforcement departments should take the similarities between traditional crimes and new cybercrimes as a starting point, focus on the innovative points of the criminal means and results of new cybercrimes, and conduct timely expansion and seminars with reference to relevant judicial cases, so as not to allow the law to lag too far behind the judgement of the case. At the same time, law enforcement departments should strengthen cross-departmental and cross-regional collaboration and co-operation, introducing and going out. High-tech technologies developed by experts in the cyber sector and cyber technology will be brought in and integrated with the legal network, and publicity and education will go out to reduce the incidence of cybercrime.

3. Conclusion

The purpose of this study is to discover the commonalities and differences between traditional crimes and new cybercrimes in the process of their transformation into new cybercrimes, and to propose policies on how law enforcement departments should adjust their policies in conjunction with other studies on the types, characteristics and difficulties in the management of new cybercrimes. Law enforcement agencies should cooperate with each other and perform their respective duties to achieve the accurate collection of evidence, the correct use of offences and the appropriateness of guilt and punishment for new cybercrime at the stages of investigation, prosecution and litigation, and pay attention to the innovative points of the means and results of new cybercrime, which can be applied by analogy with the judicial interpretations of previous legislation on traditional crime.

References

[1] *Chen Longxin, Sasha, Study on the Systematization of New Cybercrime Governance,journal of Journal of Shanghai Public Security College, 2023, p.36-41*

[2] *Pi Yong, Prevention and management of new cybercrime,2016, p. 11-16.*

[3] *Du Wenhui, Study on the Criminal Law System of Cybercrime,2020, p.25-45*

[4] *Jiang Wenrong, Characteristics, Causes and Response Strategies of New Types of Crimes in the Age of Big Data, journal of Hang Zhou Normal University Humanities and Social Sciences, 2020, p. 130-132.*

[5] *Chen Yun, An Analytical Study of New Types of Cybercrime in the Age of Big Data, journal of China Security, 2023, p.104-106.*

[6] *Liu Yanhong, Research on cutting-edge issues of new cybercrime,journal of Articles,2023,p.57*

[7] *Shan Yong, Generational renewal from traditional to digital criminology, Journal of Shanghai University (Social Sciences Edition),2023, p. 2-4*

[8] *Yu Zhigang, Intergenerational Evolution, Criminal Law Samples and Theoretical Contributions to Cybercrime in China, journal of legal forum, 2019, p.5-7*

[9] *Pi Yong, On the new cybercrime legislation and its application, China Social Science Journal, 2018, p.126-130*

[10] *Meng Xiaofan, Difficulties and Paths in the Governance of New Cybercrime,journal of Network Security Technology and Application, 2023, p.142-143*

[11] *Zhang Jiahua, The Dilemma of Punishing New Types of Cybercrime in the Age of Big Data and the Way Forward, journal of Learning and Practice,2022, p.85-95.*

[12] *Li Yajie, Guo Qi, Problems in the Judicial Application of New Types of Cybercrime and Strategies for Responding to Them, journal of legal system,2022, p.7-9*

[13] *Kim Hong-ho, Systematic change of the theoretical paradigm of cybercrime criminal law, journal of China Law Review,2023, p.124-131.*

[14] *Ouyang Benqi, Wang Qian, Amendment (IX) to the Penal Code adding the legal application of cybercrimes, Journal of Jiangsu Administration Institute,2016, p. 126-128*

DOI: 10.54254/2753-7048/53/20240076

[15] *Yu Haisong, Legislative Expansion and Judicial Application of Cybercrime, journal of Application of the law, 2016, p.2-10.*