Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime

XiaoLing Wang*
Hainan College of Economics and Business, China, 571127

*Corresponding author e-mail: xiaolingwang@163.com

Abstract. As the development of artificial intelligence (AI) is unfolding, cybersecurity faces the invasion of AI. AI-based cybercrime becomes a product of technological development, posing a threat to national security, public security, and the protection of citizens' personal property rights and privacy rights. In particular, the derivation of cybercrime that follows the development of science and technology leads to a qualitative change in the patterns of cybercrimes, expanding the scope and depth of the harm caused by cybercrime, producing a series of impacts on the conviction rules of traditional criminal law in China. The defects such as the features of the principal offender being weakened, the definition of the responsibility for accessory to the principal offender not clear, the narrow scope applicable to one-sided accomplice are present. To this end, in the era where AI and cybercrime have deep integration, given the derivative trend of AI-based cybercrime, it is urgent to adjust the focus of criminal strategy against cybercrime. The horizontal docking of domestic substantive law and legal interpretation is performed to achieve a gradient balance between judicial interpretation and legislative amendment and adjust the criminal boundary in cybercrime evaluation, thereby changing the current high threshold of conviction in the cybercrime governance and late launch of punishment power.

Keywords: Cybersecurity, AI, Cybercrime, Legislative Improvement, Criminal Policy

1. Introduction
We are on the eve of a new round of scientific and technological revolution. The sense of survival crisis thus triggered covers every one of any gender, race, or country[1-2]. Human beings have experienced thousands of years of vicissitudes from the primitive society of taking fire from brick and wood to the agricultural to the industrial society [3-4]. Nowadays, the network impact brought by the information age expands the social activity scope of each unit in the social organization structure from the physical space to the network space. The expansion speed may be in years, or in five years as an iteration cycle. Therefore, we need to go with the times and accompany the self revolution. In the era
of AI rapidly occupying the market, it has changed our cognition of cybersecurity [5-6]. For example, AI with deep self-learning feature has learned and completed the chess manual accumulated by a human for thousands of years in a unit of days. Under the rational perspective of “the future is here”, we are naturally required to pay attention to cybersecurity, facing the reality of AI accelerating the alienation of cybercrime, update the value orientation of cybersecurity at the national level and in the public and private fields, and at the same time carry out beneficial exploration in the criminal legal system.

2. From the era of the traditional internet to AI: Iterative evolution of cybersecurity

With the iterative evolution of the network, the content of cybersecurity has changed greatly. In the traditional network era, the content of cybersecurity is based on the physical stability of the network. Today, cybersecurity has completed the transformation from the media to the carrier of national security, public security, and economic security, and realized the shift from the focus of work and life to the online and the transition of network space.

| Table 1. layer appearance of cybersecurity content in the traditional network era |
|----------------------------------|---------------------------------|---------------------------------|
| Times series | Types of cybersecurity | Content of cybersecurity |
| Network 1.0 Era | system safety | Illegal intrusion |
| | data security | Illegal acquisition, theft and use |
| Application Security | Destroy application and software |

In the era of AI, the legal interest of cybersecurity is not a single legal interest, but compound legal interest. With the high dependence of the whole society on the network and the living of intelligent technology, paying attention to cybersecurity is to pay attention to national public security, public security and information security, which is also the logical starting point of studying cybersecurity.

| Table 2. layer appearance of cybersecurity content in the era of AI |
|----------------------------------|---------------------------------|---------------------------------|
| Times series | Types of cybersecurity | Content of cybersecurity |
| The age of AI | Space Security | National security, public security, economic security |

3. Impact of AI-based criminals on cybersecurity in the era of AI

Whether it is the crime against computer software and computer information system in the pre network era or the increasingly rampant cybercrime in recent years, it can be punished based on the traditional criminal law system and charges, which has not yet brought impact on the application of criminal law rules. AI-based cybercrime contains higher technology content than the general cybercrime. However, it also means that once the technology innovation, the harm and victims of cybercrime are exposed to a series of criminal risks. The essential reason for these risks is that each of us is in the development process of cyberspace.

Given the sample data set, \( D = \{x_1, x_2, ..., x_n\}, x_i \in R^d, i = 1, ..., n \). Assuming that the first sample is labeled, mark it as \( e = (x_1, x_2, ..., x_i) \), and the corresponding label is \( \eta = \{y_1, y_2, ..., y_i\} \).

Consider the problem of classification, and note the following symbols:

\( S = \{(x_i, x_j) \colon x_i \text{ and } x_j \text{ is the same kind. } x_j \text{ is } x_i \text{ neighbor}\} \).

\( R = \{(x_i, x_j, x_k) \colon x_i, x_j \text{ is adjacent and in the same class, } x_i \text{ and } x_j \text{ in various classes}\} \).

The importance of each feature dimension in the classification problem is different. To a certain
extent, the cybercrime data can overcome the shortcoming that the cybercrime data treat each feature dimension equally. Its definition is as follows:

The cybercrime data between samples \( x_i \) and \( x_j \) are defined as follows

\[
d_A(x_i, x_j) = \sqrt{(x_i - x_j)^T A (x_i - x_j)}
\]  \hspace{1cm} (1)

\( x_i \in \mathbb{R}^d, A \in \mathbb{R}^{d \times d} \) stands for a symmetric semi-positive definite matrix

According to the properties of positive semidefinite matrix, \( A \) decomposable into \( A = L^T L \), the above equation can be expressed as follows:

\[
d_A(x_i, x_j) = \sqrt{(x_i - x_j)^T L^T L (x_i - x_j)}
\]
\[
= \sqrt{(Lx_i - Lx_j)^T (Lx_i - Lx_j)}
\]  \hspace{1cm} (2)

This is equivalent to the matrix as a mapping, mapping the data in the original space to the new space, and converting the cybercrime data in the unique space to the cybercrime data in the new space.

As far as AI-based cybercrime is concerned, we should clarify whether it is the cyber crime committed by using AI technology or the criminal behavior caused by AI simulation. The cybercrime supported by AI technology is mainly criminal behavior caused by the extensive use of AI technology. The crime caused by AI simulation is mainly due to the design loopholes of AI technology. This paper mainly discusses the use of AI skills in the implementation of cybercrime. This consideration is based on the fact that from the industrial revolution to the post-Internet era, every technological innovation has brought some changes to our lifestyle, and we are experiencing the convenience of AI technology every time. At the same time, we are worried about the popularity of this technology. The rapid penetration of AI technology in daily life will not make all cybercrimes upgrade iteratively, but it will indeed hatch new methods of cybercrime.

4. Positive feedback of AI-based cybercrime: Guarantee of cybersecurity based on criminal law in the era of AI

The negative effect of the development of AI technology is the AI of cybercrime, which reveals the mutual flow between technology and law. Today’s cyberspace is no longer a pure place for data exchange, but a quasi-real world constructed by information technology. It almost provides the same place for human activities as the reality and the world and makes all preparations for physical social behaviors such as food, clothing, housing, and transportation. After human behavior extends to the network world, the legal rules of the real world also need to enter the network space, especially in the era of AI. When facing new social problems, China tends to solve them through legislation. For example, in dealing with the issue of cybercrime, we should directly criminalize the preparatory act through legislation and set up the crime of “helping information cybercrime”, but their application is conditional and can not fundamentally solve the high incidence of cybercrime. Our legislative act is
certainly proactive. However, it is impossible to address new problems through legislation immediately, which is contrary to the modesty of criminal law and the spirit of the law. We need to find a balance between legislation and justice in the face of a new round of technology, that is, objective interpretation, to implement the national responsibility of maintaining cybersecurity. Objective interpretation emphasizes that legal interpretation is not only about revealing the legislative intention, but also exploring the legal essentials in line with social development from the legal norms. It can flexibly resolve the rigidity of substantive law in the governance of cybercrime. The reasons are as follows: first, objective interpretation theory is the most influential theory of legal interpretation today, following the pulse of scientific and Technological Development and making objective and appropriate legal interpretation is the fundamental task of fair interpretation and the product of the development of AI technology and positivism. Second, the objective interpretation makes up for the mechanical nature of the article itself. Through the vitality of language and words, objective interpretation revives the criminal charges and enables the traditional criminal law system to show its vitality in cyberspace. Thirdly, objective interpretation is conducive to the realization of fairness and justice. An objective interpretation has important significance in alleviating the rigidity of law by focusing on the exploration of the essence of law while exploring the law of social development. Judge Richard A. Posner once said that he knew the basic features and necessary background knowledge of a technical field through his assistants who had dealt with science, which would help him to conduct a fair trial. Therefore, “the law should go deep into the essence rather than the reality, and pay attention to the spirit rather than the literal meaning” has become the guiding ideology of objective interpretation in the governance of AI-based cybercrimes. Expansion of the punishment scope in the current criminal law through objective interpretation does not lead to the trend of the abuse of penalty power leading to the expansion of charges, because the objectivity and preciseness of objective interpretation need to pay attention to the circumstances of the crime, and the use of “serious circumstances” to limit the interpretation can avoid the expansion of charges. Furthermore, we should clarify the independent status of the crime of information cybercrime as the principal offender through objective interpretation, and reduce the conditions for criminal conviction, thereby preventing the crime from being vacant in the future judicial activities, and improve the practicality of the crime.

5. Conclusions
Einstein once said, “I never think of the future – it comes soon enough.” We are now in the dawn of the AI era, when the forms of cybercrime are changing with each passing day. The theoretical exploration and institutional innovation of cybersecurity triggered by the intelligent revolution is in full swing. We need to ensure that the first concern of AI-based cybercrime – stable implementation of cybersecurity before carrying out subsequent studies. Under this background, the study of cybersecurity and criminal law should not be delayed or even absent. It is imperative to make the technological development and legal rationality shine in the era of AI.

References
[1] Xu, J. J. , & Chen, H. . (2015). Crimenet explorer: a framework for criminal network knowledge discovery. ACM Transactions on Information Systems, 23(2), 201-226.
[2] Brahan, J. W. , Lam, K. P. , Chan, H. , & Leung, W. . (1998). Aicams: artificial intelligence
crime analysis and management system. Knowledge-Based Systems, 11(5-6), 355-361.

[3] Ai, X. . (2014). Inferring a drive-response network from time series of topological measures in complex networks with transfer entropy. Entropy, 16(11), 5753-5776.

[4] Tomás-Rosselló, Juana, Rawson, R. A. , Zarza, M. J. , Bellows, A. , Busse, A. , & Saenz, E. , et al. (2010). United nations office on drugs and crime international network of drug dependence treatment and rehabilitation resource centres: treatnet. Substance Abuse, 31(4), 251-263.

[5] Costa, J. P. , Jo?o C. Climaco, & JoséF. Craveirinha. (1992). On the potentialities of ai to deal with the combinatorial complexity of a telecommunication network planning problem. Engineering Applications of Artificial Intelligence: The International Journal of Intelligent Real-Time Automation, 5(1), 59-68.

[6] Yuanqing Qin, Qi Zhang, Chunjie Zhou, & Naixue Xiong. (2018). A risk-based dynamic decision-making approach for cybersecurity protection in industrial control systems. IEEE Transactions on Systems Man & Cybernetics Systems, PP(99), 1-8.