I. Introduction

With the rapid development of information technology, cybercrime has gradually become a global security problem. Belarus and China, as two important countries, are facing the challenge of cybercrime. The purpose of this report is to compare the differences and similarities between Belarus and China in terms of the definition of cybercrime, legal penalties, and notable cases.

2. Definition of cybercrime

Belarus:

In Belarus, cybercrime generally refers to illegal activities carried out using computer network technology, including but not limited to data theft, Internet fraud, spread of malware, cyber attacks, etc. These actions are aimed at disrupting the normal operation of information systems, stealing or tampering with data, or committing other forms of cyber fraud.

China:

In China, cybercrime refers to the use of computer technology, with the help of the network to attack its system or information, damage or use the network to carry out other crimes. This includes hacking, network fraud, network infringement and other forms. Chinese law has a clear definition of cybercrime, and relevant legal provisions are constantly updated and improved with the development of technology.

Three, possible punishment

Belarus:

The penalties for cybercrime are harsher in Belarus. Depending on the severity of the crime, the offender may face penalties such as fines or imprisonment. For example, in online fraud cases involving large amounts of money, criminals can be sentenced to long prison terms.

China:

In China, punishments for cybercrime are equally severe. According to the Criminal Law of the People's Republic of China and other relevant laws, cybercriminals may face criminal detention, fixed-term imprisonment or even the death penalty, depending on the nature and severity of the crime. In addition, China has stepped up efforts to prevent and crack down on cyber crimes, and maintained cyber security through a combination of technical and legal means.

4. Famous cases

Belarus Case:

One of the most notable cases of cybercrime in Belarus in recent years was the prosecution of a Belarusian national in the United States for illegal activities involving cryptocurrency exchange BTC-e. The national is accused of being at the helm of BTC-e, suspected of money laundering and operating an unlicensed money services business. If convicted, he could face up to 25 years in prison.

China Case:

In China, there are many cases of cybercrime. Among them, the telecom network fraud case is particularly prominent. For example, a telecommunications network fraud gang fraudulently obtains the trust and property of victims by posing as public prosecutors and legal authorities, bank customer service and other means. After careful investigation by the police, the gang was eventually destroyed, and a number of criminal suspects were arrested and punished according to law.

V. Conclusion

By comparing the situation of cybercrime in Belarus and China, we can find some similarities and differences in the definition of cybercrime, legal punishment and specific cases. With the continuous development of network technology, the forms and methods of cybercrime are also constantly evolving. Therefore, both countries need to continuously strengthen legislation and law enforcement, and raise public awareness of cyber security and prevention awareness to jointly deal with the challenge of cyber crime. At the same time, strengthening international cooperation is also an important way to combat cyber crimes, through sharing experience, coordinated actions, and jointly build a safe and stable cyber environment.