Discussion on the Legal Regulation of Computer Network Attack

Min Zhang [1, a], Shuangxi Zhong *[2, b]

[1,2] Jiangxi University of Traditional Chinese Medicine, Nanchang, Jiangxi, 330004

[a] email:zhangminrd@163.com,

[b] Corresponding author,email:zshuagnxi@126.com

Keywords: Cyber attack; critical infrastructure; legal regulation

Abstract. Since the 20th century, network technology continues to progress, and is widely used in various fields of society. To the 21st century, network technology has entered all aspects of human life and human beings have entered the information age of the network. But the high-end technology since it can bring great convenience and benefits, but also there is a great danger, network technology is also true. In the era of the development of information technology network background, the key information infrastructure for the preservation and collation of the masses of the network system is constantly subjected to attacks from the network, and the more frequent, more serious damage. In order to reduce the damage caused by network attacks on countries, the world began to focus on prevention and control of network attacks. Chinese large population, the people have a great dependence on network technology, but Chinese prevention and treatment of attacks against the network is not perfect, there is a big hidden dangers.

Introduction

Highly developed network technology brings us into the information society, but the ensuing network attacks have posed a great threat to the country and the masses. Through the past network attacks can be found in the critical information infrastructure network system under attack, the national security, social order, economic order and the masses of the private information will be seriously violated. China should attach great importance to the harm of network attacks to our country, at the same time enhance the construction of the key information infrastructure network, and introduce relevant policies and regulations to deal with network attacks, to minimize the damage to our country's national information security and citizen information security.

Network attack concept and characteristics

Network attacks derived from the continuous development of computer network technology, mobile terminal technology and information technology improvement. All aspects of modern social life have a strong dependence on network technology, therefore, the occurrence of network attacks will exist its inevitability. With the development of network technology, cyber attack is becoming more and more diversified and destructive. Now it has become a major hidden danger to the information security of the world. For now, cyber attack has become the focus of information security in all countries, but our country did not define the concept of network attacks. China should raise the attention of network attacks, and keep up with the world trend, as soon as possible to regulate the network attacks and governance.

With the continuous development of network technology, network attack has more obvious characteristics, which has created a new problem for the legal regulation of cyber attack in the world.

There is no time limit for launching network attacks. Unlike traditional network attacks, network attacks can be launched at any time as long as the network is in normal operation, and can be continuously attacked at any time without any interference from external conditions. .

The coverage of network technology is very extensive, which makes the network attack has the characteristics of wide coverage and wide coverage. Small to remote terminals, large to cover the

global information network system, network attacks can make it into a paralyzed state, causing great harm.

Network technology itself has a virtual and open, and now the network technology has spread to countries in the world, as long as the ability to attack with the network, regardless of the state or individuals can become the implementation of network attacks. Moreover, network attackers can use various techniques to disguise and hide location information, attack source information, and identity information. The uncertainty of network attacker's range makes the network attack hidden, which is the main reason that the network attack is difficult to cure.

The Harm of Network Attack

In order to save a lot of manpower and resources, the state generally use network technology to control and operation of critical infrastructure, but it gave the network attack opportunity. Once the attacker attacks the key infrastructure such as the national key infrastructure and the industrial operation system and causes it to be paralyzed and the various procedures can not work normally, it will seriously endanger the national security, the national interest and the public interest. Since the 21st century, network attacks have been carried out by organized hacking groups, cybercrime groups, and even national units in order to obtain targeted data and information, destroying targeted information systems, etc. The main objectives of the industry involved are financial, power resources and Fuel resources and other key infrastructure industries.

Once the critical infrastructure is destroyed by cyberattacks, it is bound to cause great damage to the public interest, and lead to the emergence of public fear, and ultimately social unrest. Network attacks on critical infrastructure and industrial operation systems and other key hubs after the implementation of destructive blows, will inevitably lead to damage to facilities and unpredictable economic losses, but also the loss of public safety, the public recognition of national credibility quickly Down, greatly affected the stability and harmony of society.

Legal Regulation of Network Attacks in the World

In the United States in the 90's began to build a network attack threat prevention system, in the "9.11" incident, the United States began to attach great importance to the legal system of network attacks, the regulation covers a number of areas of network technology. In February 2015, the United States built a network threat and intelligence integration center, the department will integrate the United States a number of intelligence forces, efforts to improve the United States against network attack prevention ability. In March the same year, the United States, "cyberspace security information sharing law" introduced and the network environment to achieve the national loopholes in the open information sharing.

The legal regulation of cyber attack should establish the law and draw up the combination of strategy and practice. At the beginning of the 21st century, the European Union adopted the Convention on Cybercrime, and made relevant provisions on the content of cyber attack. In 2009, the EU adopted a policy on the protection of critical information infrastructure, the EU in response to network attacks, prevention, monitoring of network attacks, reduce losses and the ability to rebuild after a larger upgrade.

The Method China should Adopt to control network attacks

First, all levels of our society should be clearly aware of network attacks on the various fields of social harm, and to establish a collaborative management of network attack prevention concept. Government departments, network law enforcement agencies, social organizations, enterprises and the masses of citizens to contribute their own efforts to achieve the sharing of responsibility to refine and ensure the participation of all the people of the synergy, and ultimately benefit sharing.

Second, the relevant government departments should establish the concept of process control to deal with network attacks. In the event of a network attack, the relevant departments of the incident

process should always have a considerable degree of control. The relevant departments of the government should not only do a good job in the network control of the overall control work, but should take preventive measures to improve the network attack monitoring system and the establishment of various emergency response measures, the first time to achieve control of network attacks.

Today, China is also facing a very grim situation. At the same time, our country should look at the world, and combine its own actual situation, to achieve the greatest degree of perfection on the network attack prevention and control strategy.

On the domestic level of strategy: First, our government should improve the cyberspace strategy, so that our response to network attacks can be implemented when a series of effective measures; Second, China should attach great importance to prevention and control of network attacks, Prevention, control and punishment in place in three areas, through a scientific mechanism to damage the degree of reasonable classification of network attacks, and attacks according to the number of stages of process control; Third, the establishment of network information sharing loopholes in the system , Whether it is the state organs or the private sector, will monitor their own network information leaks to each other and even the public disclosure, to maximize the sharing of information to protect the country, society and the interests of citizens.

On the international level of strategy. Globalization of the network and the global requirements of the Internet In response to network attacks, countries should cooperate with each other. In order to ensure the stability and harmony of the international community and ensure the sustainable development of economic globalization, all countries should deepen cooperation, participate in and actively communicate on the cyber attack events. At the same time, for the occurrence of transnational network attacks, countries in the world should formulate a set of reasonable countermeasures and perfect legal punishment system. Countries should also implement a joint security exercise in network attacks, to improve the resistance of countries around the world to attack the network.

Conclusion

Network attack is the era of information network era reflects the shortcomings of the threat of network attacks on the machine will cause national interests and public interest incalculable losses. China should attach great importance to the dangers of network attacks, change the concept of timely, combined with the effective prevention and control of international network attacks, to develop with Chinese characteristics, network attack prevention strategy.

References

[1] Huang Zhixiong. "Network War" under the Perspective of International Law and Chinese Countermeasures - Focus on the Right to Recourse to Military Power [J]. Modern Law, 2015, 05: 145-158.

[2] weng Zhen. Network attack from the perspective of public international law [J]. Theoretical observation, 2016,04: 88-89.

[3] Zhang Tao, Wang Yue, Huang Daoli. Information System Security Governance Framework: EU Experience and Implications - Based on Network Attack [J] .Journal of Information, 2016,08: 17-24.

[4] Liu Deliang. Chinese network information security issues of legal regulation [J]. Information Security and Communications, 2011, 06: 31-35.