ISSN: 2688-9323

Analysis of Prominent Problems and Countermeasures of Internet Security Governance

Xiao Shen

[1]BNU, School of Journalism & Commun, Beijing100875, China

[2]School of Theatre, Film and Television, Communication University of China, Beijing 100024, China

277524335@qq.com

Abstract

The development of the Internet has changed people's way of life, and the network has become an indispensable part of people's work and life. Internet security governance is the core content of Internet governance, and the security of Internet is even directly related to national security. At present, China's Internet security governance has taken a number of measures, including special action, clear responsibility subject and regulate the behavior of Internet users. These measures have achieved remarkable results. But even so, there are still some problems in the process of Internet security governance, such as frequent security incidents, single governance mode and the gap with advanced countries Seriously hindered the long-term and stable development of China's Internet.

Keywords

Internet; security governance; problems.

1. Introduction

With the rapid development of the Internet, the network has been widely used in many fields, which has played a role in promoting the development of many fields. Naturally, the Internet has become an effective auxiliary means for the development of various fields, whether it is lifestyle or work efficiency. With the improvement of the application rate of the Internet in life and work, people pay more and more attention to the Internet security problems. Therefore, it is necessary to start with the outstanding problems of Internet security governance, conduct in-depth analysis of the outstanding problems, and then formulate targeted countermeasures to ensure that the prominent problems of Internet security governance can be solved, so as to improve the network security Security, and can create a secure network environment [1].

2. The Concept of Internet Security Governance

The subject of Internet security governance is not the government or a certain department, but the government, enterprises, associations and individuals work together to formulate the Internet system and rules through cooperation, and implement the Internet Security Governance on this basis, so as to ensure the high-speed operation of the Internet under the premise of ensuring security. The security governance of the Internet needs the supervision of the whole society and the self-discipline of the network users, so as to ensure the security of the Internet. The main goal of Internet security governance is to give full play to the advantages of the Internet, promote social progress and development, and realize the dissemination of advanced ideas. In addition to respecting other people's intellectual property rights, we should learn to treat other people's intellectual property rights equally and protect their national security. When evaluating the Internet security governance, we need to examine whether the

ISSN: 2688-9323

Internet security governance has promoted the development of social productivity, whether it has caused a blow to cyber crime, and whether it has stimulated positive social energy, which has also laid a good foundation for the development of the Internet [2].

3. Outstanding Problems in Internet Security Governance

3.1. The Problem of Information Leakage is Serious

Information leakage mainly refers to that the confidential information is known by others without authorization. Information leakage is a serious problem and may even have a great negative impact on the society. In recent years, network information technology has made great progress, but the situation of information leakage has become more and more serious, whether it is for individuals, enterprises or the country have a small or large impact. Through analysis and research, it is found that the causes of information leakage are various, including the loss of information storage equipment, document management out of control and external information release out of control.

3.2. Network Security Integrity Issues

Network security integrity is one of the main problems of Internet security governance, which will seriously affect the normal use of the Internet. Internet security integrity is affected by many factors, such as Trojan virus intrusion, authorization infringement, etc., these problems will affect the integrity of Internet security. Through research and investigation, it is found that the problem of Internet security integrity is mainly reflected in two aspects, namely network investigation and network attack. Network investigation refers to the illegal interception of confidential information without affecting the normal operation of the network; network attack refers to the direct destruction of normal network operation, so as to achieve the acquisition of confidential information. Network attacks are also the main reason for the destruction of Internet security integrity [3].

3.3. The Awareness of Network Security is Relatively Weak

Although the development of Internet technology in China is relatively late, the development speed is very fast. In the process of development, Internet technology has been widely used, especially in people's life and work, which makes people's life and work style have undergone great changes, but at the same time, there are also many new problems, the most prominent of which is people's network security The whole consciousness has not been improved, and it is still weak. For example, many enterprises do not implement the network security education, lack of network security awareness, pay too much attention to the interests in the work, and do not invest more funds in the network security management, which leads to the illegal elements to obtain benefits by using the network loopholes, and even causes the occurrence of security accidents, which seriously threatens the development of social economy.

4. Effective Measures of Internet Security Governance

4.1. Strengthen the Management of Mobile Storage Devices

With the development of network information technology, mobile storage devices have a high utilization rate. Common mobile storage devices include USB flash disk, optical disk and tape. USB disk has become the most common mobile storage device because of its small size and easy to carry. However, it is also because of its high utilization rate and is most vulnerable to virus invasion. Once the USB disk invaded by virus is connected to the computer, there is a great probability that the virus will spread. In order to improve the security of the use of mobile storage devices, it is necessary to take effective management measures for mobile storage devices: first, actively improve the management regulations of mobile storage devices, and

ISSN: 2688-9323

make registration records of the use of the devices, but also carry out regular virus detection on the devices, so as to timely check and kill viruses; second, to use mobile storage devices The user needs to be strictly standardized, especially when using more important equipment, the USB interface needs to be turned off; thirdly, the internal network and external network should be isolated, even if the mobile storage device is frequently used, it will not affect the use safety of the intranet [4].

4.2. Effective Control of Network Access

Network access is one of the main ways to cause network security risk factors to invade the Internet. Strengthening the effective control of Internet network access can reduce the invasion of network security risk factors. There are two ways to control Internet access, namely mandatory access control and autonomous access control. The function of network access control is mainly reflected in two aspects: one is to allow legitimate users to access, and the other is to deny illegal users access to protected network resources. The effective control of network access mainly includes three forms: access control, server control and firewall control.

4.3. Enrich Security Authentication Methods

Perfect security awareness can realize the security governance of the Internet, and the authenticity, confidentiality and integrity of Internet information can be guaranteed by rich security authentication. There are mainly several security authentication methods: first, setting a high security password can improve the confidentiality of information; second, online signature authentication has irreplaceable characteristics; third, a perfect electronic authentication system can determine the identity information of both parties and ensure the authenticity of information [5].

4.4. Strengthen Training to Improve the Network Security Awareness of Users

With the development of society, Internet technology has been widely used in many fields, and has played an important role in different fields. At the same time, it has also produced a lot of information security problems, which makes the domestic information security form not optimistic. It is urgent to improve the network security awareness of personnel. Whether in the production, management or information dissemination, personnel play an important role, need to rely on manpower to build a human firewall, in order to ensure the security of information. In addition, in the Internet security governance, it is necessary to establish correct values and regulate their own behavior, which helps to establish a correct sense of network security, and then improve the level of Internet security governance.

5. Conclusion

To sum up, in the face of increasingly complex Internet security governance issues, we must improve the awareness of security management, fully understand the Internet security governance issues, and formulate corresponding network security management countermeasures. In order to improve the security of Internet use, in addition to establishing the awareness of network security, we should also strictly abide by the rules and regulations related to network security, timely repair network vulnerabilities, and jointly do a good job in network security defense, so as to avoid the occurrence of Internet security incidents from the source, so as to provide a good network environment for the development of all sectors of society and effectively promote the whole society The development and progress of the association.

ISSN: 2688-9323

Acknowledgements

This paper is a partial result of the Major Fine Arts Project "Network Culture Security Studies" (19ZD12) supported by National Social Science Fund of China.

References

[1] Tong Nannan, Dou Yue, Wang Jiandong: eight principles to be adhered to in China's Internet Governance [J]. E-government, 2016, issue 4: 38-44.

[2] Jiang Li, Zhang Di: Xi Jinping's thought of network security governance and its guiding significance. [J]. ideological and theoretical education guide, 2017 8 issue: 30-34 pages.

[3] Miao guohou, Xie Xiaonan: the path of legalization of cyberspace Governance: running the network according to law, surfing the Internet, and pipe network [J]. Journal of Chongqing University of Technology (SOCIAL SCIENCE EDITION), Issue 9, 2015: 87-90 pages.

[4] Liu Bing: improve the strategic layout of cyberspace and enhance the execution of building a strong network country [J]. China information security, 2015 issue 2: 34-36 pages.

[5] Xu Jun, Su Yinshan: new problems faced by Internet industry antitrust -- Based on Tencent QQ and Qihu 360 lawsuit [J]. Financial issues research, 2012 Issue 9: 32-39 pages.