Research on Governance of Bad Network Information Based on Operators

Wei Wu

China academy of information and communications, 100037, Beijing, China
Wsidy@126.com

ABSTRACT. *With the continuous development of global network informatization, various types of network security problems have emerged. By analysing various practical problems of network and information security faced by mobile operators, this paper gives the construction goals and principles of mobile operator network security management platform, proposes a security strategy as the centre, and security inspection as the engine to drive The overall architecture of the network security management platform of project business function modules. The architecture includes the construction of a complete network security management platform such as system framework, platform function division, and business interaction process. Practice shows that the mobile operator's network security management platform adopting this solution can solve the construction goals of quantifiable network security management and control, visualization of security situation, and guarantee of soft and hard data.*

KEYWORDS: *Bad information, governance, Internet, operators*

1. Introduction

With the development of communication technology, the dissemination technology of bad information is also constantly updated. In recent years, the number of commercial advertising SMS messages, fraudulent SMS messages and other spam messages received by mobile users has continued to increase, which has brought many adverse effects on the normal life and social stability of users. After a series of investigations and in-depth analysis, it was found that the characteristics of brands, network access channels, and tariffs for sending spam SMS numbers are highly concentrated. The card sales channels of some branches have poor quality, suspected card maintenance, and a large number of numbers are used to send spam messages. And other issues. The sales of these numbers not only did not increase the company's income, but generated a large amount of arrears and caused a large number of customer complaints, which seriously affected the company's social image. This article mainly combines the actual situation of bad information governance of a branch of China Mobile, focusing on spam text messages. Through a large number of data analysis, we found problems such as the quality of market business development behind the behaviour of spam text messages. From the perspective of source control, we control spam messages [1].

2. Analysis of bad Internet information

Generally speaking, the elements included in information transmission are: information source, network, and sink (user), so the governance of bad information can be developed around these three elements. Governance methods can be summarized in two aspects: controlling information sources and restricting user access. Controlling the information source refers to detecting and identifying bad information, and shielding and filtering it. Restricting user access refers to restricting the network spread of information and user access from the network and user levels.

2.1 The existence of bad information

The identification of bad information is the premise of governance. With the development of technology, the existence of bad information on the Internet has expanded from pure text to images and videos. According to different ways of existence, there are different detection methods for bad information.

2.1.1 Text information

At present, there are mainly two methods of keyword matching and pattern recognition. The former is simple to implement, but it is easy to be circumvented, and the rate of misjudgement is high; the latter involves natural language processing, machine learning and other disciplines with high recognition accuracy, can be automated detection.

2.1.2 Image information

Specifically, it includes gesture recognition, skin colour recognition, scene recognition and other different recognition methods, but its essence is all pattern recognition methods. The recognition accuracy of current identification methods needs to be improved, and semi-automatic detection with manual control can be achieved.

2.1.3 Video information

The main implementation method is to extract key frames to obtain images, and use image analysis technology. The storage space of video files is large, which requires high storage and computing power of the system. Since the relevant identification technology is not very mature at present, it is recommended to mainly regulate illegal video content through management means. At present, the text detection technology is relatively mature, which can realize high-precision and high-efficiency automated detection. For images and videos, due to the high cost and limited effect of detection technology, the method of combining management and technology should be considered to reduce the cost of technology implementation and improve governance efficiency.

2.2 Dissemination characteristics of bad information

2.2.1 Openness

The network as the fundamental carrier of information highway construction and network economy, the content of the network stipulates and restricts the concept orientation of users who use the network. Because in the online world, anyone can express an opinion on anything, and it can achieve the effect of rapid dissemination, which makes the form and content of online culture present a diversity, and also reflects Openness.

2.2.2 Vitality

The network world is a virtual world, and the network behaviour has a distinct hidden nature. In the online world, everyone can fully show the true human characteristics. However, due to the virtual nature of the network, the virtual information on the network is also labelled with a value tag, which has led to network hackers, network viruses, and the spread of network viruses through network pornography, which has led to a large number of social problems such as cybercrime and Internet drunk , Has become a major factor that jeopardizes social order and hinders social security, and these cyber disasters are another negative and inevitable result of the virtual nature of cyber culture.

2.2.3 The carrier of human nature

In the traditional moral ethics principles, people sometimes find no suitable carrier to vent the inherent diversity and complexity of human nature, they will vent through the Internet, and this catharsis can get a response on the network. This kind of truth, goodness and beauty the performance of fake and ugly people is unreservedly integrated into the tide of the Internet. In a sense, the Internet has become a true carrier of human nature. Since human nature is divided into good and evil, then this network carrying human nature is by no means only good and healthy.

2.2.4 Uncontrollability

The characteristics of network culture cannot be controlled by administrative orders, simple morals, ethics and legal norms. This uncontrollability represents the essence of all characteristics of network culture. On the one hand, using computers and entering the Internet age is an inevitable result of the objective development of the entire human social productive forces entering the stage of the information revolution. The intrusion of the Internet into people’s lives is already an objective existence; It has nothing to do with the realisation of the management and control methods and methods in the field of consciousness and management. But we must fully realize that with the continuous deepening of the understanding of the network and the continuous development of the network economy, the uncontrollability of the network culture can be recognized and ultimately controllable [2].

3. Overall architecture

The research field of network security refers to related technologies and theories related to information authenticity, information integrity, information availability, and information confidentiality and information controllability on the network. By collecting a large amount of network security data, all the quality management activities are displayed, and the quality plan is executed cyclically, and the whole process of making and organizing the plan is implemented. The construction of the network security management platform is closely integrated with national laws and regulations. Its design principles should strictly follow the basic characteristics of network security, adhere to the combination of platform technology and customized implementation, and realize the construction content can be implemented, while also realizing daily work. Automated execution and process-based management and control mechanisms have effectively improved the depth and scope of control of data and system security, and further strengthened the display of effective data information for security management.

Following the design principles and construction goals of China Mobile's network security management platform, this article divides the overall architecture of the platform into four layers: presentation layer, function layer, strategy layer, and procurement control layer. 1 shown.

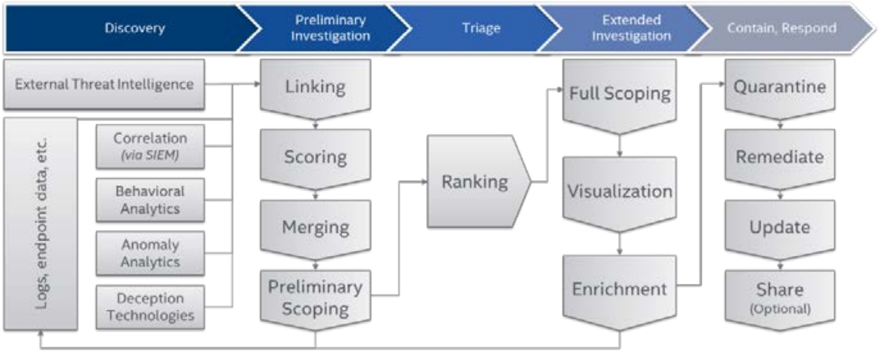

Figure 1. Network security management platform system framework

3.1 Presentation layer

As the presentation layer of the platform, the presentation layer mainly meets the user's need to display various types of security data. As a basic layer, it can provide various management themes for various levels of security management staff, security audit related personnel at various levels, and various types of operation and maintenance personnel involved in security protection management.

3.2 Strategy layer

The strategy layer is the core layer of this architecture and the core embodiment of PDCA architecture. Following the definition of the PDCA ring, this layer collects and sorts out various management and control rules and regulations related to network security, and integrates all the related security data sets by continuously extracting security specifications. The security strategy model of the strategy layer imports various security strategies into the security management platform in a standardized format.

3.3 Functional layer

The security management platform requires the active management and control of device policies in the full life cycle management of security devices, and the active delivery and control of device control policies based on security policies. Therefore, with the strategy as the centre, through all levels of architectural design. On the basis of the strategy layer, the function layer subdivides business functions into three sub-layers: basic functions, security management and control functions, and security management functions.

3.3.1 Basic functional layer

It mainly realizes the asset maintenance, security incident response and security operation automation management of the security strategy, including the management of security assets, the management of security incidents and the scheduling management of various security operations.

3.3.2 Security management function layer

Mainly realize the key protection network and system data, implement security management and control strategies and supporting technical measures. Implement network control strategies and system configuration strategies [3].

4. Platform business interaction process

The design of a healthy and reasonable platform architecture should fully ensure the safe and efficient operation of the various business flows that are operated. The business interaction process between the functions of the network security management platform designed in this paper is shown in Figure 2.

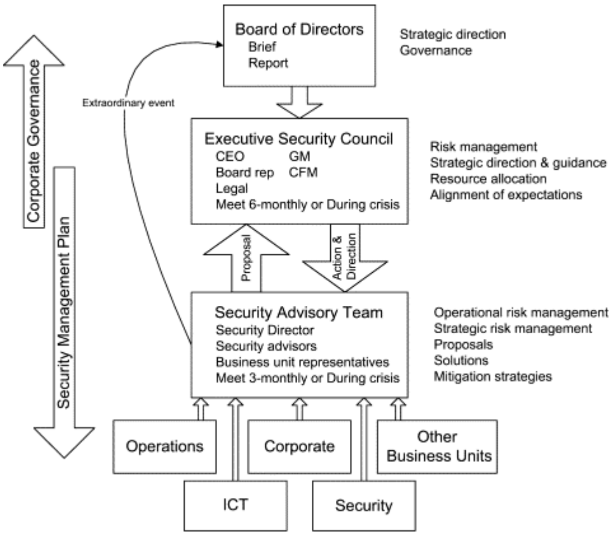

Figure 2. Platform business process

In Figure 2, the network security management platform is based on the security strategy to efficiently control and control the business data flow in the business function module. As the source of executing various business plans, the security policy formulates various security policy templates through the policy library, and then configures detailed inspection requirements to formulate detailed task details for various businesses. The completed strategic plans are distributed to various business modules through release and policy management and control, such as: network security management, system security management, data security management, etc., and each business module internally differs according to business details. Each has its own complete business circulation configuration content. Taking data security management as an example, the security policy centre will directly deliver the formulated data security policy to the data security management business module, that is, to implement the application deployment of the data security policy.

5. Bad information governance algorithm

5.1 Text recognition

Keyword recognition technology is a relatively mature recognition technology. The realization principle of keyword recognition technology is very simple. First, match the keywords with the keyword library, and then count the number of occurrences of keywords in a document, and compare with the pre-set discrimination threshold. If it is greater than the threshold, it is considered to be bad text. In addition, in order to improve the accuracy of keyword discrimination, keywords can be graded and set with different weights, that is, for very sensitive words, the weight can generally be set higher, or it can be directly intercepted / blocked, for general For more neutral vocabulary, you can set a lower weight. It briefly introduces the Naive Bayes algorithm.

Naive Bayes is commonly used in text classification. Naive Bayes is based on the Bayesian formula and is based on a basic assumption: It is assumed that the feature terms of the samples are independent of each other, thus forming the Naive Bayes method. It is generally assumed that $D=\{d_1,d_2,...,d_n\}$ is a collection of texts, where d_1 is the itch text in the document set and c is the category of the text (for example, $c=0$ stands for normal text and $c=1$ stands for junk text). Let the text consist of a sequence of words $d=\{w_1,w_2,...,w_N\}$, where w_1 is a word. After a new text is given, according to the Bayesian formula, the probability that the text is normal text is:

$$p=\left(c=0\middle|d\right)=\frac{p\left(d\middle|c=0\right)p\left(c=0\right)}{\sum_{k=0}^{1}p\left(d\middle|c=k\right)p\left(c=k\right)} \tag{1}$$

5.2 SIFT image fuzzy matching technology

Offenders often zoom, stretch, intercept, cover, change colour, flip, distort, feather, etc. the same picture to form a series of deformed pictures that do not affect the visual meaning, so as to easily bypass the recognition of the surveillance system, resulting in surveillance strategies The recall rate is very low. Therefore, it is necessary to introduce the picture fuzzy matching technology, which is mainly based on the relatively mature SIFT feature operator method in computer graphics. The SIFT feature operator has many invariances such as scale, translation, rotation, affine, etc. At the same time, it represents the essential attribute characteristics of the image content, which can effectively affect the image content under complicated conditions such as large changes in observation conditions, occlusion, and clutter. Description. By separately extracting SIFT features from the sample pictures and the pictures to be matched, and performing similarity comparison, the similarity of the two images can be determined [4].

6. Summary

After years of development, the Internet has penetrated into political, economic and other social fields and has had a huge impact. For bad information on the Internet, the country has always used the term "governance" rather than "regulation". There is a big difference between "governance" and "regulation": "regulation" emphasizes the leading role of the government, but it does not exclude the role of enterprises and individuals; while "governance" tends to cooperate with the government, enterprises and individuals. For the bad and harmful Internet information at the moral and cultural level, it is clear that governance is more scientific and effective than regulation. Therefore, in the future work, integrating more social participation and fully mobilizing the enthusiasm of enterprises and individuals is the direction of Internet bad information governance.

References

[1] Egners, André, Herrmann, P. & Meyer, U. Multi-operator wireless mesh networks secured by an all-encompassing security architecture. International Journal of Information Security, 14 (2) (2015) 169-186.

[2] Petermeijer, S. M. Abbink, D. A. & winter, J. C. F. D. Should drivers be operating within an automation-free bandwidth? Evaluating haptic steering support systems with different levels of authority. Human Factors, 57 (1) (2015) 5-20.

[3] Kuldeep Nagiya, Mangey Ram, & Ayush Kumar Dua. A tree topology network environment analysis under reliability approach. Nonlinear studies, 24 (1) (2017) 193-202.

[4] Gangele, S, & Patil, S. Internet traffic distribution analysis in case of multi-operator and multi-market environment of computer network. International Journal of Computer Applications, 130 (4) (2015) 29-36.