Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 3, No. 1, 2025

An Exploration of Network Security Based on Entropy Weight Method and Fuzzy Comprehensive Evaluation Modeling

Yibo Zhang *

School of Mechanical Engineering, Northwestern Polytechnical University, Xi'an, China
* **Corresponding author**: 916881864@qq.com

Abstract: This paper focuses on cybercrime characteristics and cybersecurity assessment, with the aim of understanding the global distribution of cybercrime and conducting modeling analysis. In terms of research methodology, data on cybercrime rates, frustration rates, success rates, reporting rates and prosecution rates of many countries and regions such as the U.S., China and the U.K. are collected; entropy weighting method (EWM) is used to calculate social coefficients and analyze the relationship between socio-economic factors and crime rates; and fuzzy comprehensive evaluation model is used to establish a comprehensive evaluation model for cybersecurity. The strengths of the study are that it reveals the characteristics of cybercrime in different countries and regions in a more comprehensive way through multifaceted data and models, and the model constructed can comprehensively assess the cybersecurity situation of each country, and the reliability of the model is verified by sensitivity analysis, which makes it clear that the policy score and the social score have a greater impact on the cybercrime rate.

Keywords: Cybersecurity; Entropy Weighting Method; Fuzzy Comprehensive Evaluation Model.

1. Introduction

In this paper, a systematic study is conducted on network security assessment [1]. The study utilizes a combination of entropy weighting method (EWM) [2] and fuzzy comprehensive evaluation model [3]. With the help of EWM, the demographic characteristics of each country (Internet access, wealth and education level) are correlated with the crime rate, and the influence of each factor on the crime rate is analyzed and the social coefficient is calculated. On this basis, a fuzzy comprehensive evaluation model is utilized to construct a set of assessment factors and a collection of scoring gauges to provide a comprehensive assessment of the country's cybersecurity status. Through these methods and models, the global distribution of cybercrime, the characteristics of cybercrime in different countries and regions [4], and cybersecurity policies [5] are studied in detail. The strength of the research in this paper lies in the comprehensive and precise revelation of cybercrime characteristics, which provides a strong basis for the development of scientific and effective cybersecurity policies [6].

2. Characterization of Cybercrime

To understand the global distribution of cybercrime and model it to analyze the situation, this paper collects cybercrime rates, thwarting rates, success rates, reporting rates, and prosecution rates for countries/regions such as the United States, China, the United Kingdom, and France. The data is shown in Figure 1 below.

After a preliminary analysis of the data, the following conclusions can be drawn.

(1) Eastern Europe: Russia tops the global cybercrime index and Ukraine also ranks high. The Eastern European region has a richer pool of cyber technology talent, but some people are driven by financial gain and other factors to engage in cybercrime.

(2) Africa region: South Africa ranked first around cyberfraud. Several local organizations and individuals use cybertechnology to target victims globally through phishing and fraudulent investment scams, especially in countries and regions where English is the primary language.

(3) Asia region: China ranked third in the global cybercrime index, with a diverse range of cybercrime types covering all aspects of cyberfraud, cybertheft and cyberattacks.

(4) Americas: Cybercrime is also more prominent in the U.S. The U.S., as a country with highly developed Internet technology, is on the one hand a high incidence of cybercrime, and on the other hand a major target of cyberattacks. Malicious actors use cyber technology to carry out activities such as data theft, cyber fraud and ransomware attacks.

(5) Western Europe: Cybercrime in the United Kingdom is mainly of a financial nature, with a well-developed local financial system and frequent online financial transactions, enabling cybercriminals to target cash-out and money-laundering activities in the financial sector. French cybercrime activities also cover a wide range of aspects, although the overall situation is relatively good compared with some other high-prevalence countries.

(6) Other countries and regions: Other countries and regions around the globe also have cybercrime problems to varying degrees. For example, developed countries such as Australia and Japan also face cybersecurity problems such as cyberfraud and data leakage; some developing countries also face the risk of attacks on cyberinfrastructure and theft of personal information due to relatively weak cybersecurity protection capabilities.

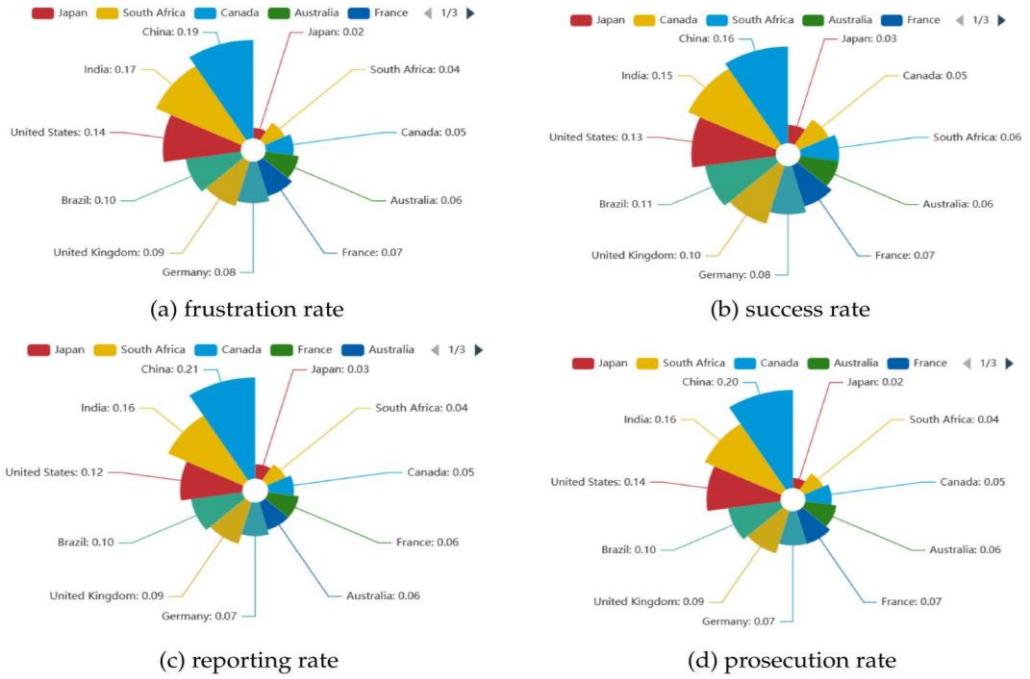

Figure 1. Global distribution of cybercrime

Regional and national cybercrime characteristics are further analyzed as follows.

(1) United States: As one of the most developed countries in the world in terms of network technology, the United States has a large group of network users, rich financial information and a large amount of corporate data and other resources. Various types of cyber-attacks, data theft, cyber-fraud and other criminal activities occur frequently.

(2) China: China has a large Internet user base and a rapidly developing digital economy, and online shopping, mobile payments and other businesses are popular, which gives cybercrime more targets and opportunities. Criminal activities such as telecommunication network fraud, network theft and network infringement of personal information are more prominent.

(3) Australia: According to a report by the Australian Competition and Consumer Commission (ACCC), economic losses due to fraud in Australia have exceeded A$3.1 billion in 2022, a surge of 80% compared to 2021.In 2023, more than 600,000 fraud reports were received in Australia, with related losses In 2023, more than 600,000 fraud reports were received in Australia, with related losses amounting to A$2.74 billion.

(4) United Kingdom: The United Kingdom has a well-developed financial and business system and is active in online financial transactions, e-commerce, and other activities, which makes it an important target for cybercriminals trying to carry out activities such as financial fraud and stealing trade secrets in the United Kingdom through online means.

(5) Japan: Within the Asian region, Japan has also received increased attention for its cybercrime problem. The country's well-developed financial and technology sectors and the presence of a large amount of valuable information and assets on the Internet have become coveted targets for cybercriminals, with incidents such as data breaches and phishing occurring from time to time.

The United States, China, India and Brazil had high crime success rates, all exceeding 0.1 per cent; the success rate in thwarting cybercrime in the United States, China, India and Brazil exceeded 0.1; and China had the highest rate of cybercrime reporting and prosecution of the four countries, at over 0.2 per cent.

3. Comprehensive Cybersecurity Assessment Analysis

3.1. Calculating Social Factors Using EWM

By collecting the demographic characteristics of each country, primarily Internet access, wealth, and education level, and correlating them with the previously obtained crime rates for each country, this section analyzes the extent to which each of these three factors affects the crime rate, as well as the use of entropy weighting to arrive at which country is stronger in terms of socioeconomic factors. The specific visualization is shown in Figure 2.

The results show that all three factors are negatively correlated with crime rates. Higher levels of education and wealth were associated with lower crime rates, while the impact of Internet access on cybercrime was bidirectional. Countries with high rates of Internet access usually invest more in information technology and network infrastructure development and therefore focus on building cybersecurity protection systems. These countries usually have more comprehensive cyber laws and regulations, with clear definitions and severe penalties for various cybercrimes. A sound legal system not only serves as a deterrent and reduces the motivation of potential offenders, but also provides a strong legal basis for law enforcement agencies to combat cybercrime. Meanwhile, due to the widespread popularization of the Internet, the public has more opportunities to access and understand cybersecurity knowledge, and generally has a higher awareness of cybersecurity.

High Internet access rates mean that more vices and systems are connected to the network, which provides more targets for cybercriminals to attack. Large amounts of sensitive information from businesses, government agencies and individuals are stored in networks, which are easy targets if there are security vulnerabilities. The network environment will also become more difficult to manage and monitor. New technologies and applications are emerging, such as the

Internet of Things and cloud computing, which bring convenience but also new security risks. Cybercriminals can take advantage of the loopholes in these new technologies to carry out criminal activities, thus increasing the opportunities for cybercrime. It will also have an impact on international cybercrime. The Internet is global, and cybercrime is not limited by national borders. Countries/regions with high Internet access usually play an important role in international cyberspace and are more vulnerable to cyberattacks from around the globe. Therefore, it is important to focus on how much weight should be set for Internet access rate when determining the weights of the scores using entropy weighting method. Based on the solution results, the corresponding weights are education level: 0.5, Internet access: 0.3, and GDP per capita: 0.2. Obtaining the corresponding scores for these countries/regions is tentatively called social scores.

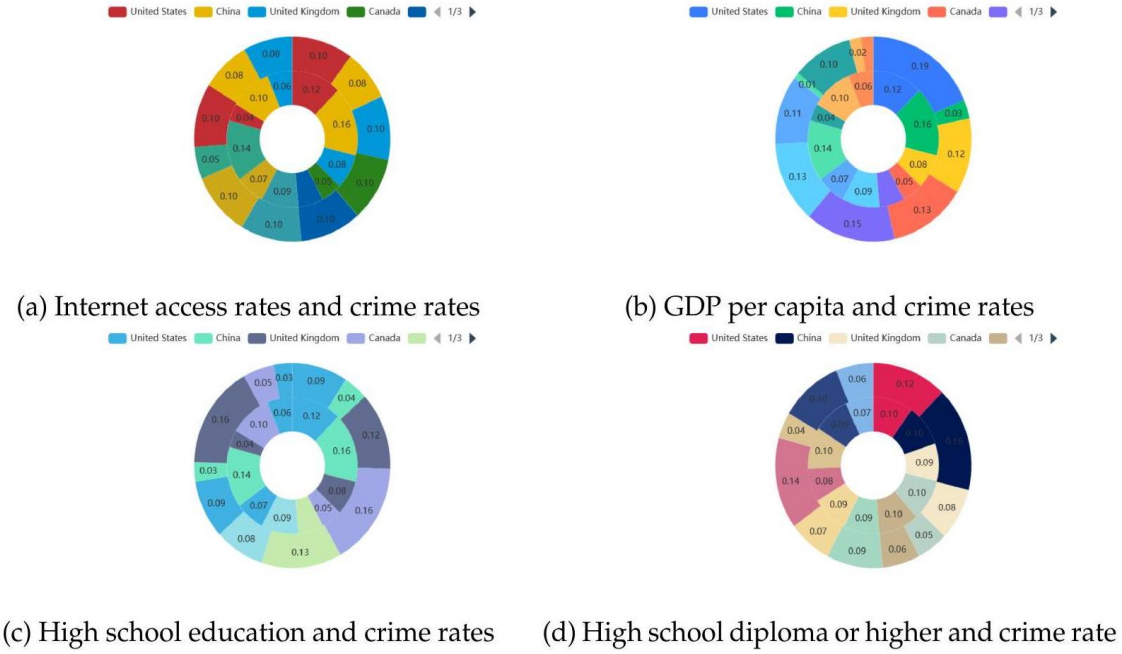

Figure 2. Relationship between socio-economic factors and crime rate

3.2. Establishing a Comprehensive Evaluation Model for Cybersecurity Using the Fuzzy Comprehensive Evaluation Model

Having dealt with the above three scenarios, this section allows for the construction of the final model, the fuzzy comprehensive evaluation model, to develop a theory on a strong national cybersecurity policy. First, a set of assessment factors were constructed, which were designated into three assessment factors based on the scores obtained: the national cybersecurity score, the policy score, and the societal score, as illustrated in Figure 3. Since the prevention, prosecution, and mitigation strengths of the policy are more abstract, this section decides to multiply each of the three strengths again by their own weights in order to obtain the policy scores for each country/region.

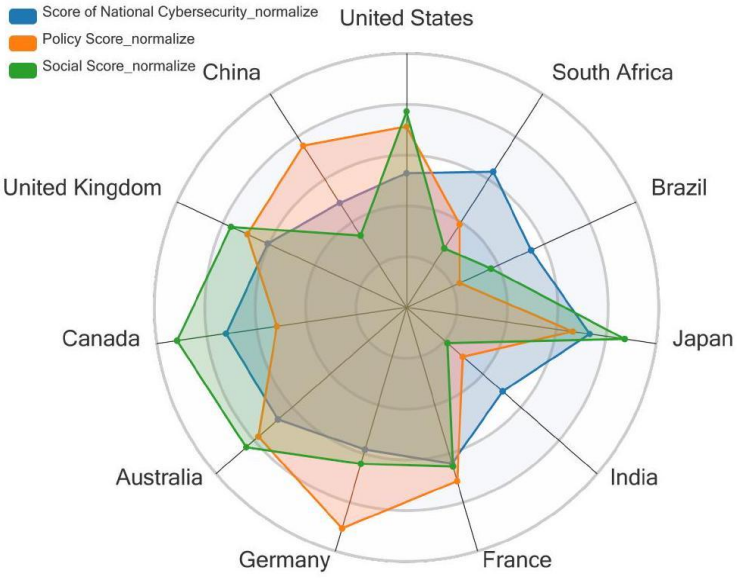

Figure 3. Standardized national cybersecurity scores, policy scores, and societal scores

After the analysis, the final modeling can continue: Construct the set of assessment factors:

$$U = \{Cybersecurity \text{ Score, Policy Score, Social Factors Score}\} \quad (1)$$

Construct the set of rating scales:

$$V = \{\text{Very good, better, average, poor, very poor}\} \quad (2)$$

Perform one-factor fuzzy assessment:

$$R = (r_{ij})_{n\times m} \quad (3)$$

Perform single factor fuzzy assessment:

$$A = (a_1, a_2, \dots, a_n) \quad (4)$$

Satisfy:

$$\sum_{i=1}^{n} a_i = 1, a_i \geq 0 \quad (5)$$

Fuzzy comprehensive evaluation:

$$B = A \circ R = (b_1, b_2, \dots, b_m) \quad (6)$$

Where:

$$b_j = \sqrt[n]{\wedge_{i=1}^{n} (a \wedge r_{ij})} \quad (7)$$

Or:

$$b_{ij} = \sum_{i=1}^{n} (a_i \times r_{ij}) \quad (8)$$

Calculate the composite assessed value:

$$C = B \times V^T = \sum_{j=1}^{m} a_i \times v_j \quad (9)$$

View the final comprehensive evaluation results as in Figure 4.

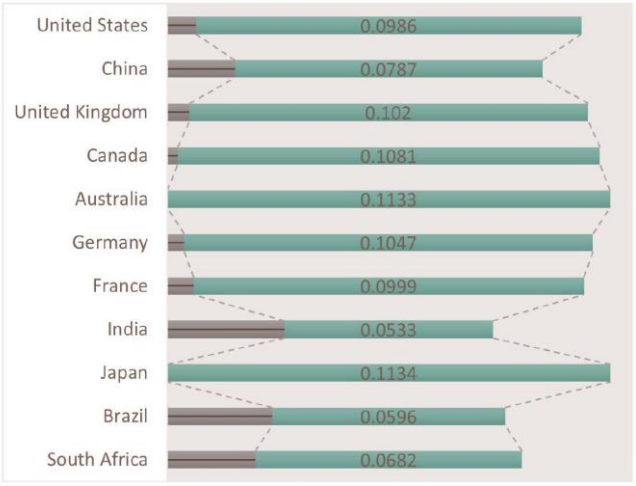

Figure 4. Comprehensive cybersecurity valuation

Very Good: Australia, Japan, Canada, Germany, UK, France, US.

Good: China.

Average: South Africa.

Poor: Brazil, India.

According to a report based on the International Telecommunication Union's 2024 edition of the Global Cybersecurity Index:

T1: United States, United Kingdom, Canada, Australia, Germany, France, Japan.

T2: China.

T3: Brazil.

T4: South Africa, India.

This demonstrates the accuracy of the modeling in this paper. The only drawback is that there are some errors in Brazil and South Africa, which may be caused by insufficient data collection to analyze the dimensions.

In the light of the above results and analysis, the paper then makes a few recommendations for cybersecurity policy:

First, policies must include preventive intensity, i.e. be forward-looking and could take the form of educational and awareness-raising measures, such as cybersecurity training and public information campaigns. Second, policies must include strong prosecutorial intensity, strengthened legal frameworks and strict cybercrime laws with some legal force, as cybercrime is increasing in some countries due to lagging laws or inadequate enforcement. International cybersecurity cooperation should then be strengthened to enhance law enforcement against transnational crime. Finally, the policy must also have good mitigation efforts, i.e. flexibility and adaptability. Effective policies are usually accompanied by feedback mechanisms that enable law enforcement agencies and policymakers to continuously optimize policies based on crime data and public feedback. With the rapid advancement of technology, it is important to keep optimizing policies based on the actual situation, otherwise crime rates will gradually rebound, as predicted.

In addition to policies, there is also the social situation, i.e. the impact of socio-economic factors on this country, which the study analyzes mainly in terms of Internet access rate, wealth and education level. Therefore, in addition to developing good cybersecurity policies, the country should also strive to improve its technological capabilities, raise the standard of living of its people and increase the level of well-being, which would allow the country to develop itself while achieving the goal of preventing crime and killing two birds with one stone.

4. Sensitivity Analysis

The fuzzy comprehensive evaluation model constructed in this section itself contains ambiguities and uncertainties, and sensitivity analysis can help identify and analyze how these uncertainties affect the model results, to improve the reliability of the model. At the same time, sensitivity analysis can provide a clearer understanding of which indicators have the greatest impact on the comprehensive evaluation, to optimize the indicator system or adjust the strategy. This is crucial for improving the decision-making process and increasing the validity of the model. So, it began to gradually adjust each weight:

In this paper, the weight combinations were adjusted 3 times respectively: [0.60, 0.20, 0.20], [0.20, 0.60, 0.20], [0.20, 0.20, 0.60].

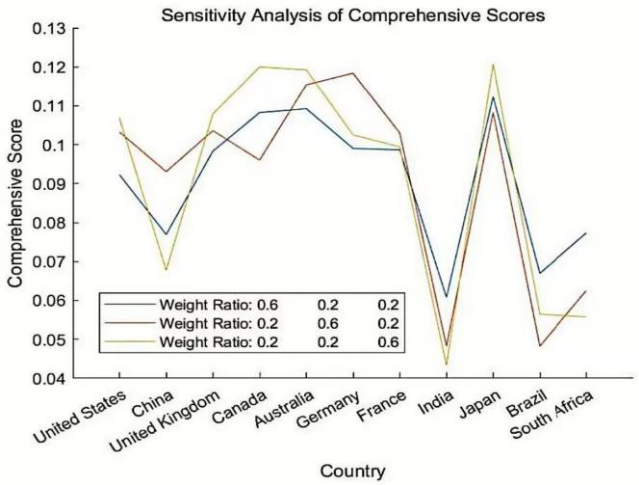

Figure 5. Results of sensitivity analysis

As in Figure 5, the average impact of each factor on the

composite score is obtained after solving.

National cybersecurity score: 0.0012.

Policy score: 0.0014.

Society score: 0.0015.

The corresponding percentages are:0.293,0.341,0.366.

Therefore, it can be concluded that the policy score and the social score have a greater impact on the country's cybercrime rate, which also represents that to reduce the cybercrime rate, the country first needs to formulate a good policy as well as to improve the level of social development and people's happiness.

5. Conclusion

Through the study of cybercrime-related data from several countries, this paper uses the entropy weighting method (EWM) and fuzzy comprehensive evaluation model to draw the following core conclusions: in terms of cybercrime characteristics, different regions and countries show different features, such as the high index of cybercrime in Russia in Eastern Europe, and the prominence of cyber fraud in South Africa in Africa in Africa, and so on. In terms of research methodology, EWM is used to analyze the relationship between socio-economic factors and crime rates, and to determine the weights of education level, Internet access, and per capita GDP; the fuzzy comprehensive evaluation model constructs an assessment system to comprehensively assess the cybersecurity situation of each country. The significance of this study is to deeply analyze cybercrime and provide reference for the formulation of cybersecurity policies. The practical application value is reflected in the sensitivity analysis to clarify that the policy score and the social score have a greater impact on the cybercrime rate, which in turn provides a direction for countries to reduce the cybercrime rate and is of great significance in promoting the construction of global cybersecurity.

References

[1] Han Chengzhe. Analysis of network information security protection strategy and evaluation algorithm [J]. Network Security Technology and Application, 2025, (01):41-42.

[2] Chen Lu. Application of entropy weight method in information security risk assessment [J]. Information Systems Engineering, 2021, (09):62-64.

[3] Zhou Jie. Research on the application of fuzzy comprehensive evaluation model in network system security assessment [J]. Network Security Technology and Application, 2013, (12):78-79.

[4] Lu Chenxi, Zhou Ming. Research on cross-border cybercrime governance in China under the perspective of data sovereignty [J/OL]. Journal of Jiangxi Police College, 1-7 [2025-02-15]. http://kns.cnki.net/kcms/detail/36.1316.D.20241224.0913.002.html.

[5] Zhang Yupeng, Lu Xiaowen, Lu Mingxin, et al. A Comparative Study of Chinese and American Cybersecurity Policies Based on the Three-Dimensional Framework of “Evolution-Tool-Theme” [J]. Journal of Intelligence, 2025, 44(02):124-135.

[6] Wang Wenzhi. Characteristics of computer network crime and prevention strategy analysis [J]. Law and Society, 2021, (19): 191-192. DOI: 10.19387/j.cnki.1009-0592.2021.07.083.