ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

Research on the Effectiveness of Network Security Policies Based on Interrupt Time Series and Natural Language Processing

Shuyuan You[a], Yichen Zhong[b], Jiajin Du[c], Guorui Zhao[d,*]

School of Computer Science and Engineering, Guangdong Ocean University, Yangjiang, China
[a]17520205242@stu.gdou.edu.cn, [b]dawnchime@foxmail.com, [c]13825651778@163.com,
[d]zhaoguoruimath@foxmail.com
**Corresponding author*

Abstract: *With the evolution of The Times, cybercrime has also spread rapidly around the world. An in-depth exploration of the effectiveness of cybersecurity policies is of great significance for all countries to formulate scientific prevention and control strategies. Most existing studies have conducted qualitative research from the perspectives of transnational governance and legal frameworks, lacking quantitative research and text mining on global policies. Given that traditional time series prediction is vulnerable to trend interference, this study selected the interrupted time series model. By analyzing the natural trends before and after policy intervention, the inhibitory effects of 145 policies in 137 countries on cybercrime were quantified. Subsequently, NLP technology was used to conduct TF-IDF modeling and word cloud analysis on the policy text, and core factors such as "international cooperation" were extracted. Research has found that effective policies usually focus on cross-regional collaboration, technological innovation and institutional construction, etc., and the differences in policy effects are closely related to the implementation background and the intensity of enforcement. Based on the above results, this paper constructs a data-driven policy analysis framework for cyber security, emphasizing the equal importance of dynamic assessment and multi-dimensional governance. It suggests establishing a continuous assessment mechanism, strengthening global collaboration, and coordinating technical means and institutional guarantees.*

Keywords: *Cybersecurity Policy, Policy Effectiveness, Interrupt Time Series Analysis, Natural Language Processing, TF-IDF Model*

1. Introduction

The World Economic Forum's "Global Cybersecurity Outlook 2025" [1] points out that the cyberspace landscape is becoming increasingly complex, which not only strengthens global connections but also provides new tools for criminals. Although many countries have formulated cybersecurity policies to address challenges, cybercrime continues to evolve and the threat keeps escalating. Therefore, it has become an urgent task to conduct in-depth research on policy effectiveness and explore data-driven optimization methods.

In 2011, Harknett et al. emphasized that the outlook for cybersecurity policy is characterized by its complexity and evolving nature. They stressed the lack of a comprehensive policy framework that systematically addresses problems and constraints[2]. In 2011, Andreasson provided an easy-to-understand overview of cybersecurity threats and response measures in the public sector, emphasizing the integration of globalization, connectivity, and the online migration of government functions[3]. In 2020, Calderaro studied the challenges of cross-border governance and cross-border network capacity building on a global scale[4]. Wong's research in 2022 demonstrated that enhancing awareness and understanding of cybersecurity strategies can improve and enhance compliance, which is crucial for organizational resilience[5]. In the context of national and regional policies, evaluations usually focus on the current cybersecurity situation and the effectiveness of enacted laws. For instance, research on African countries[6] provides insights into the status of cybersecurity policies in six countries, emphasizing the significance of assessing policy implementation and its practical impact on cybersecurity resilience. Similarly, the New York State Department of Financial Services[7] emphasized the role of cybersecurity policies being consistent with risk assessment to measure their effectiveness within financial institutions, and explained how to implement the policy framework through continuous

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

assessment. International and organizational standards also play a crucial role in formulating the assessment of cybersecurity strategies[8].

Although existing research has conducted qualitative studies from the perspectives of cross-border governance and legal frameworks, most of them explore based on a single country as a sample and lack quantitative research on the effects of cybersecurity policies in various countries from a global perspective. In particular, a data-driven analytical approach and framework have yet to be formed for the mining of core factors in policy texts.

This study focuses on the effectiveness of cybersecurity policies. Firstly, it has traversed global statistics related to cybercrime[9-10], as well as the cybersecurity policy texts on the official websites of various governments. Then, by using interruption time series analysis(ITSA), the inhibitory effects of 145 policies formulated by 137 countries on cybercrime were quantified, and the conclusions were verified through differential paired sample t-tests. Secondly, natural language processing and the TF-IDF model are used to parse the effective policy texts and extract the core factors. Finally, by integrating the results of quantitative and textual analysis, the core dimensions were extracted, and dynamic evaluations, global collaborative governance, and multi-dimensional policy design suggestions were conducted, providing theoretical support for global cybersecurity governance.

2. Introduction to Research methods and Model Construction

2.1 Analyze the effectiveness of national cybersecurity policies based on ITSA

This paper adopts the Single Interrupt Time Series Analysis (ITSA) method to provide data support for the evaluation and optimization of the effectiveness of national cybersecurity policies[11]. Based on multi-time point data before and after intervention at equal time intervals, the inhibitory effect of national cybersecurity policies on cybercrime was quantitatively evaluated through a piecewise regression model. This method separates the immediate effects and long-term trend changes after policy implementation by controlling the natural changing trends of the outcome variables before intervention. The model formula is:

$$Y_t = \beta_0 + \beta_1 \text{time} + \beta_2 \text{intervention} + \beta_3 \text{post} \quad (1)$$

Among them, is the observation result, is the continuous time variable, is the intervention indicator variable (0 before intervention and 1 after intervention), and is the time count after intervention (0 before intervention and increasing period by period).

The coefficient fitted by the least square method is the initial level, reflecting the trend before intervention, indicating the immediate effect of the policy, and demonstrating the trend change after the policy.

2.2 Analyze the keywords of national cybersecurity policies based on NLP

2.2.1 Policy text processing

This paper selects the national cybersecurity policy texts that have been verified by ITSA analysis to have inhibitory effects (covering 145 policies from 137 countries), and uses Python's pandas and nltk libraries to structure the policy texts. The policy text is divided into blocks based on key dimensions such as legislation, law enforcement, technology, international cooperation, prevention and education of the national cybersecurity policy[12-14]. Based on the python-docx library and with the help of the JIEBA library, the document collection is segmented to eliminate non-standard words, and the Chinese Academy of Sciences' lexical analysis tool NLPIR is used to assist in keyword segmentation processing.

2.2.2 TF-IDF model

The model is used to achieve keyword extraction. It calculates the value of a word and the product of its values to obtain the score of the statistic, and then sorts them in descending order according to the score size, and selects the words with higher scores as keywords.

The value calculation formula is as follows:

$$TF_{i,j} = \frac{n_{i,j}}{\sum_k N_{k,j}} \quad (2)$$

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

Among them, $n_{i,j}$ represents the number of times word w_i appears in document set j; $\sum_k N_{k,j}$ is the number of words in document set j after filtering the stop word.

Reverse File Frequency (IDF) is used to measure the occurrence frequency of words in the entire text library. Its function is to balance the frequency impact of common words. The calculation formula is as follows:

$$IDF_i = \log \frac{|D|}{|\{j: w_i \in d_j\}|} \tag{3}$$

Here, $|D|$ represents the total amount of text in the text library, $|\{j: w_i \in d_j\}|$ represents the number of texts containing words in the text library, but the denominator is usually used $1 + |\{j: w_i \in d_j\}|$.

Then, find the $TF - IDF$ value of each word w_i in the j-th document.The formula is as follows:

$$TF - IDF_{i,j} = TF_{i,j} \times IDF_i \tag{4}$$

Finally, based on the calculated TF-IDF values, the words in each document collection are sorted, and the words with higher TF-IDF values are selected as the high-frequency keywords.[15]

3. Empirical result analysis

3.1 Empirical Analysis Based on Interrupted Time Series

As there is a certain time lag from the announcement to the implementation of policies, when exploring the effectiveness of national cybersecurity policies in the future, we mainly consider the long-term effects after the implementation of the policies.

If the effectiveness of the "Cybersecurity Basic Law" issued by South Korea in 2013 is analyzed, the trend change after the policy implementation β_3=-10, indicating that the number of cybercrimes Y decreased by an additional 10 units each year after the intervention. This shows that the implementation of this policy in South Korea is effective in suppressing cybercrimes, as shown in Figure 1.

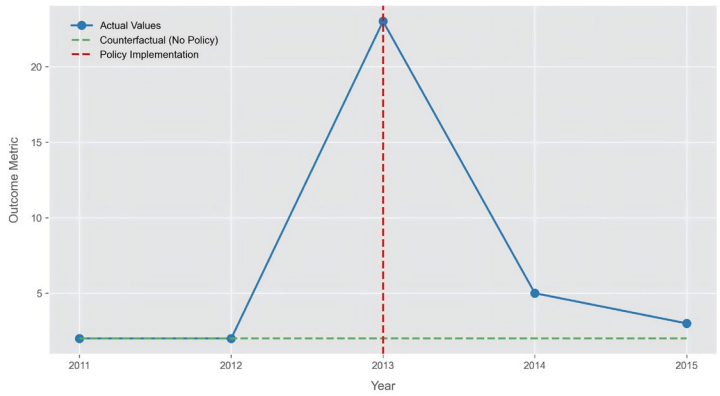


Figure 1: Change level of cyber crime in southkorea.

The effectiveness of the Data Protection Act introduced in the UK in 2018 was analyzed. The trend change after the policy was implemented β_3=14, indicating that the number of cybercrimes Y increased by an additional 14 units each year after the intervention. This shows that the implementation of this cybersecurity policy in the UK is ineffective in suppressing cybercrimes, as shown in Figure 2.

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

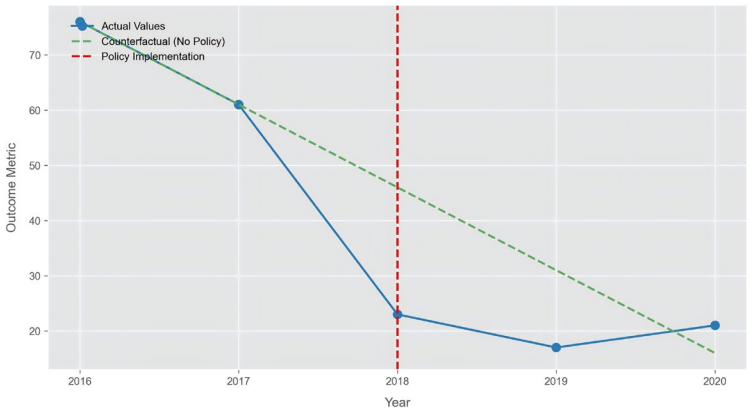


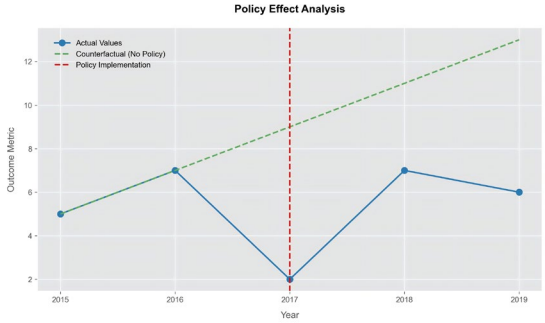
Figure 2: The change level of cyber Crime in UK.

The following is an enumeration of the trend changes after the implementation of cybersecurity policies in other countries, such as Table 1and Figure 3.

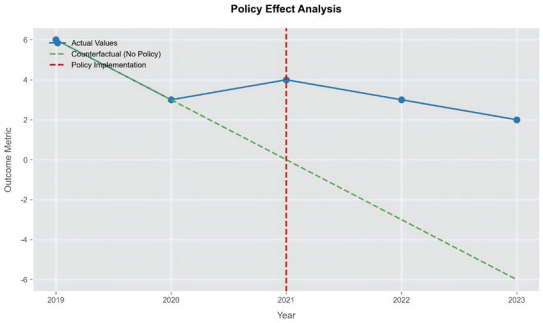
Table 1: The trend change after implementation of network security policies in some countries is $\boldsymbol{\beta_3}$.

China2017	China2021	Ukraine2016	Israel2015	Iran2014
0.01	2.00	6.50	8.00	0.50
Russia2016	Indonesia2023	India2013	Turkey2013	Brazil2020
1.50	-6.00	-21.00	-8.00	0.50
Germany2016	Italy2018	Japan2014	France2018	Poland2016
-3.50	0.01	-1.00	4.50	-0.50
Thailand2019	USA2013	USA2021	USA2023	UK2016
0.50	-796.00	380.50	-490.00	-25.50

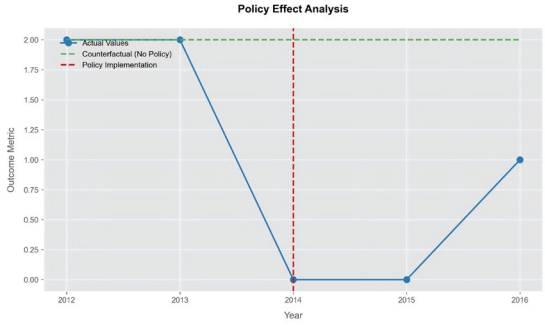
A visual analysis of the changes in the level of cybercrime before and after the implementation of national security cyber policies in some countries is shown in Figure 3.



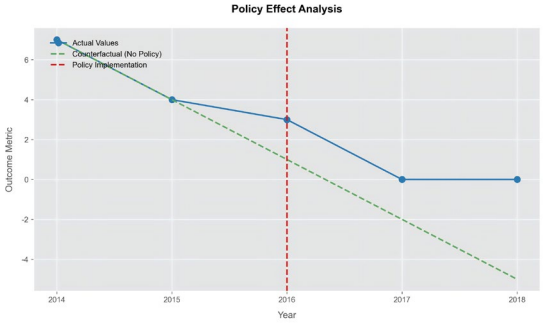
China2017



China2021

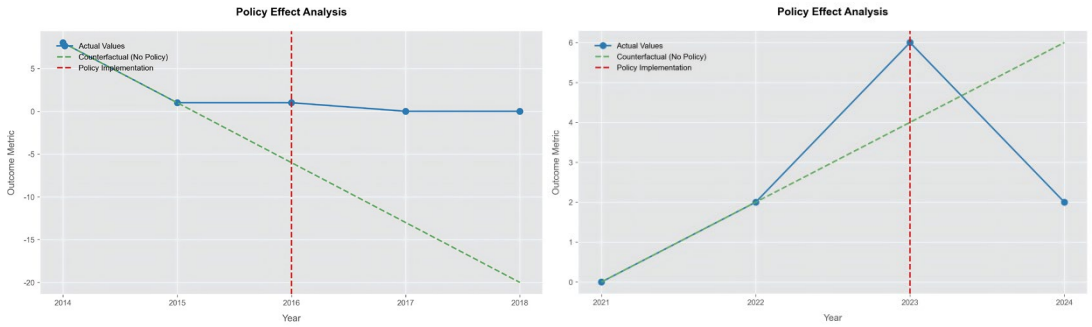


ran2014



Russia2016

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701



Ukraine2016 *Indonesia2023*

Figure 3: Changes in the level of cybercrime in some national policies.

3.2 Verify the effectiveness of national cybersecurity policies based on differential paired sample t-tests

We used the differential paired sample t-test to verify the effectiveness of the above-mentioned ITSA analysis of cybersecurity policies in various countries. When using paired t-tests to compare the mean differences before and after policy implementation, it is necessary to first perform differential processing on the time series data to eliminate trends or seasonality, and then conduct paired comparisons.

For the establishment of this mathematical model, a paired data set is first constructed (assuming the policy implementation time point is t^*)

$$\begin{Bmatrix} \text{Pre}-\text{policy difference value: } \{\triangle Y_{t^*-m}, \triangle Y_{t^*-m+1}, \ldots, \triangle Y_{t^*-1}\} \\ \text{Post}-\text{policy difference value: } \{\triangle Y_{t^*}, \triangle Y_{t^*+1}, \ldots, \triangle Y_{t^*+m-1}\} \end{Bmatrix} \tag{5}$$

Then, the test statistic is calculated:

$$t = \frac{D_{post}-D_{pre}}{s_d/\sqrt{m}} \tag{6}$$

Among them, $\overline{D}_{pre}$ and $\overline{D}_{post}$ are the sample means of the difference values before and after the policy, s_t are the standard deviation of the paired difference, and $df = m - 1$ are the degrees of freedom.

Based on the calculated t-statistic and degrees of freedom, the corresponding p-value is looked up. Due to space limitations, only the P-values of 20 policies are listed, as shown in Table 2.

Table 2: P-values after pairedt-test for difference samples in some countries.

China2017	China2021	Ukraine2016	Israel2015	Iran2014
0.32	0.26	0.02	0.07	0.5
Russia2016	Indonesia2023	India2013	Turkey2013	Brazil2020
0.15	0.01	0.008	0.012	0.34
Germany2016	Italy2018	Japan2014	France2018	Poland2016
0.02	0.33	0.04	0.41	0.05
Thailand2019	USA2013	USA2021	USA2023	UK2016
0.61	0.001	0.78	0.002	0.005

If the P-value is less than 0.05, the null hypothesis is rejected and it is considered that there is a significant difference in the means between the two time points (or conditions). As can be seen in Table 2, its analysis of policy effectiveness is highly consistent with ITSA. In this regard, the use of this model corroborates our previous analysis of policy effectiveness.

Finally, the preprocessed policy data is formed into a corpus and modeled to obtain the vector space of the corpus. The vector space contains information on the distribution of all words in the corpus:

$$D = (d_1, d_2, d_3, \ldots, d_{145})^T \tag{7}$$

$$d_i = (w_{i,1}, w_{i,2}, \ldots, w_{i,887}) \tag{8}$$

Among them, d_i represents the i-th vector of the policy th in the vector space; $w_{i,j}$ represents the weight of the ij-th feature item in the j-th comment.

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

3.3 Empirical Analysis Based on Natural Language Processing

The word cloud of high-frequency terms related to effective policies is shown in Figure 4:

Figure 4: Effective policy high-frequency word wordcloud.

(1) Enhancing International Cooperation: Encourage collaboration with other countries in the field of cybersecurity to jointly address transnational cyber threats. Strengthen cyber law enforcement capabilities through international cooperation, including participating in cyber operation simulation exercises and signing cybersecurity cooperation agreements.

(2) Cybersecurity Research and Education: Support the development of cybersecurity research and education programs to cultivate more cybersecurity professionals and promote technological innovation in cybersecurity.

(3) Protection of Critical Infrastructure: Ensure the security of information systems in critical sectors such as power and transportation, and enhance cybersecurity defense capabilities.

(4) Leveraging Market Forces: Utilize market forces to raise cybersecurity standards. Work with both private and public sectors to ensure that individuals, businesses, and organizations implement effective cybersecurity measures.

(5) Institutional Establishment: Set up cybersecurity departments to share cybersecurity knowledge and address systemic vulnerabilities.

4. Conclusion

This study, from a global perspective, employs quantitative research methods such as Interrupt Time series analysis (ITSA) and natural language processing (NLP) to analyze 145 cybersecurity policies from 137 countries. The aim is to reveal the influencing factors and patterns of policy effectiveness and provide data support for global cybersecurity governance.

4.1 Quantitative Differences in the Effects of Global policies

Through the analysis of the ITSA model, it is found that the inhibitory effects of cybersecurity policies in different countries on cybercrime vary significantly:

After the implementation of South Korea's "Basic Cybersecurity Law", the number of cybercrimes has decreased by an additional 10 units each year (β_3=-10). The policy effect of the United States in 2013 was particularly prominent (β_3=-796), demonstrating a strong and effective inhibitory effect. However, after the implementation of the UK's Data Protection Act, the number of cybercrimes has increased by 14 units (β_3=14) each year, reflecting deficiencies in policy design or implementation. Moreover, the effectiveness of policies is closely related to a country's governance capacity and resource input. For instance, in developing countries like India and Ukraine, India's policy in 2013 (β_3=-21) had a relatively good effect, while Ukraine's policy in 2016 (β_3=6.5) had a limited effect.

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

4.2 Suggestions

By using NLP technology to analyze policy texts, four core policy dimensions, namely international cooperation, protection of critical infrastructure, cybersecurity education and technological innovation, and institutional and system construction, were further summarized. The following suggestions are put forward:

(1) A dynamic evaluation mechanism will be adopted, and quantitative methods will be used to regularly assess the effectiveness of policies, so as to adjust strategies in a timely manner.

(2) Global collaborative governance will be pursued to strengthen international cooperation, particularly in areas such as data sharing and joint exercises, in order to address transnational cybercrimes.

(3) Policies should be designed in multiple dimensions, taking into account both "technical means" and "institutional guarantees", and resources should be allocated in light of the country's national conditions.

4.3 Research Limitations and Future Directions

Although this study covers many countries around the world, the availability of data in some countries is limited. The sample range can be expanded in the future. Furthermore, no in-depth analysis was conducted on the specific obstacles encountered during the policy implementation process. Subsequent research can combine quantitative and qualitative methods to further explore the full-chain influencing factors of policies from text to implementation, providing more comprehensive theoretical support for global cybersecurity governance.

Acknowledgements

This research was supported by the following project: Guangdong Ocean University 2025 Provincial College Students' Innovation and Entrepreneurship Training Program Project (S202510566001S). The 2025 Annual Scientific Research Project of the Guangdong Provincial Undergraduate Mathematics Teaching Steering Committee - "Research and Practice on the Integration of Constructivist Theory in Higher Mathematics Teaching under the Background of New Engineering". Guangdong Ocean University 2025 University-level Educational and Teaching Reform Project (PX-972025016).

References

[1] World Economic Forum. (2025). The 2025 global cybersecurity outlook reveals the increasingly complex cyberspace: News release [Press release]. Retrieved August 6, 2025, from https://www.weforum.org/press-release/2025/01/the-2025-global-cybersecurity-outlook-reveals-the-increasingly-complex-cyberspace

[2] Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. Public Administration Review, 71(3), 455–460.

[3] Andreasson, K. J. (2011). Cybersecurity: Public sector threats and responses. Taylor & Francis.

[4] Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917–938.

[5] Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management, 66, 102520.

[6] Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liability index. SSRN. Retrieved August 6, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3142296

[7] New York State Department of Financial Services. (2023). 23 NYCRR 500: Cybersecurity requirements for financial services companies. Retrieved August 6, 2025, from https://www.dfs.ny.gov/system/files/documents/2023/03/23NYCRR500_0.pdf

[8] PurpleSec. (n.d.). How to develop an effective cybersecurity strategy. Retrieved August 6, 2025, from https://purplesec.us/learn/cybersecurity-strategy/

[9] International Telecommunication Union. (2024). Global cybersecurity index 2024. Retrieved

ISSN 2616-7433 Vol. 7, Issue 7: 1-8, DOI: 10.25236/FSST.2025.070701

August 6, 2025, from https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[10] Verizon. (n.d.). The VERIS community database (VCDB). Retrieved August 6, 2025, from https://verisframework.org/vcdb.html
[11] Gong, C., Liu, G. Z., Li, C. J., et al. (2024). Evaluation of the implementation effect of health management model for stroke patients based on interrupted time series. Chinese Journal of Public Health Management, 40(5), 640–644.
[12] Chung, A., Dawda, S., Hussain, A., Shaikh, S. A., & Carr, M. (2021). Cybersecurity: Policy. In L. R. Shapiro & M. H. Maras (Eds.), Encyclopedia of security and emergency management. Springer, Cham.
[13] Elkhannoubi, H., & Belaissaoui, M. (2015, December). A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification. In 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA) (pp. 1–6). IEEE.
[14] Ghernouti-Hélie, S. (2010, February). A national strategy for an effective cybersecurity approach and culture. In 2010 International Conference on Availability, Reliability and Security (pp. 370–373). IEEE.
[15] Lu, H., & Zheng, W. Y. (2021). Public sentiment research on long-term care insurance policy based on natural language processing. Shanghai Insurance, 7, 47–51.