ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Analysis of global cybercrimes using the fuzzy analytic hierarchy process and multiple regression model summary

Yanan Song, Xirui Jin

Xi'an Eurasia College Yulin, Shanxi, 710065, China

Abstract: The popularization of the Internet has promoted globalization, but it has also increased the risk of cybercrime. Cybercrime is difficult to combat due to its cross - border nature, and many institutions choose not to disclose attack incidents to avoid damage to their reputations. To address this challenge, countries have formulated cybersecurity policies, while the International Telecommunication Union (ITU) plays a leading role in setting standards, promoting cooperation, and assessing global cybersecurity. After researching this issue, our team believes that the core of the problem should focus on three aspects: the distribution and pattern recognition of global cybercrime, the evaluation of policy effectiveness, and the correlation analysis of demographic data. Therefore, this paper analyzes the core issues based on VCDB data and provides effective suggestions for the development and improvement of national cybersecurity policies and laws.

Keywords: Cybercrime; Fuzzy analytic hierarchy process; Multiple regression analysis; Policy evaluation

1. Introduction

1.1. Problem background

Cybercrime refers to the act of using computer technology to attack or damage computer systems or information via the internet, or to commit other illegal activities through the network. Since the 21st century, the history of cybercrime is closely related to the development of computer and network technologies and can be divided into the following stages:

Rapid development stage (Early 2000s - 2010s)

The Internet spread rapidly worldwide, and applications such as e-commerce and social networks emerged continuously. Cybercrime entered a period of rapid development. The means of online fraud became increasingly diverse, and online theft became more rampant. Hackers stole users' account passwords, corporate business secrets, and customer information of financial institutions through various means, causing huge losses to individuals and enterprises. In addition, criminal acts such as online defamation, online rumors, and online intellectual property infringement also emerged in large numbers, seriously affecting social order and the healthy development of the network environment.

Diversification and globalization stage (2010s - Present)

The development of new tech like mobile Internet, big data, and cloud computing has diversified and complicated cybercrime. Viruses and malicious software target mobile devices, stealing info and seizing control. Attacks on IoT devices are rising, threatening smart homes and industrial control systems.Cybercrime is now global. Criminals use the network's borderless nature to operate worldwide, challenging law - enforcement and disrupting the global cyber - security order. Cyber - terrorist activities have also emerged, with terrorist groups using the Internet for propaganda, recruitment, and attack planning, threatening global security and calling for

international cooperation.

1.2. Restatement of the problem

We address three main problems:

Problem 1

Establish a quantitative grading model for cybercrime incidents based on data analysis

Problem 2

Compare policies from 2010-2024 with cybercrime patterns to predict policy impacts.

Problem 3

Cluster policies in five dimensions (law, technology, organizational capacity, capacity building, and cooperation) and evaluate their effectiveness against cybercrime.

2. Assumptions and justifications

- **Assumption 1:**The data used are accurate and valid.
- **Explanations:**Data are sourced from reliable databases and literature.
- **Assumption 2:**Missing data have minimal impact on results.
- **Explanations:**Data concentration is low, and missing values do not significantly affect overall trends.
- **Assumption 3:**Crime rates below 0.5 are excluded.
- **Explanations:**These values represent rare or non-existent cases, simplifying analysis.

3. Descriptive analysis

Question 1 belongs to the problem-description type. Locate the VCDB database according to the literature in the question, and then analyze the corresponding data through the formula for calculating the crime rate. The calculation process is as follows:

$$CCI_i = \left(\frac{Number_i}{population_i} \right) \times Success_i \times Reporting_i \times Pro_i + \epsilon_i \tag{1}$$

Analysis of the VCDB database shows cybercriminals mainly concentrate in the US. This is based on examining malicious IPs, malware - spreading sources, and attack server locations. The US's advanced tech and large digital ecosystem, with many connected devices and high - value digital assets, may attract them, providing more targets and hiding places.

The research indicates that cybercriminals tend to achieve success in the Russian region. In contrast, the South Korean region is where their attempts are often thwarted. It should be noted that due to the lack of data for some countries, relevant information is not included in the table.

Upon comparing the data, it becomes evident that the rates at which crime victims report in regions such as Colombia, Bolivia, and Peru have hit 100%. Consequently, these regions are regarded as the ones with the highest reporting frequencies across all regions. In the figure, the region painted the darkest indicates the area with the highest reporting rate, whereas the region in the lightest shade represents the one with the lowest reporting rate.

An analysis of cyber - crime industry distribution shows criminals mainly target public administration, medical, and educational services.

Data examination reveals economic and cultural factors are key in high - crime regions. In the US, cyber -

crimes focus on densely - populated, wealthy urban areas with a large wealth gap.

South Korea is seen as a cyber - crime - prevention area. Thanks to manual interception, cyber - security education, and strict laws, criminal activities have been reduced.

4. Analysis of policies and crime rates

To better understand cyber - crime and develop effective countermeasures, we compare policies from different countries to assess their impact on cybercrime. This analysis covers legislative frameworks, law - enforcement strategies, and public - awareness efforts.

After comparing the data on cybercrime cases and non - success rates before and after policy implementation, we can observe clear trends. Some countries have witnessed a significant drop in cybercrime cases after implementing strict laws and strengthening law - enforcement cooperation. However, in some regions, the non - success rate of preventing cyber - attacks remains high, possibly due to policy implementation loopholes or evolving cyber - criminal tactics.

5. Correlation Analysis

We use a multiple regression model to analyze the correlation between cybercrime rates and factors like per capita GDP, Internet usage, education levels, and policy scores. The model is based on data from 2010 to 2020.

Analysis of Symbol Meanings

1. $\bar{X}$ and $\bar{Y}$

It represents the sample means of variables (X) and (Y).

Calculation method:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i, \quad \bar{Y} = \frac{1}{n}\sum_{i=1}^{n} Y_i \tag{1}$$

For example $\bar{X}$ is the average value of the per capita GDP of all countries.

Using the above formula to organize the data and conduct a correlation analysis, we obtain the following heatmap:

Table 1. Multiple regression analysis.

variable	Crime rate	Per capita GDP	Internet average usage share per capita	Master's degree or above	Total public expenditure on education	Policy Score	Educational level (high school)
Crime rate	1.00	0.45	0.82	-0.18	0.10	-0.68	-0.22
Per capita GDP	-0.45	1.00	0.65	0.25	-0.30	0.52	0.15
Internet average usage share per capita	0.82	0.65	1.00	-0.05	0.12	-0.55	-0.10
Master's degree or above	-0.18	0.25	-0.05	1.00	-0.18	0.20	-0.33
Total public expenditure on education	0.10	-0.30	0.12	-0.18	1.00	-0.25	0.05
Policy Score	-0.68	0.52	-0.55)	0.20	-0.25)	1.00	0.18
Educational level (high school)	-0.22	0.15	-0.10	-0.33	0.05	0.18	1.00

6. Sensitivity analysis

We standardized the regression model using Z-scores and found that Internet usage rate (0.72) and per capita GDP (0.31) have the most significant impact on crime rates. Policy scores (-0.58) also play a crucial role in reducing crime rates.

According to the calculation results, the standardized coefficients are as follows:

Table 2. The standardized coefficients.

variant	β_i coefficient	Explain
Internet usage rate	0.72	For every one - standard - deviation increase in the Internet usage rate, the crime rate rises by 0.72 standard deviations (having the greatest impact).
policy score	-0.58	For every one - standard - deviation increase in the policy score, the crime rate drops by 0.58 standard deviations.
per capita GDP	0.31	The level of economic development has a certain impact on the crime rate.
Master's degree or above	-0.12	An increase in the proportion of people with high - level education may curb the crime rate, but the effect is weak.
Education expenditure	0.05	The impact is negligible.
High school education level	-0.03	The impact is extremely weak.

7. Model evaluation

7.1. Strengths

We used diverse analytical techniques, including global heatmaps and regression models, to explore data from multiple perspectives.

The model integrates fuzzy AHP and multiple regression analysis, providing scientific support for policy recommendations.

7.2. Weaknesses

Data interpretation may not fully cover all dimensions, potentially limiting comprehensive understanding.

8. Memo

Our analysis shows that cybercrime is positively correlated with per capita GDP and Internet usage rates. High-income countries like the US and UK are primary targets. Effective policies, such as those in New Zealand, demonstrate successful crime rate control through strong social welfare and security management. Despite high policy scores, countries like the US face challenges due to socioeconomic disparities. International cooperation and policy sharing are essential for combating global cybercrime.

About the author

Yanan female Song
Year of birth: 2005
Degree: Undergraduate
Family: Han
His main research interests are primary education
School: Xi'an Eurasia University
Zip code: 710065
Telephone: 13325407129
Nationality: Yulin City, Shaanxi Province

About the author of the second work: Xirui Jin male
Year of birth: 2003
Degree: Undergraduate
Ethnicity: Han
Main Research Directions: Primary Education (Mathematics)
School: Xi'an Eurasia University
Zip code: 710065
Telephone: 13506618517
Nationality: Wenzhou City, Zhejiang Province

AI Usage Report

This article uses AI to assist in searching for data, literature and other materials, leveraging it to improve the team's data search efficiency. Except for the data and materials part, the rest of the content was independently completed by our team.

References

[1] Ntogwa Ng'habi Bundala.(2024).Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures.Asian Journal of Research in Computer Science(12),234-251.

[2] Namseol Baek.(2024).Analysis of Cybercrime Organization and Status in North Korea.International Journal of Terrorism & National Security

[3] DiMolfetta D .US disables global cybercrime network that enabled theft of billions in fraud schemes[J]. Nextgov.com (Online),2024,

[4] Shuai C ,Mengmeng H ,Fangyu D , et al.Exploring the global geography of cybercrime and its driving forces.[J].Humanities & social sciences communications,2023,10(1):71-71.

Appendices

Appendix 1

Introduce: All vector graphics in the article

https://github.com/Y-1-one/2025-ICM-Problem-F-Appendix-Data.git

Problem Chosen: F
2025MCM/ICM
Summary Sheet Team Control Number: 2509327