# Research on cybercrime and cybersecurity based on the '2M+A' theory

Zhenzhong Liu *

Hunan Agricultural University, Changsha, China

* Corresponding Author Email: 17873866858@163.com

**Abstract.** Nowadays, cybercrime is becoming more and more frequent, and it is necessary to find a balance between the development of Internet technology and cybercrime. This paper focuses on cybersecurity and cybercrime, and conducts an in-depth study based on the '2M+A' theory. Using panel data on the number of cybercrimes in each country from 2012 to 2021, it adopts the AHP-TOPSIS model, the multiple linear regression model, and the two-way fixed effect model to study the distribution pattern of cybercrime. The results of the paper show that: (1) Countries with perfect legal and organization measures mostly choose to report and prosecute, and the stricter the legal measures and the more advanced the technical measures, the faster the number of cybercrimes decreases. (2) The number of people using the network, the level of economic development, the level of education and other factors are closely related to the number of cybercrimes. This paper analyses the potential factors behind cybercrime and cybersecurity from multiple perspectives by using a variety of models, with a view to providing new theoretical perspectives for optimizing cybersecurity.

**Keywords:** AHP-TOPSIS Model, cybercrime, cybersecurity multiple linear regression, two-way fixed effect.

## 1. Introduction

With the rapid development of information technology, cyberspace has been deeply integrated into all areas of people's lives and has become an indispensable part. However, the rapid development of Internet technology has also given rise to cybercrime. At present, the problem of cybercrime is getting more and more serious, which brings huge losses and threats to individuals, enterprises and even the state. Its transnational, virtual and anonymous nature has given rise to more and more diversified means of attack, which makes dealing with cybercrime a very challenging task.

In past studies, many scholars have explored cybercrime and cybersecurity from different perspectives. Bruce M (2024) and others found through expert surveys that cybercrime is a worldwide problem, with a small number of countries (or regions) accounting for the majority of cybercrime [1]. Lee (2022) found that insufficient self-discipline and attitudes towards cybercrime had a significant impact [2]. Rosario D (2022) found that the development of Internet technology has made cybercrime more prevalent and that a broader legal strategy needs to be established to limit its growth [3]. Nguyen H V (2019) also suggests that the jurisdiction of regulators over cybercrime should be a little more expansive [4]. Hamed Taherdoost (2024) found that the current state of cyber is not the same in different countries, then the type of cybercrime will also tend to be different [5]. Althibyani H A (2023) and others proposed to enhance digital skills education for citizens to improve digital skills and prevent cybercrime [6]. AlDaajeh S (2022) and others also found that training in cybersecurity education is an important part of reducing cybersecurity [7]. Chai S M (2012) and others proposed to increase the employment of qualified and professional cybersecurity technicians in order to prevent cyber senior intellectuals from going astray, which can lead to more serious cybercrime incidents [8]. AlDaajeh S and others (2024) suggested that the importance of enhancing cybersecurity for the maintenance of the nation cannot be overstated [9]. Wang L (2020) and others noted that institutions of higher education need to update their cybersecurity curricula to continually meet the needs of cybersecurity education for today's college students [10].

A review of the above literature reveals that the current academic community is still deficient in comprehensively analyzing the factors influencing cybercrime and in providing comprehensive guidance for the development of strategies. Specifically, some studies tend to explore the role of a single factor on cybercrime in isolation and lack a systematic and comprehensive consideration of multiple factors. In addition, some studies have failed to adequately connect the use of data to practice, resulting in a certain degree of disconnect between theory and practice. Accordingly, this paper takes countries around the world as the object of research and uses a variety of theoretical models to analyse the potential influencing factors of cybercrime, with a view to providing new theoretical perspectives on cybersecurity strategies and the reduction of the number of cybercrimes in countries around the world.

## 2. Data and methodology

### 2.1. Sample Selection and Data Sources

The data used in this paper come mainly from publicly available data from The International Telecommunication Union, the United Nations, the VERIS website, and the SEON website. The main variables in the paper include the number of cybercrimes, gross domestic product, secure Internet server, the public expenditure on education, the number of people using the network. Due to inconsistencies in data collection methods and lack of standardization. Many of the data were not reported or recorded and were not included in the study. After removing samples with significant data gaps, a global sample of 87 countries was finalized for the study. After data collection, in order to deal with these missing data, the missing values were predicted to be filled in by building regression equations based on a linearly interpolated version of the data using information on the core variables in the original dataset, and the reliability of the data was ensured by cross validation. However, the data may have certain limitations, for example, cybercrime data may not fully reflect the actual situation, which provides a direction for future research.

### 2.2. Introduction to the Methodology

#### 2.2.1. Cybercrime Pattern Analysis

This paper examined information and reports on cybercrime and chose to use the GCI indicator, the CSI indicator, as the basis for the discussion of the distribution of cybercrime in this study, and to use an evaluation model to comprehensively examine which countries report incidents and prosecute offenders when cybercrime occurs.

#### 2.2.2. Strategic Impact Analysis

Data visualization was first used to find out whether there is a correlation between the change in the number of cybercrimes in each country and whether there is a correlation between the unit time of enactment of cybersecurity strategies, and then regression analyses were used to verify whether there is any of the above relationships.

#### 2.2.3. Cybercrime Effects Analysis

The relationship between the number of people using the network and the distribution of cybercrime is analyzed using two-way fixed effects using the published data from the United Nations on human characteristics, and then the reliability of the results is provided by doing sensitivity analyses on the reduction of the number of people using the Internet by one, two, and three standard deviations.

#### 2.2.4. Suggestion

Synthesise the results and analyses of the first three to provide guidance for a national cybersecurity strategy.

Methodology can be visualized in the following flowchart, as is shown in Figure 1.

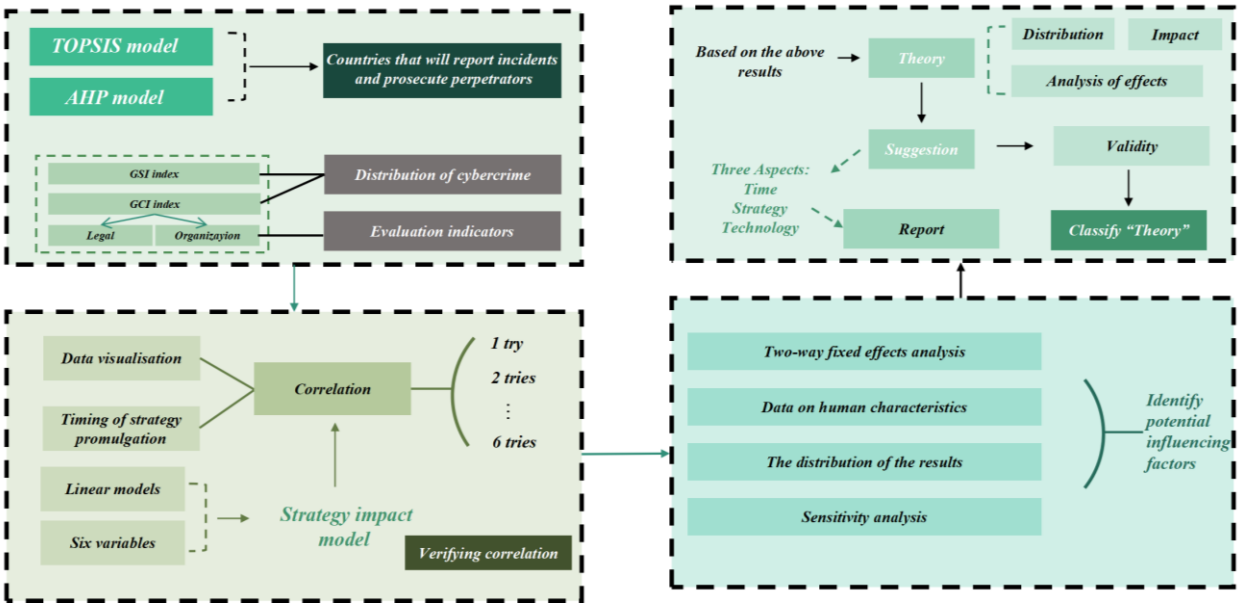


**Figure 1.** Flow chart

## 3. Modelling and solution

### 3.1. The Cybercrime Pattern Model

#### 3.1.1. Selection of Indicators

This paper chooses 2 metrics to measure the high rate of cybercrime reporting and prosecution, namely 2 primary indicators (PI) each, as is shown in Figure 2.

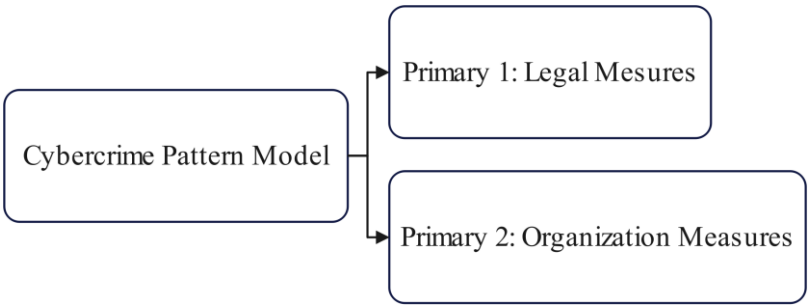


**Figure 2.** Indicators chart

#### 3.1.2. AHP and Topsis Analysis

*(a) Topsis Determination of PI Weights.*

(1) The normalized matrix C obtained from the data processing in the previous step:

$$C = \begin{bmatrix} c_{11} & \cdots & c_{1m} \\ \cdots & \cdots & \cdots \\ c_{n1} & \cdots & c_{nm} \end{bmatrix} \quad (1)$$

(2) Defining the maximum value:

$$Z^{+} = (Z_1^{+}, Z_2^{+}, \cdots Z_m^{+}) = (\max\{c_{11}, c_{21}, \cdots, c_{n1}\}, \max\{c_{12}, c_{22}, \cdots, c_{n2}\}, \max\{c_{1m}, c_{2m}, \cdots, c_{nm}\}) \quad (2)$$

(3) Defining the minimum value:

$$Z^{-} = (Z_1^{-}, Z_2^{-}, \cdots Z_m^{-}) = (\min\{c_{11}, c_{21}, \cdots, c_{n1}\}, \min\{c_{12}, c_{22}, \cdots, c_{n2}\}, \min\{c_{1m}, c_{2m}, \cdots, c_{nm}\}) \quad (3)$$

(4) Define the distance of the ith (i = 1, 2, ..., n) the distance of the evaluation object from the maximum value is

$$D_i^+ = \sqrt{\sum_{j=1}^{m}\left(Z_j^+ - Z_{ij}\right)^2} \quad (4)$$

(5) Define the ith (i=1, 2, ..., n) the distance of the evaluation object from the minimum value is

$$D_i^- = \sqrt{\sum_{j=1}^{m}\left(Z_j^- - Z_{ij}\right)^2} \quad (5)$$

(6) The calculation yields a score for the ith (i=1, 2, ..., n) evaluation object not normalized score:

$$S_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad (6)$$

*(b) AHP Calculation of PI Weights.*

Although Topsis model gives us an objective weight through entropy measurement, in the context of the current gradual implementation of cybercrime legal supervision, we must pay more attention to the implementation of legal measures under cybercrime.

In order to deal with this situation, we introduced AHP to adjust the weight. We believe that cybercrime reporting and prosecution rates are equally important to the extent of future improvement, while legal measures are more important than other measures. Through the Eigenvector Method, we calculate the weights of PIs, with $a_1$= 0.7, $a_2$= 0.3 for legal measures and organization measures, respectively. Then, we allocate weights the indicators according to their internal data and relative weights of PIs.

The consistency test for the PIs guarantees each, as is shown in Table 1.

**Table 1.** Consistency test results

| Maximum Eigenvalue | Consistency Index (CI) | Random Index (RI) | Consistency Ratio (CR) | Result (CR<0.1?) |
|---|---|---|---|---|
| 2 | 0.04 | 0 | 0 | PASS |

We can see that the consistency ratio is less than the threshold, hence, we are confident to determine $\beta_j$, as is shown in Figure 3 below. It shows that the AHP algorithm has successfully adjusted the weights we find out with Topsis model, for the largest weights are all distributed to the first PI: legal measures.

### 3.1.3. Quantitative Analysis and Visualization Analysis Definitions

By collecting, sorting out and analyzing the global cybersecurity index of each country (the average of the national cybersecurity index, global cybersecurity index and cybersecurity exposure index), the top ten and bottom ten countries in the global cybersecurity index ranking and their scores are sorted out, and analyzed, as shown in Figure 4 below. Obviously, the top ten countries in network security scores are all developed countries, and the last ten are developing countries. The data shows that the level of economic and technological development is positively related to the cybersecurity index. Developed countries generally invest more in cybersecurity protection, the relevant security equipment is also relatively comprehensive, and the technology is also relatively advanced, it shows that a country's economic development level is closely related to the national cybersecurity index.

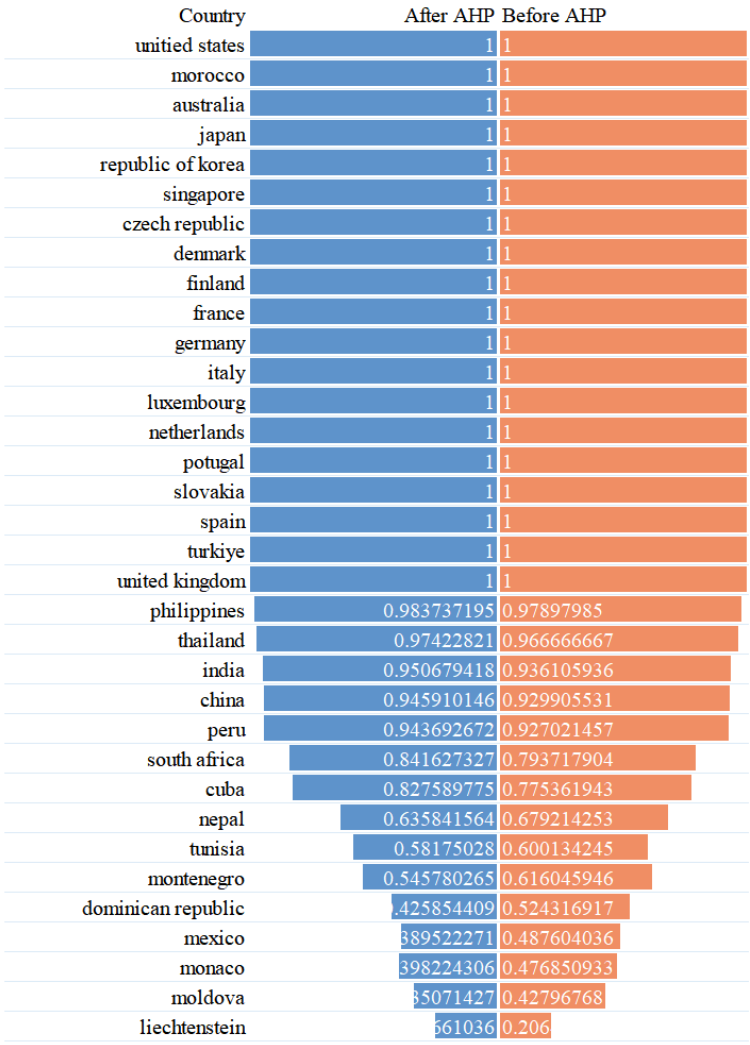


**Figure 3.** The weights of PIs

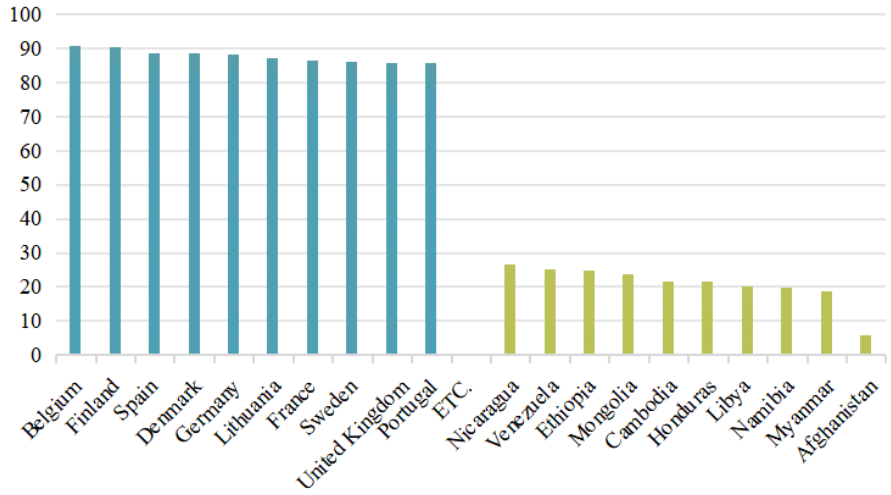


**Figure 4.** Top 10 and bottom 10 cybersecurity index countries

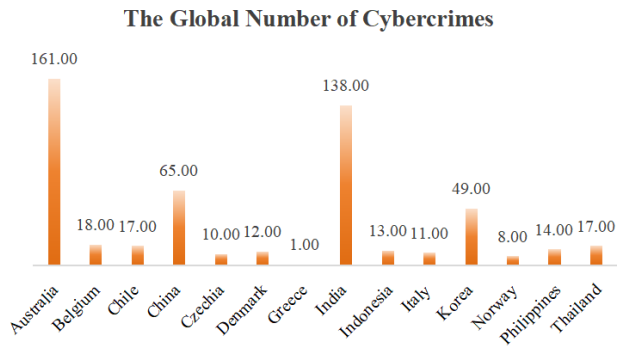


**Figure 5.** The Global Number of Cybercrimes

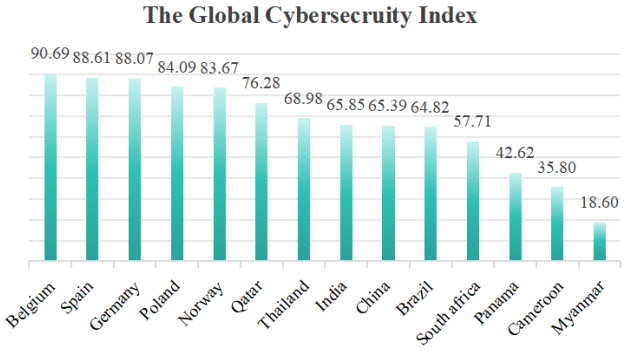


**Figure 6.** The Global Cybersecurity Index

As shown in figures 5 and 6 above, the comparison between the global cybersecurity index distribution and the network crime number distribution shows that some developed countries have high cybersecurity index and more cybercrime incidents, while some areas with low cybersecurity index have relatively few cybercrimes. For the occurrence of this phenomenon, it may be that some developed countries such as North America have advanced technology, strong economic strength, and have a large investment in cybersecurity construction, showing a good cybersecurity situation, but also because of the highly developed Internet economy, they have become the target coveted by cybercriminals. On the contrary, the cybersecurity index in economically backward areas is low, but at the same time, the level of network development is limited, which limits the development of cybercrime to a certain extent.

In a word, there are many relationships between the cybersecurity index and the number of cybercrimes. When formulating cybersecurity strategies, countries need to carry out cybersecurity protection and governance in a targeted manner in combination with their own Internet development level, network application scenarios and other factors.

### 3.2. Strategy Impact Model

#### 3.2.1. General Situation of Global Network Strategy

Indeed, the digital frontier we enjoy today opens up a world of risk and opportunity. Cybercrime is extremely complex and specifically covers six areas: Geopolitical tensions, Cyber skills gap, AI and emerging tech, Regulatory requirements, Supply chain interdependencies, Cybercrime sophistication. With the click of a mouse, it is easier than ever for fraudsters and other criminals to find unsuspecting victims. This has created a new area of prosperity for people with criminal intent who can attack innocent Internet users from the comfort and security of their homes.

Cybercrime, which has emerged with the development of information technology, has brought some harm to the world. In order to cope with these growing cyber threats, countries have formulated strong cyber security policies and enacted laws aimed at combating cybercrime and protecting their countries from the dangers of the Internet. The International Telecommunication Union (ITU) created the Global Cybersecurity Index (GCI) in order to standardize the effectiveness of cybersecurity strateyies developed by countries in five different aspects, including legal measures, technical measures, organizational measures, capacity development, cooperation measures. The results of the index highlight significant improvements made by countries, such as increasing basic legislation, establishing incident response mechanisms, developing clearer national plans, training people across society and working with national and international partners.

#### 3.2.2. Model Preparation

Analysis of changes in cybercrime situations:

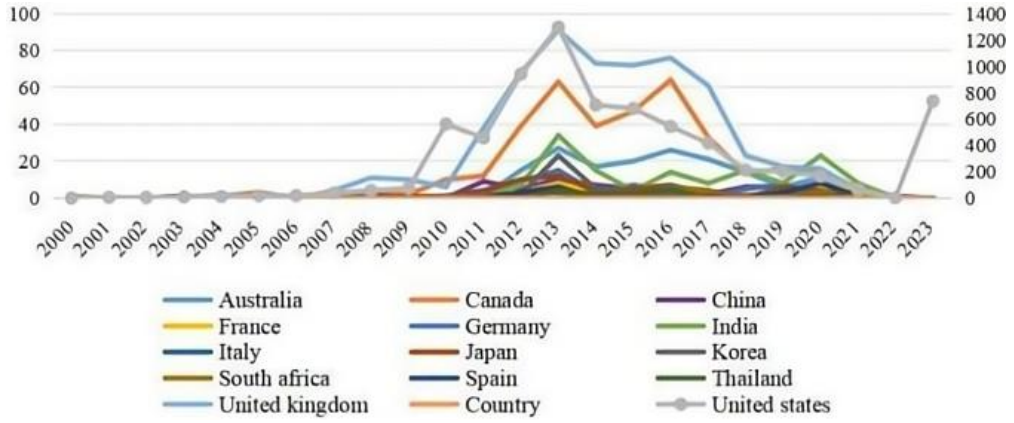


**Figure 7.** The change of the number of cybercrimes in some countries from 2000 to 2023

Figure 7 shows the changes in the number of cybercrimes in multiple countries such as Australia, Canada, China, and India from 2000 to 2023. Overall, it went through a low - level stable period from 2000 to 2009, a significant upward period from 2009 to 2013, a high - level fluctuating growth period from 2013 to 2017, and a downward trend from 2017 to 2023.

During the initial stage of Internet development from 2000 to 2009, the narrow scope of popularization, small number of users, and high technical threshold limited the number of crimes. From 2009 to 2013, with the popularization of mobile devices, the number of users skyrocketed. The rise of online social networking and online payment provided more targets and opportunities for cybercrimes, leading to a significant increase in the number of such crimes. From 2013 to 2017, cybercrimes became industrialized and organized. Criminals illegally obtained and sold data, carried out precision fraud, and the development of the Internet led to the accumulation of security vulnerabilities in software and systems. With lagging security protection, the number of crimes was difficult to control.

From 2017 to 2023, governments and enterprises of various countries attached importance to network security, increased investment, enhanced protection capabilities, improved laws and regulations, strengthened law enforcement, carried out special campaigns and international cooperation to deter criminals. From a strategy perspective, Belarus introduced the "Personal Information Protection Law" in May 2021. Russia approved and promulgated the "Framework of State Strategy in the Field of International Information Security of the Russian Federation" on April 12, 2021. The United Kingdom released the "National Cyber Strategy" in December 2021. The United States introduced the "IoT Cybersecurity Improvement Act of 2020" in 2020. The chart shows that after 2020, the number of cybercrimes decreased significantly, indicating that cybersecurity strategies can effectively reduce crimes.

### 3.2.3. Model Establishment

Based on this, in order to better explain the impact of policies on the number of cybercrimes, we have established the following multivariate regression model.

$$Y_i = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \varepsilon_i \quad (7)$$

$Y_i$ represents Total Events, which is an interpreted variable, that is, the variable that tries to predict or explain its changes in the analysis. $\varepsilon_i$ represents the random error term

$X_1$ represents the independent variable Legal Measures (LM), $X_2$ represents Organization Measures (OM), $X_3$ represents Technical Measures (TM), and $X_4$ represents Capacity Development (CD), $X_5$ represents Cooperation Measures (CM). These variables are used to explain the changes of the dependent variable Total Events and explore their impact on the dependent variables through regression analysis.

First of all, the Z-score standardization method is used to standardize the model:

$$Z_i = \frac{X_i - \mu_i}{\sigma_i} \quad (8)$$

$X_i$ is the value of the original variable, $\mu_i$ is the mean of the variable, and $\sigma_i$ is the standard deviation of the variable; through standardization, the framework is eliminated and the unfair impact caused by the difference in the framework is avoided.

### 3.2.4. Results and Regression Analysis

The results of the multiple linear regression are shown in Table 2 below:

**Table 2.** Multiple regression analysis results of each variable

| Variable | LM | OM | TM | CD | CM |
|---|---|---|---|---|---|
| $\hat{\beta}$i | -31.88<br>(123.0) | 2.786<br>(137.6) | -10.63<br>(162.1) | 78.48<br>(192.4) | 27.22<br>(128.8) |

Based on the regression results, the variables of legal measures and technical measures show a negative correlation with the number of cybercrimes. The improvement of legal measures can clearly define various types of cybercrime behaviors and penalty standards. The investment in cybersecurity technology can enhance the technical levels of network monitoring, early warning, and defense, preventing cyberattacks, thus inhibiting the occurrence of cybercrimes to a certain extent.

However, the variables of organization measures, capacity development, and cooperation measures show a positive correlation with the dependent variable. This may be because an increase in organization measures, along with adjustments in institutional personnel, leads to organization incoordination, thereby reducing the prevention and control capabilities. During the construction of capacity development, the new technologies and systems adopted have security vulnerabilities. The increase in cooperation measures also provides new opportunities for criminals. They take advantage of some loopholes in international cooperation, such as legal differences and information transfer time lags, to evade crackdowns, ultimately resulting in an increase in the number of cybercrimes.

## 3.3. Cybercrime Effects Analysis

### 3.3.1. Variable Description

The variable to be interpreted is the number of cybercrimes. According to the definitions derived from multiple international organizations and the above, cybercrime includes many types. And the Verizon website used its way to collect the number of cybercrime incidents around the world. Therefore, we use the number of cybercrime incidents provided by that website as the explained variable of this analysis and renamed it to the number of cybercrimes.

The core interpretation variable is the number of people using the network. The larger part of the relevant research has rarely dealt with factors related to demographic characteristics. Therefore, this analysis discusses the distributional characteristics of cybercrime in terms of demographic characteristics, taking into account the human factor and the fact that ‘the global village is getting smaller and smaller’, and therefore chooses to use the number of cybercrime offenders to describe demographic characteristics.

In order to control the interference of other influencing factors that bring uncertainty to empirical results, the following control variables are selected by referring to relevant research.

*(a) The level of economic development:*

The gap in the level of economic development is an important factor affecting cybercrime. Cybersecurity problems will occur frequently in areas with low levels of economic development, which will affect the number and distribution of cybercrime. Here, gross domestic product is used to characterize the gap in the level of economic development of different countries.

*(b) Technological development*

The gap in the level of technological development is one of the factors in the increasing number of cybercrimes. The better the technological development of the area, the more complete the number of cybersecurity equipment suitable for it will be, and the higher the complete level. Secure Internet servers are used here to characterize the technological development gap between countries.

*(c) Education level:*

The level of education directly affects the quality of people who use the Internet. Highly educated Internet users usually have a higher quality of using the Internet and can regulate their own behavior, thus affecting the distribution of cybercrime. Here, the public expenditure on education is used to characterize the gap in education levels between countries.

### 3.3.2. Analysis and Solution Stage

*(a) Model Establishment*

In this analysis, the two-way fixed effect model is mainly used to analyze the impact of the number of people using the network in countries on the distribution of cybercrime. The two-way fixed effect model can control the year fixed effect and the country fixed effect at the same time, so as to effectively solve the possible problem of missing variables and improve the accuracy of the estimate. The specific model settings are as follows:

$$Y_{it} = \alpha_i + \lambda_t + \beta X_{it} + \gamma_j \sum_{j=1}^{n} Z_{jit} + \varepsilon_{it} \quad (9)$$

Among them, $Y_{it}$ indicates the number of cybercrimes in country i in year t, $X_{it}$ indicates the number of people using the network, $\alpha_{it}$ indicates the fixed effect of the country, $\lambda_t$ indicates the fixed effect of the year, and $\varepsilon_{it}$ represents the random error term.

*(b) Solving Steps*

(1) Verify whether there is a correlation between each variable, and test the multiple colinear problems between variables.

(2) Do the regression analysis of ordinary least squares first, and then add the country fixed effect and the year fixed effect.

(3) Finally, use data tailing, changing the sample interval, and the system GMM method to test the robustness.

*(c) Results*

As shown in Table 3, the Person correlation matrix shows that the correlation between variables is very small, which can exclude the endogenous problem of variables.

**Table 3.** Correlation results

| | lnSIS | lnGDP | lnPEE | lnNUN |
|---|---|---|---|---|
| lnSIS | 1 | | | |
| lnGDP | 0.347 | 1 | | |
| lnPEE | 0.271 | 0.0007 | 1 | |
| lnNUN | 0.786 | 0.378 | 0.255 | 1 |

As shown in Table IV below, all VIF values are lower than the critical value of 10, which indicates that multiple collinearities does not pose a threat to the effectiveness of regression estimates.

**Table 4.** Multi-collinearity test

| Variable | VIF | 1/VIF |
|---|---|---|
| NUN | 2.720 | 0.367 |
| SIS | 2.680 | 0.374 |
| GDP | 1.190 | 0.839 |
| PEE | 1.100 | 0.909 |

Judging from the analysis of two-way fixed effect and the regression results of controlling other variables, as shown in Table V, there is a positive correlation between the number of people using the network (NUN) and the number of cybercrimes. The possible reason is that the more people using the network, the more people may engage in cybercrime, resulting in being deceived, data leakage and other events. The higher the frequency will be; however, gross domestic product (GDP) and secure Internet servers (SIS) have an inverse relationship with the number of cybercrimes. The reason may be that the better the economic level develops, the more secure Internet servers, the richer people's living standards, the fewer the number of people engaged in cybercrime, and the lower the possibility

of accessing the insecure Internet; the impact coefficient of the public expenditure on education is significantly positive, which indicates that the higher the level of education, the more people who want to learn advanced technology will create an "opportunity" for them to engage in cybercrime.

**Table 5.** Two-way fixed effects results

| | OLS (1) | OLS (2) | TFE (3) | TFE (4) |
|---|---|---|---|---|
| lnSIS | -2.182*** (0.676) | -1.585*** (0.587) | -1.185*** (1.021) | -0.031*** (1.033) |
| lnGDP | | -8.036*** (2.638) | | -17.801*** (10.312) |
| lnPEE | | 11.343** (4.532) | | 6.556** (5.611) |
| lnNUN | | 9.136*** (3.157) | | 14.536*** (5.334) |
| _cons | -3.895** (1.965) | -186.016*** (62.051) | 16.272** (5.570) | 398.485*** (237.414) |
| Adding Control Variables | No | Yes | No | Yes |
| Country Fixed Effects | No | No | Yes | Yes |
| Year Fixed Effects | No | No | Yes | Yes |
| F | 10.432 | 3.016 | 1.346 | 2.689 |

Standard errors in parentheses
* p < 0.1, ** p < 0.05, *** p < 0.01

## 4. Conclusion

This paper collects cybercrime data from 87 countries and Global Cybersecurity Index (GCI) indicators through quantitative and visual analyses, and explores the potential factors of cybercrime and cybersecurity in an in-depth, comprehensive, and comprehensive manner by using models such as AHP-TOPSIS, Multiple Linear Regression, Two-way Fixed Effect, etc., in order to support the theory of '2M+A' theory. The paper shows that legal measures, technical measures, cooperation measures and exchanges among countries, the level of economic development, and the number of secure Internet server are inversely proportional to the rate of cybercrime; and that the organization measures of each country, capacity development, the number of people using the Internet, and the level of education are inversely proportional to cybersecurity.

Through large-scale data collection and multi-model analysis, this study provides new explanations for the differences in global cybersecurity strategies and highlights the application value of the '2M+A' theory. The study suggests adopting regional differentiated governance and strengthening international cooperation and data sharing to optimize cybersecurity strategies and reduce cybercrime. Future research could further expand the indicators, broaden the scope and adopt more complex models to analyse the problem of cybercrime in depth, so as to better meet the challenges posed by the development of information technology.

## References

[1] Bruce M, Lusthaus J, Kashyap R, et al. Mapping the global geography of cybercrime with the World Cybercrime Index [J]. Plos one, 2024, 19 (4): e0297312.

[2] Lee, Seong-sik. "The Effects of Three Major Factors and the Moderating Effect of Pro-Illegal Cultural Environment on Cybercrime." Journal of Criminal Policy Research, 2022, 33 (4): 71 - 89.

[3] Rosario D. Relationship between Cybercriminal Activity and Legislative Treaties: A Quantitative Correlative Study [D]. Northcentral University, 2022.

[4] Nguyen H V. Cybercrime in Vietnam: A critical analysis of its regulatory framework [D]. University of Portsmouth, 2019.

[5] Hamed Taherdoost."Insights into Cybercrime Detection and Response: A Review of Time Factor."Information 15.5 (2024).

[6] Althibyani H A, Al-Zahrani A M. Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime [J]. Sustainability, 2023, 15 (15): 11512.

[7] AlDaajeh S, Saleous H, Alrabaee S, et al. The role of national cybersecurity strategies on the improvement of cybersecurity education [J]. Computers & Security, 2022, 119: 102754.

[8] Chai S M, Kim M K. A road to retain cybersecurity professionals: An examination of career decisions among cybersecurity scholars [J]. Journal of the Korea Institute of Information Security & Cryptology, 2012, 22 (2): 295 - 316.

[9] AlDaajeh S, Alrabaee S. Strategic cybersecurity [J]. Computers & Security, 2024, 141: 103845.

[10] Wang L, Yang J, Wan P J. Educational modules and research surveys on critical cybersecurity topics [J]. International Journal of Distributed Sensor Networks, 2020, 16 (9): 1550147720954678.