World Journal of Information Technology
Print ISSN: 2959-9903
Online ISSN: 2959-9911
DOI: https://doi.org/10.61784/wjit3051

QUANTITATIVE ASSESSMENT AND COMPARATIVE STUDY OF NATIONAL CYBERSECURITY POSTURE BASED ON GLOBAL CYBERSECURITY INDEX

ZiHan Jin
Hohai University, Nanjing 210000, Jiangsu, China.
Corresponding Email: 1401062329@qq.com

Abstract: The Internet is indispensable for everyone, but with its rapid development, the accompanying problem of cybercrime has gradually become a significant challenge that countries worldwide must face. In order to assist countries in formulating better policies and establishing effective cybersecurity models, this study conducts an in-depth analysis of the effectiveness of existing policies from multiple dimensions, based on the GCI scoring mechanism. The research involved the collection of substantial data related to cybercrime, leading to the creation of heat maps depicting the number of cybercrime cases, the GCI scoring level, and the prosecution rates of cybercrime cases. The analysis and comparison of these graphs revealed that developed countries in Europe and the United States are the primary targets of cybercrime and have a high probability of sanctioning such crimes. Additionally, a ridge regression model was established based on the demographic characteristics of each country to examine the relationship between cybercrime cases and factors such as GDP, population size, Internet penetration rate, education penetration rate, and policy implementation environment. The coefficients for these factors were found to be 1. 22, 0. 54, 2. 55, -1. 46, and -0. 45, respectively, with population size being the most influential factor in the number of cybercrime cases. A sensitivity analysis further confirmed this finding. The study also classified the cybersecurity policies of various countries based on the five dimensions of the GCI and used a Difference-in-Differences (DID) model to evaluate the effectiveness of these policies. The results revealed that the most effective policy types differ across countries. International cooperation proved most effective in less developed countries, lawmaking in developing countries, and technological upgrading in developed countries.
Keywords: Cybercrime; Cybersecurity; Ridge regression model; GCI; DID model

1 INTRODUCTION

Cybersecurity challenges are becoming increasingly grave, resulting in substantial financial losses for both individuals and enterprises. Phishing, ransomware, DDoS assaults, and online fraud on social media constitute significant dangers. Confronting these difficulties necessitates a collaborative endeavor among individuals, enterprises, and governmental bodies.

The increasing interdependence of contemporary technology has revolutionized worldwide communication and commerce while simultaneously creating new vulnerabilities, since cybercrime presents a considerable risk to national and international security. Cybercrimes frequently transcend national borders, resulting in jurisdictional complications, while many industries refrain from reporting breaches, thereby allowing hackers to function without consequence. In response to these challenges, numerous countries have established national cybersecurity regulations, while the International Telecommunication Union (ITU) is crucial in establishing global standards and promoting international collaboration in cybersecurity initiatives. The current and future cybersecurity workforce in the public and private sectors are essential frontline defenders of our nation's digital infrastructure[1].

In the existing literature system of cybersecurity, there are several pressing issues that need to be addressed. Firstly, although various cybersecurity protection measures have been proposed, such as enhancing information security through kryptogra phishing message authentication codes (MAC)[2], these methods are often limited to a single technical dimension and fail to fully consider the complexity of multi-dimensional threats. Secondly, Axel Wirth and Christopher Falkner point out that solving cybersecurity issues typically requires "stakeholder cooperation," but in reality, such cooperation often becomes superficial, resulting in "a lot of talking but little action"[3]. This indicates that the effectiveness of existing collaboration mechanisms is insufficient in practice. Additionally, the current cyber threat environment is becoming increasingly complex, with frequent security incidents, continuously emerging vulnerability information, and a large amount of IOC (Indicators of Compromise) data [4], making the management and analysis of threat intelligence more challenging. Although Li Aichao and Fu Qiyang emphasize the two major aspects of computer network security—physical security and logical security[5]—existing research still shows significant shortcomings in the implementation of logical security, particularly in the comprehensive assurance of information integrity, confidentiality, and availability. Finally, current cybersecurity threat intelligence management technologies tend to focus on in-depth analysis of a specific type of threat intelligence, lacking effective integration and deep mining of multiple intelligence sources[6]. This fragmented approach limits the overall utilization efficiency of threat intelligence, hindering the ability to comprehensively address the evolving and multi-faceted nature of modern cyber threats.

Given the severity of cybersecurity challenges, the study should pay attention to the current key issues. The ultimate goal is to assess the effectiveness and resilience of a country's cybersecurity system and provide data-driven recommendations and policies to enhance protection and future development.

First, the study analyzed the Global Cybersecurity Index (GCI), the Verizon Cybersecurity Database (VCDB), and the Cybersecurity Risk Index (CEI) to map cybercrime hotspots and cybersecurity assessments for each country.

Second, the study constructed a ridge regression model on the number of cybercrimes, taking into account economic level, population size, Internet penetration rate, education level, and the policy implementation environment for cybersecurity as the main influencing factors. The model verified that the frequency of cybercrime incidents was linearly related to these demographic indicators in each country.

Thirdly, based on the cybersecurity policy evaluation model, the study introduce the Difference in the Difference-in-Differences (DID) model and propose a reasonable assumption regarding the timing of policy implementation and actual conditions to quantify policy effectiveness. The study categorize policies into five major categories and discuss them in the context of countries at different levels of development. Finally, the study analyzed policy effectiveness by comparing model predictions with actual outcomes.

Otherwise, the results derived from models reveal the diverse impacts on achieving global cybersecurity health and sustainability. The study conclude with an analysis and evaluation of the strengths and weaknesses of the model implementation.

2 DATA SELECTION AND ANALYSIS ON GLOBAL GCI

2.1 Data Selection and Analysis

The study gathered GCI-related score data, VCBD Website data, and additional information about current and historical cybercrimes to construct pertinent datasets for assessing policy success. Furthermore, the research gathered several national demographic attributes of countries globally, including population size and GDP, for subsequent analysis. To guarantee the thoroughness and credibility of the data, the research designated the following The websites as sources, as shown in Table 1.

Table 1 Data Sources

Data Item	Source
GDP	World Bank
Population	World Bank
Global Network Coverage	World Economic Forum
Primary School Completion Rate	World Bank
GCI (Global Cybersecurity Index)	ITU (International Telecommunication Union)
VCDB Index	VERIS
Global Crime Prosecution Rate	United Nations Office on Drugs and Crime, IRS, etc.

2.2 Data Processing and Visualization

The accessibility of data is essential, as inaccurate or erroneous information might hinder a precise evaluation of overall equity.

Consequently, the continuity and authenticity of the data must be guaranteed. Nonetheless, data inadequacies frequently result from inadequate disclosure by countries. The study employs many ways to guarantee data integrity, including regression analysis and averaging techniques.

These approaches preserve data integrity, which is crucial for precise and dependable analysis. In certain models, other data processing approaches will be employed.

Simultaneously, the study has employed visualization processing techniques to facilitate data analysis.

2.2.1 Cybersecurity index assessment

Recognizing cybersecurity as a global concern, nations worldwide have allocated specific efforts in this domain. The International Telecommunication Union (ITU) has evaluated the cybersecurity index of several nations based on five criteria: legal, technological, organizational, capacity building, and collaboration, culminating in the Global Cybersecurity Index (GCI) score for each nation. By aggregating the GCI scores of 193 nations, the study has developed a GCI score level map (Figure 1). The map indicates that nations with elevated security standards are predominantly located in Europe and the Americas, whereas countries in Africa, Asia, and other areas exhibit lower cybersecurity scores. Furthermore, it has been determined that underdeveloped countries exhibit lower cybersecurity index scores compared to both developed and developing nations, whereas developed countries possess greater cybersecurity index levels than their developing counterparts.

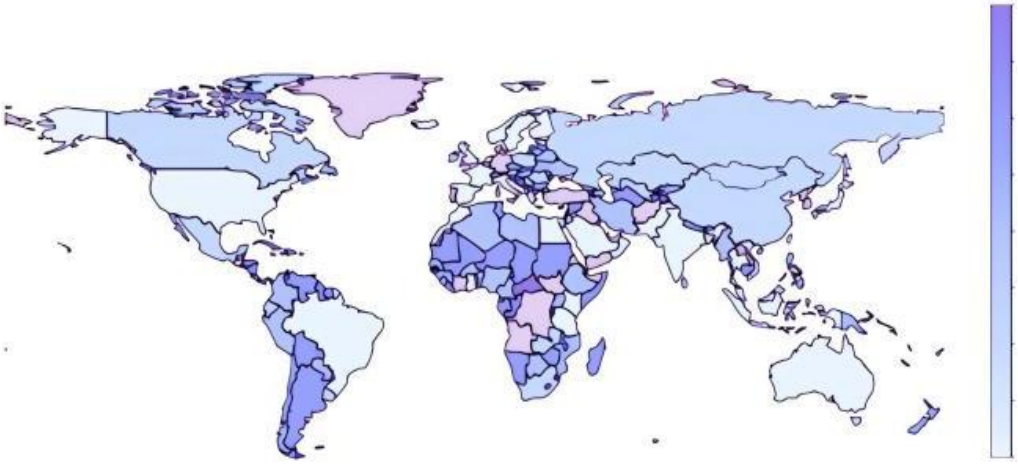

Figure 1 GCI Score Level Map
Source: VERIS Community Database (VCDB)

2.2.2 Crime volume analysis

Cybercrime is a highly significant criminal issue in todays society, especially with the rapid advancement of computer technology and the widespread adoption of the Internet.

The type and volume of cybercrime are on the rise. By collecting data on the number of cybercrime cases from 140 countries, the study has created a global heatmap of cybercrime volume (Figure 2) to illustrate the distribution of cybercrime cases. The heatmap reveals that developed countries have a significantly higher absolute number of cybercrime cases compared to developing countries, with the United States experiencing a far greater number of cybercrime incidents than other nations.

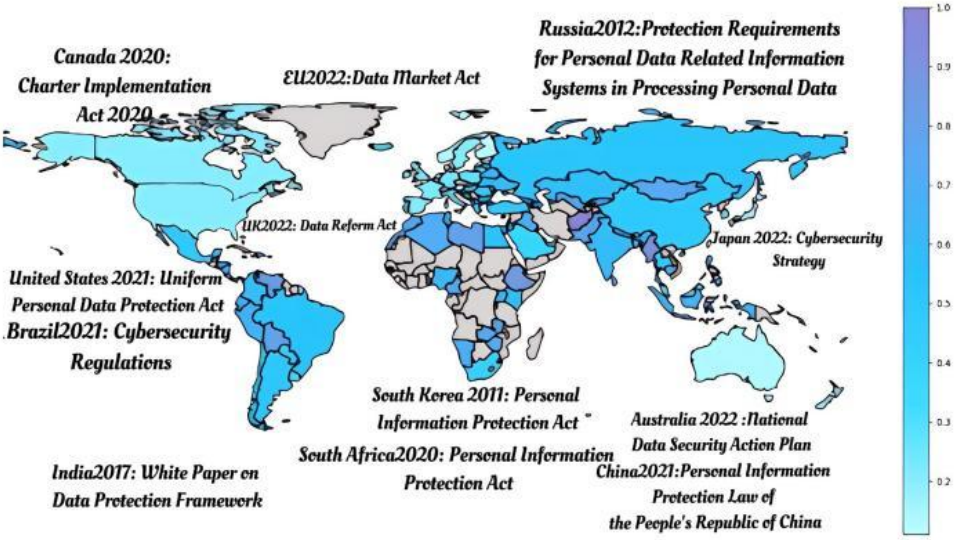

Figure 2 National Crime Statistics and some Policies
Source: CrimeMapping.com

2.2.3 Legal success rate analysis

The prosecution rate of cybercrime is an excellent indicator of a countrys cybersecurity strength. By collecting data on the number of cybercrime cases prosecuted in various countries and combining it with the overall number of cybercrime cases in each country, the research has created a global map of cybercrime prosecution rates (Figure 3). On the map, it can be observed that the prosecution rate for cybercrime in the European and American regions is significantly higher than that in the Asian and African regions.

Additionally, developed countries generally have higher prosecution rates for criminal cases than developing countries. However, some developing countries also have relatively high prosecution rates for criminal cases.

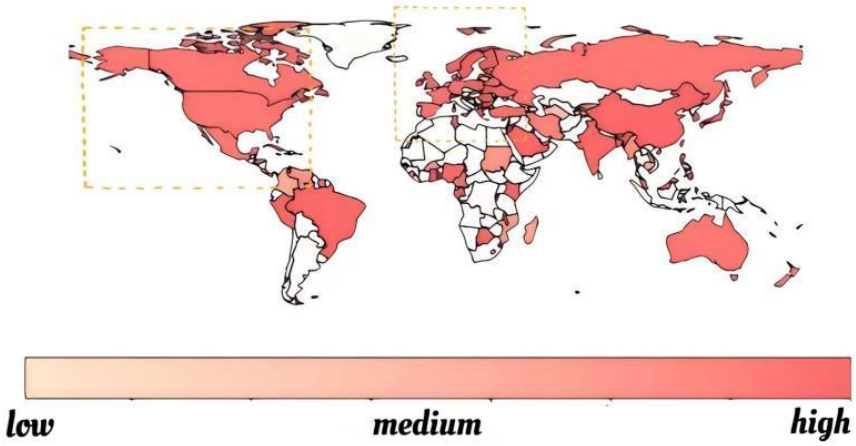

Figure 3 National Crime Prosecution Rate
Source: CrimeMapping.com

2.3 Policy Data Analysis

National policies serve as the principal mechanism for improving a nation's cybersecurity index. The study picked eleven nations based on their national development levels, gathered and assessed their cybersecurity policies, and classified them according to the five characteristics outlined by the Global Cybersecurity Index (GCI). The resultant policy classification chart (Figure 4-5) indicates that policies in industrialized, developing, and underdeveloped nations predominantly emphasize the legal dimension. Moreover, wealthy nations exhibit a wide array of policies across all dimensions, including the legal aspect, whereas emerging and undeveloped countries possess comparatively fewer policies in the other dimensions.

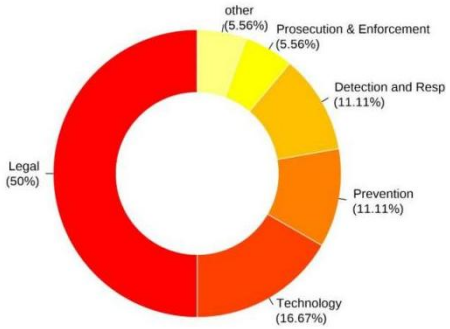

Figure 4 Distribution Ratio of Policy Types in Low Network Security Countries

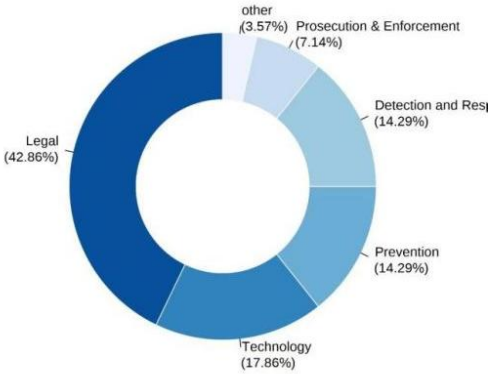

Figure 5 Distribution Ratio of Policy Types in High Network Security Countries

3 EVALUATION SYSTEM AND MODEL

To comprehensively analyze and predict the factors influencing the prevalence of cybercrime across different nations, the study established the Multi-Factor Regression Assessment Model (MRAM). Through this model, the study defined a mathematical relationship to quantify cybercrime levels C. The study considered five pivotal dimensions: GDP per capita, Population, Secure internet servers, Policy effectiveness, and Education level, which together serve as the key independent variables in the framework.
The model coefficients represent the magnitude and direction of each factor's contribution to cybercrime, which will be interpreted in subsequent sections.

3.1 Main Factors

To conduct a comprehensive evaluation of the cybersecurity landscape, it is essential to measure its robustness and adaptability. Similar to the definition of system health, the robustness of cybersecurity refers to its ability to effectively counter threats and adapt to the ever-changing challenges in the digital domain. For a resilient cybersecurity system model, it is not only necessary to identify cybercrime factors based on national development conditions but also to cover potential cybersecurity issues within the country. This study divides the task of data transmission into multiple transmission units Each transmission unit models the network condition based on an autoregressive model, predicting the required deduplication processing time for the next transmission unit and the available bandwidth during this period[7]. Based on the above definitions, the research has identified five key factors that measure the cybersecurity system, which will be detailed below:
(1) GDP per capita
The GDP per capita factor measures the likelihood of criminal groups targeting citizens of a country and is one of the most important indicators. On the one hand, a higher level of economic development usually means better social welfare and more employment opportunities, which may reduce the crime rate. On the other hand, economic growth can also lead to an increase in the wealth gap, which may increase certain types of crime rates. At the same time, criminal groups are more likely to target wealthier individuals to obtain higher illegal profits.
(2) Population
The population factor measures the potential risk a country faces from cybersecurity threats. The larger the population, the more Internet users there are, and the more targets there are for cyberattacks. This factor is measured by the population size, reflecting the pressure on cybersecurity in a country.
(3) Internet Penetration Rate
The number of secure Internet servers is a measure of a country's cybersecurity infrastructure. A higher number of secure Internet servers indicates a stronger capability for cyber defense. This factor is measured by the quantity of secure Internet servers, reflecting a country's investment and capability in cybersecurity technology.
(4) Education level
The education level factor measures a country's investment and effectiveness in cybersecurity education. A higher education level means more professional talent and stronger cybersecurity awareness. This factor is measured by indicators such as the number of graduates in cybersecurity-related fields and the prevalence of cybersecurity training.
(5) Policy effectiveness
The policy effectiveness factor measures the implementation results of a country's cybersecurity policies. Effective policies can significantly reduce the rate of cybercrime and enhance the level of cybersecurity. This factor is measured by indicators such as the enforcement of cybersecurity laws and the frequency of policy updates.

3.2 Evaluation Model

The study assumes that the number of cybercrimes (C_i) is influenced by the variables mentioned . And the regression model is expressed as:

$$C_i = \beta_0 + \beta_1 P_i + \beta_2 N_i + \beta_3 S_i + \beta_4 E_i + \beta_5 O_i + \epsilon_i \tag{1}$$

P_i represents GDP per capita, which indicates the level of economic development; N_i represents population size, which indicates the potential scale of internet users; S_i represents the number of secure internet servers, reflecting the strength of network security infrastructure; E_i represents education level, measuring public awareness and capacity in cybersecurity; O_i represents policy effectiveness, which scores the country's policy conditions in global cybersecurity efforts; β_0 is the intercept, representing the baseline cybercrime level when all variables are zero; $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$ are the regression coefficients, indicating the influence of each variable on the cybercrime level; and ϵ_i is the error term, capturing unexplained random factors affecting cybercrime. The letters in the following equation represent the same meanings.
The Residual Sum of Squares (RSS) is a measure of the discrepancy between the observed values and the values predicted by a regression model. In the context of the given problem, the RSS is given by the formula:

$$RSS = \sum_{i=1}^{n} \left(C_i - \hat{C}_i\right)^2 \tag{2}$$

The Residual Sum of Squares (RSS) is a measure of the discrepancy between the observed values and the values predicted by a regression model. In the context of the given problem, the RSS is given by the formula:

$$\hat{C}_i = \beta_0 + \beta_1 P_l + \beta_2 N_i + \beta_3 S_i + \beta_4 E_i + \beta_5 O_i \tag{3}$$

The Ordinary Least Squares solution:

$$\beta = (X^{\top} X)^{-1} X^{\top} Y \tag{4}$$

The study used VCDB statistics to draw a global cybercrime heat map, selected typical countries, and drew a line chart of cybercrime changes each year. The study also selected the United States and Australia and marked the laws enacted by these two countries where the line chart showed significant changes.
The results of calculations are presented in Table 2:

Table 2 Regression Results

Variable	Coefficient	Std. Error	t-Statistic	P-Value
Constant	256. 3456	56. 156	11. 1345	0. 074
GDP per capita	0. 0321	0. 011	2. 5634	0. 421
Population	0. 0452	0. 015	3. 1289	0. 417
Internet Penetration Rate	0. 0234	0. 010	2. 3487	0. 229
Education level	-2. 1234	0. 021	-12. 3489	0. 251
policy effectiveness	-4. 587	0. 019	-6. 3451	0. 135

The correlation of parameters in the formula is shown in Figure 6:

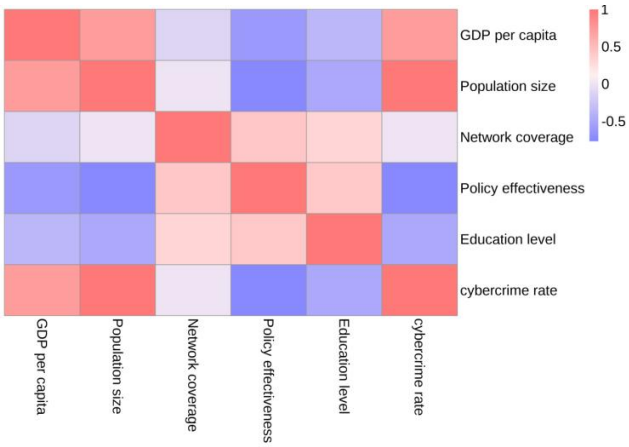

Figure 6 Objective Impact Indicators of Various Indicators

Light colors indicate lower correlation, and dark colors represent higher correlation.
The correlation between parameters cannot be ignored, as can be seen from the figure. Therefore, it is necessary to improve the model on this basis.

3.3 Improved Model

Incomplete data is stored in complex distributed networks [8-9], involving the insertion, deletion, updating, and reading of data, making it prone to redundancy, anomalies, or missing data [10]. To make the regression coefficients more stable, reduce the impact of multicollinearity, and maintain the predictive power of the model, the study calculates the Variance Inflation Factor(VIF) for each variable to evaluate potential multicollinearity issues:

$$VIF(N_i) = \frac{1}{1 - R_j^2} \tag{5}$$

In this equation, R_j^2 is the R^2 value obtained by regressing N_i on all other predictor variables.
To address this, the study turns to the Ridge Regression model[10]. The basic equation of the Ridge Regression model is:

$$\hat{\beta} = \underset{\beta}{argmin} \left(\sum_{i=1}^{n} \left(y_i - \beta_0 - \sum_{j=1}^{p} \beta_j X_{ij} \right)^2 + k \sum_{j=1}^{p} \beta_j^2 \right) \tag{6}$$

k is the Ridge Regression parameter used for regularization to penalize excessively large regression coefficients.

The results of calculations are presented in Table 3 :

Table 3 Multiple Linear Regression Results

Variable	B.	S. E.	Beta	t	P>|t|	VIF
Constant	277. 36	0. 12	------	19. 90	0. 087	------
GDP per capita	1. 22	0. 15	0. 42	3. 15	0. 035	1. 25
Population	0. 54	0. 12	0. 32	3. 76	0. 037	1. 20
Internet Penetratio--n Rate	2. 55	0. 20	0. 56	2. 55	0. 026	1. 30
Education level	-1. 46	0. 18	-0. 38	-11. 33	0. 046	1. 40
policy effectiveness	-0. 45	0. 10	-0. 15	-5. 08	0. 041	1. 1

The regression equation the study calculated is:

$$y = 277.36 + 1.22x_1 + 0.54x_2 + 2.55x_3\text{-}1.46x_4\text{-}0.45x_5 \tag{7}$$

The study has collected the data as a dataset from which the study randomly selected four countries and predicted the y-values, and the fitting results are shown in Figure 7. This shows that the study is relatively feasible within a certain error allowance.

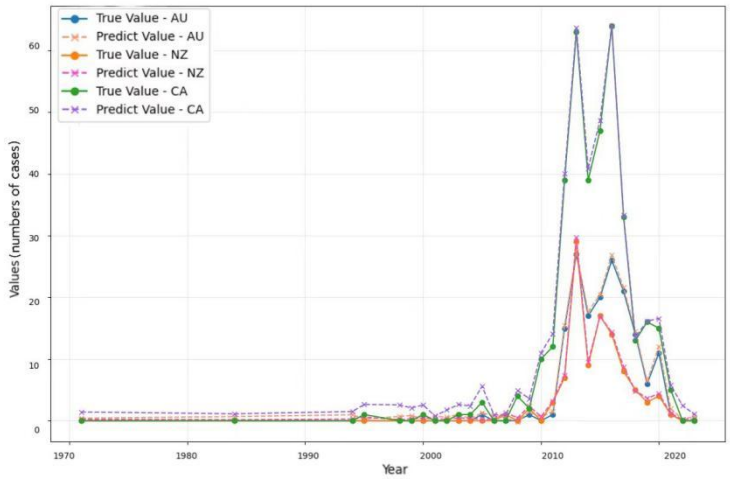

Figure 7 Testing results of regression model

3.4 Sensitivity Analysis

The study calculated the sensitivity of each explanatory variable to the dependent variable using the following formula:

$$S_i(Y,x_i) = \frac{1}{n}\frac{\partial x_t}{\partial y_i}\cdot\frac{x_i}{y_t}, i = 1,2,3,4,5 \tag{8}$$

In the previous part, the Ridge Regression Model was constructed and the proximity between the countries and the optimal solution was obtained. Then, the study conducted sensitivity analysis on the Ridge Regression Model respectively. The specific methods are as follows: Select Central African Republic as the research object, keep the weights of each indicator fixed, and gradually increase the value of each indicator individually, and observe the changes in the degree of proximity (assessment score) to the optimal solution. The faster the evaluation score changes with the index value, the higher the sensitivity of the model. Conversely, the slower the evaluation score changes with the index value, the lower the sensitivity of the model. Figure 8 respectively represents the sensitivity of indicators in the selected single country and the Average prediction sensitivity of indicators.

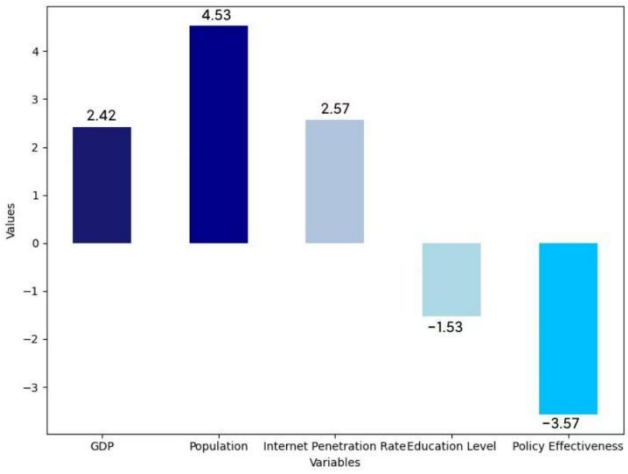

Figure 8 Average Prediction Sensitivity

According to the above results, it can be found that population size, education penetration rate, and the policy implementation environment have a greater impact on the number of cybercrimes. Therefore, since the member states of the International Telecommunication Union hope to build network security together, they must promulgate policies to try their best to improve domestic education penetration rates, maintain a stable domestic political environment, and reduce the number of cybercrimes. At present, some countries have not paid enough attention to related aspects, so the study strongly recommended that member states pay more attention to issues such as education that accompany population growth.

4 EVALUATION OF NATIONAL POLICIES

The study aimed to analyze the effectiveness of the cybersecurity policy. Since the factors influencing cybersecurity may be subject to sample selection limitations or difficulties in controlling other factors, which could lead to the possibility of overestimating the estimates, the study adopted the DID model proposed by Ashenfelter and Card (1985), originally used to study whether participation in government vocational training programs could increase participants' earnings. The study divided the sample into an experimental group and a control group, and subtracted the pre-policy differences of the control group from the differences between the experimental and control groups. The predicted data obtained through the aforementioned ridge regression model were used to assess the differences between the two groups before and after the policy, in order to analyze the true policy effect.

4.1The Foundation of Model

To clarify whether the policy had an impact on cybercrime rates, the study constructed an experimental group (regions affected by the cybersecurity policy) and a control group (regions not affected by the policy), and compared the differences in cybercrime rates before and after the policy implementation. This approach allowed us to identify the true impact of the policy on cybercrime rates. By comparing the changes in cybercrime rates between the experimental and control groups, the study could more accurately evaluate whether the cybersecurity policy achieved its intended effect, and avoid bias caused by unobserved confounding factors (such as regional economic development levels, law enforcement efforts, etc.).

The model used for this analysis is:

$$Y_{it} = \alpha + \beta_1 Time_t + \beta_2 AREA_i + \beta_{12}(Time_t \times AREA_i) + \epsilon_{it} \quad (9)$$

Y_{it} represents the number of cybercrimes in region i at time t ; α is the constant term; β_1 is the coefficient of the time dummy variable, representing the overall before and after the policy implementation; β_2 is the coefficient of the region dummy variable, representing the baseline differences across regions; β_{12} is the interaction effect coefficient, representing the differential impact of the policy across regions; $Time_t$ is the time dummy variable, which is 0 before the policy implementation and 1 after; $AREA_i$ is the region dummy variable, indicating whether the region is affected by the policy (1 if affected, 0 otherwise); and ϵ_{it} is the error term.

In the preliminary data processing, the study first categorized national policies into five types based on the standards of the Global Cybersecurity Index (GCI). In the policy classification, the study assumed that a type of policy only affects the corresponding policy indicator. Additionally, for policies issued, the study assumed that their impact on cybersecurity gradually increases over five years and remains constant after five years. By making these assumptions, the study simplified the DID model to make it more convenient and efficient for practical application. The principle of the DID model is shown in Figure 9.

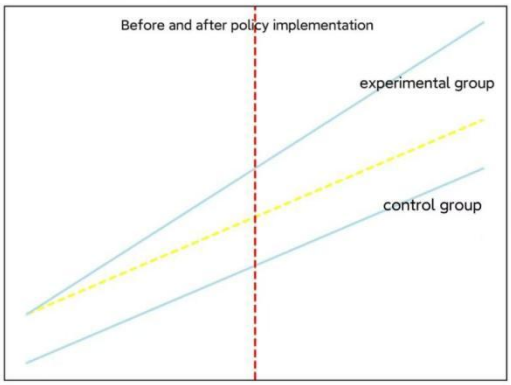

Figure 9 DID Model Principle Diagram

Due to the complexity of cybersecurity issues, in order to demonstrate predicted outcomes in reality, it is necessary to create a virtual parallel world to study the impact of policies. Therefore, the study adopted the DID model to evaluate the policies of various countries. Simply put, the DID model assumes the existence of a virtually conceived parallel world, where the study identify a region similar to the policy implementation area but without the policy in place, and then compare the differences between the two regions to assess the policy's effectiveness.

The study conducted benchmark regressions on the model through parallel trend tests, placebo tests, and robustness tests: Parallel Trend Test: By adding interaction terms to the regression model, the study examined whether the trends between the treatment group and the control group were significantly different before the policy intervention. After conducting three sets of interaction tests, the study found that the trends of the treatment and control groups were similar before the intervention, indicating that the parallel trend assumption holds.

Placebo Test: The study introduced a fake policy intervention period (placebo period) in the regression analysis the study chose a time point unrelated to the actual intervention period for regression. The regression results from the placebo period were insignificant, leading us to conclude that the actual intervention effects are reliable. Robustness Test: The study performed benchmark regressions using different error structures, specifically clustered standard errors, to examine the overall effects of the policy intervention.

4.2 Parallel Trends Analysis

This study implements a parallel trends test to verify the accuracy of the data. An interaction term of time dummy variables and group dummy variables is developed to elucidate the disparities between the model-generated parallel data and actual data before the policy execution, illustrating the variations between the treatment and control groups across several years.

Pertinent variables were incorporated into the model for evaluation. The results from the parallel trends test graph indicate that the coefficients for Before2 and Before1 lack statistical significance, whereas the coefficients for After1 and After2 are significant ($p = 0.095 < 0.1$), demonstrating a positive impact on the digital economy value index in the respective countries following the implementation of the cybersecurity policy. The coefficient for After2 is 0, indicating that the coefficients prior to the policy implementation varied about 0, whereas the coefficients after the policy implementation tend toward a positive value.

This indicates that the treatment and control groups display similar trends, thus fulfilling the necessary conditions for the use of the DID model, which adheres to the parallel trends assumption.

4.3 Application of Models

The study selected the policies of eleven typical countries, where the timing of policy impact on the DID model varied, and evaluated the policies as listed in the Table 4:

Table 4 Partial National Policy Rating

Effectiveness Rating	Law Name
1	Internet Governance Policy (2015)
	ICT Strategy and Cybersecurity Development Strategy (2016)
	Cybersecurity Education and Public Awareness Program (2018)
	Cybersecurity Education and Awareness Program (2018)
\	Cybersecurity Law (2014)
	Data Protection Law (2019)
2	Cybersecurity Law (2015)
	Personal Data Protection Law (2017)
	Cybercrime Law (2011)
	Information Technology Law (2015)

2	2 Anti-Terrorism Law (Revised 2005) Cybercrime Law (2017) Data Protection Law (2017) Electronic Transactions Act (2008) Data Protection Law (2012) Information Technology Law (2013) Data Protection Law (2020)
3	Cybersecurity Law (2017) Data Security Law (2021) Personal Information Protection Law (2021) Cybersecurity Level Protection System (Class 2. 0, 2019) Critical Information Infrastructure Protection Regulations (2021) Computer Fraud and Abuse Act (CFAA, 1986) 3 Cybersecurity Law (2018) U. S. Cybersecurity Strategy (2018) Anti-Terrorism Act (2001) Cybersecurity Act (2016) Data Protection Act (2018) Cybersecurity Strategy (2016) Emergency Response Mechanism (UK CERT, 2001)

In the Table 4, observing the policies in the table, those rated 3—such as Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021)—demonstrate a particularly robust and comprehensive approach to constructing a cybersecurity framework. These policies not only secure critical infrastructure through clear legal provisions, but they also exhibit powerful enforcement capabilities that address emerging cyber threats and combat cybercrime effectively, forming a wide-ranging security barrier. At the same time, the policies rated 2, including Cybersecurity Law (2014), Data Protection Law (2019), and Electronic Transactions Act (2008), contribute significantly to enhancing overall cybersecurity. Although there are some shortcomings in terms of implementation details or inter-sector coordination, these measures still manage to fortify security defenses and progressively refine the regulatory framework. In contrast, the policies rated 1—such as Internet Governance Policy (2015) and Cybersecurity Education and Public Awareness Program (2018)—primarily focus on providing strategic guidance and establishing an initial framework. While these initiatives lay an important foundation for future, more stringent measures, their impact remains relatively limited in the short term due to a lack of direct and robust enforcement mechanisms.

From the table, the study observed that the policy implementation efficiency in less developed countries is mostly 1, while developed countries have more policies with efficiency ratings of 2 and 3. In the policy types of less developed countries, legal measures, which focus on post-crime sanctions, are the most common. Due to the lower cybersecurity literacy in less developed countries, the crime reporting rate is lower compared to developed countries.

4.4 Solution and Result

For developed countries, such as the United States, high levels of internet coverage result in higher cybersecurity literacy among citizens. The policy effect diagram of the United States is shown in Figure 10. Although the proportion of policies and laws formulated is the highest, they demonstrate a comprehensive approach when compared to underdeveloped and developing countries. As a result, they have established a complete system for governing cybercrime.

The study has also drawn on this system for model analysis, which has helped us formulate effective policies:Due to the generally low cybersecurity literacy in underdeveloped countries, cybersecurity issues are more prominent in these countries. In these nations, the public and government agencies have relatively weak understanding and response capabilities concerning cybercrime, which leads to a lower rate of cybercrime reporting. This phenomenon contrasts sharply with developed countries, which typically have higher cybersecurity awareness and more established reporting mechanisms.

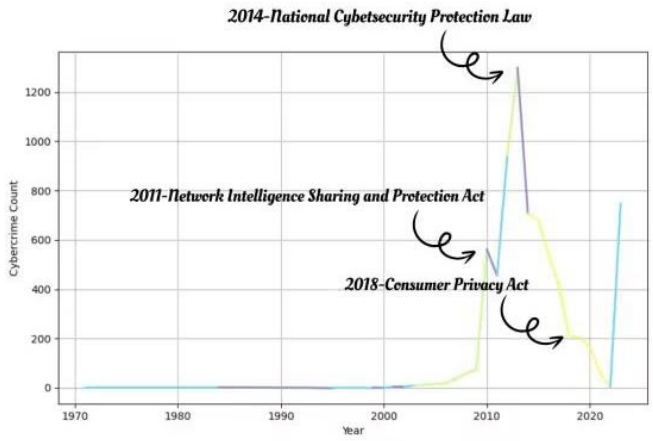

Figure 10 The Application of the Model in US

Based on this difference, when formulating cybersecurity policies, underdeveloped countries should avoid relying solely on legal measures to address cybercrime. While legal measures can play a role in regulation, relying only on the law is insufficient to effectively improve cybersecurity, particularly when cybersecurity literacy is low. Meanwhile, international cooperation shows significant potential for improving cybersecurity quality. By collaborating with developed countries, underdeveloped countries can gain technical support, share resources, and exchange experiences benefits that cannot be achieved by acting independently. Developed countries have accumulated rich experience and technical resources in the cybersecurity field, and their well-established cybersecurity frameworks, response mechanisms, and policy systems can provide valuable guidance for underdeveloped countries. Through enhanced cooperation with developed countries, underdeveloped countries can not only improve their cybersecurity defenses but also enhance their voice and participation in international cybersecurity governance.

Therefore, underdeveloped countries should regard international cooperation as a key component of cybersecurity policy formulation. They should actively engage in cooperation with developed countries and international organizations to address gaps in global cybersecurity challenges. Such cooperation will not only help underdeveloped countries compensate for their lack of technology and experience but also contribute to the improvement of the global cybersecurity environment, thus achieving global cogovernance and shared development in cybersecurity.

5 CONCLUSIONS

This study examines the effectiveness of cybersecurity policies and cybercrime, based on the GCI scoring mechanism. By collecting substantial data related to cybercrime, the study created heat maps depicting the number of cybercrime cases, GCI scores, and prosecution rates across countries. The analysis revealed that developed countries in Europe and the United States are the primary targets of cybercrime and are more likely to sanction such crimes. A ridge regression model was built to analyze the relationship between cybercrime cases and factors such as GDP, population size, internet penetration rate, education level, and policy implementation environment. The findings showed that population size is the most influential factor in determining the number of cybercrime cases. Additionally, a DID model was used to evaluate the effectiveness of cybersecurity policies, revealing that the most effective policy types vary across countries: international cooperation was most effective in less-developed countries, legislation in developing countries, and technological upgrades in developed countries.

The limitations of this study lie in the fact that, due to time constraints, more relevant data could not be collected, limiting the depth of analysis of the model's variables. Furthermore, the model itself has inherent flaws that could lead to errors in assessing the actual situation, which may affect the precision and reliability of the study's results.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Wireless News. Billington CyberSecurity Summit to feature theme: Advancing cybersecurity's impact in age of heightened risk. 2023.
[2] Dirk Bierbaum. Smarte Synthese aus Cybersecurity und Funktionssicherheit. ATZ elektronik, 2022, 4(4): 341.
[3] Axel Wirth, Christopher Falkner. Cyberinsights : Cybersecurity as a Team Sport. Biomedical Instrumentation & Technology, 2020, 54(1): 64-67.
[4] Xia Ru. A review of research on foreign cyber threat intelligence. Modern Information Technology, 2024, 8(01): 189-192+198.

[5] Li Aichao, Fu Qiyang. Analysis of Computer Network Security Issues and Countermeasures. Engineering Technology: Abstract Edition, 2022(12).
[6] Zhao Xiaolin, Zeng Chonghan, Xue Jingfeng, et al. Research on Multidimensional Network Security Measurement Model Based on TOPSIS. Journal of Beijing Institute of Technology, 2021, 41(3): 311-321.
[7] Ye Pengdi, Yao Wenbin, Li Xiaoyong. Design of network data deduplication method based on autoregressive model. Journal of Beijing University of Posts and Telecommunications, 2014(4): 5.
[8] Yao Yingle, Li Jian, Sun Bin. Simulation of Interpolation Algorithm for Fitting Incomplete Data Missing Sequence. Computer Simulation, 2023, 40(1): 523-527.
[9] Ai Zhiwei, Leng Juelin, Xia Fang, et al. A method for reducing large-scale structured data with controllable accuracy. Journal of Computer Aided Design and Graphics, 2021, 33(12): 1795-1802.
[10] Guan Lijing, He Jiefan, Zhang Liyong, et al. Missing Value Imputation Method Based on Single Output Sub Network with Iterative Learning. Journal of Dalian University of Technology, 2022, 62(4): 427-432.