Cybersecurity Assessment Based on Dynamic Panel Data Modeling

Yahui Wei[1,*], Junyu Liu[1] and Sihan Cheng[1]

[1]College of Information Science, Beijing Language and Culture University, Beijing, China

*Corresponding author: 202411680885@blcu.edu.cn

Abstract. The purpose of this paper is to assess the state of cybersecurity by constructing a dynamic panel data model. First, the study analyzes the characteristics of the global distribution of cybercrime and finds that its concentration area and related factors have a significant impact on its pattern, and that the success rate of cybercrime is related to many aspects. Second, given that cybercrime is affected by the dynamics of multiple factors, the study introduces hidden indicators such as law and technology, and after processing missing values and standardized data, the study combines the dynamic panel data model with the SIR infectious disease model to assess the effect of policies, and the results show that capacity building has the best effect on reducing cybercrime. Finally, the accuracy of the model was verified by sensitivity analysis. This study provides a theoretical basis for countries to formulate cybercrime prevention and control policies.

Keywords: Cybersecurity; dynamic panel data model; SIR infectious disease model.

1. Introduction

This paper centers on constructing a dynamic panel data model[1] to assess the status of cyber security to carry out in-depth research. Firstly, it is clear that cybercrime presents a complex distribution situation in the global scope[2], and multiple factors have a profound impact on its pattern. Second, the formation mechanism of cybercrime is extremely complex[3], affected by the dynamic interaction of legal environment, technology level, organizational structure and other factors, the study introduces a dynamic panel data model enhanced by the SIR infectious disease model[4] to assess the policy effect. Finally, the model accuracy is evaluated to provide strong support for subsequent policy formulation. This study aims to break through the existing limitations[5] and provide a solid theoretical cornerstone for cybersecurity policy formulation in various countries[6].

2. Analysis of Distribution Characteristics and Influencing Factors

2.1. Global Distribution Characteristics of Cybercrime

Globally, most cybercrime incidents occur in North America, Central and Eastern Europe, East Asia, India and Eastern Australia. Countries/regions such as Russia, Ukraine and Romania rank high in the cybercrime index. The United States is one of the main sources of cybercrime in the Americas, where cybercrime activity is highly sophisticated and organized. Nigeria in Africa and China and India in Asia also feature prominently in cybercrime. As can be seen, cybercrime is not universally distributed. Certain countries/regions are cybercrime hubs, while many others are not seriously associated with cybercrime.

Fig. 1 shows the trend in the number of crimes in the world's major countries from 2017 to 2023. Focusing on data around 2019, it can be seen that the number of cybercrimes increases significantly globally due to COVID-19. Though the epidemic likewise had a knock-on effect on administrative efficiency and therefore may have led to a slight decrease in the number of cybercrimes recorded by some governments. It is important to note that the crime data for India, which is derived from the number of cases registered by the government, may be lower than the actual situation, but is a more reliable indication of trends and is therefore used.

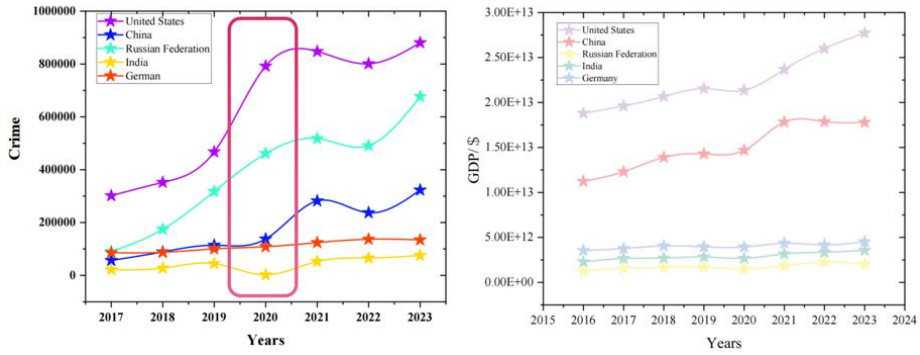

Fig. 1 Trends in crime volumes and GDP in key countries, 2017-2023

Since 2022, the Russia-Ukraine war has significantly changed the cybercrime landscape. Initially, cyberattack strategies on both sides shifted from massively destructive attacks to more targeted espionage focused on military and critical infrastructure targets. Attack tactics have also become more sophisticated, including DDoS attacks and data wiping attacks.

2.2. Analysis of National Cybersecurity Policies

Fig. 2 shows that globally, the success rate of cybercrime is closely tied to economic development and the robustness of a country's legal system. For example, countries/regions with underdeveloped economies and weak legal frameworks, such as Afghanistan and Myanmar, have relatively high cybercrime success rates. In Afghanistan, the cybercrime reporting rate is only around 15%, while the success rate is nearly 90%. This suggests that the lack of effective cybercrime monitoring and enforcement mechanisms in those countries/regions makes it easier for criminals to successfully carry out cyberattacks.

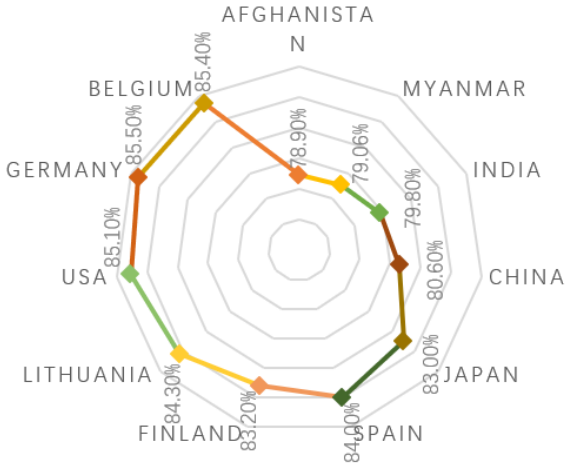

Fig. 2 Cybercrimes reported rate

In contrast, developed countries such as Belgium and Finland, which have more advanced legal systems and stronger economies, have much lower success rates in cybercrime. In Finland, the success rate of cybercrimes is below 25%. A similar trend was observed in Belgium, where more than 70 per cent of cybercrime cases were successfully prosecuted.

Further analysis showed a strong positive correlation between reporting and prosecution rates. Prosecution rates for cybercrime tend to be higher in countries/regions with well-established reporting mechanisms. In Belgium, the cybercrime reporting rate is as high as 85%, with nearly 80% of cases successfully reaching the judicial process. On the other hand, in countries such as Afghanistan and Myanmar, prosecution rates remain low due to inadequate reporting mechanisms and insufficient resources.

Cybercrime success is intricately linked to differences in technological capacity, law enforcement strength and public engagement in different countries/regions. Countries with advanced economies and strong legal systems are more effective in preventing and combating cybercrime, while countries

with weak economic and legal infrastructures face higher cybercrime success rates and lower prosecution rates.

2.3. Relationship Between Cybercrime and Demographics

Over the past seven years, there has been a general upward trend in the number of cybercrimes in major countries around the world. Comparison with population and GDP trends shows a positive correlation between the number of cybercrimes and these two factors. As shown in Fig. 3, in the United States, for example, the number of cybercrimes has increased as GDP has grown. In addition, there is a positive correlation between the number of cybercrimes and population size. More populated areas usually have more Internet users, which expands the range of potential targets for cybercriminals.

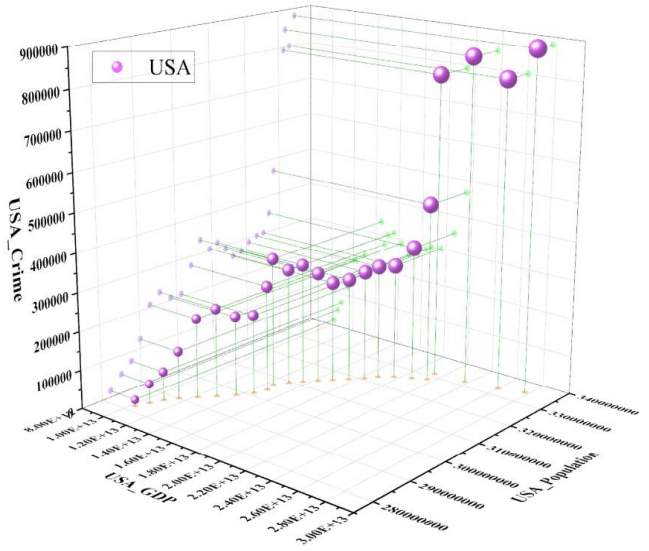

Fig. 3 U.S. GDP, population, and cybercrime volume relationships

3. Identification of Policy Effectiveness Based on Dynamic Panel Data Modeling

Cybercrime is affected by the interaction of multiple indicators, such as legal, technological, organizational, capacity-building and international cooperation, and these indicators change dynamically over time. Due to political, economic and cultural differences, different countries have different coping strategies and realities. Given the interplay of multiple indicators, temporal order and country heterogeneity in this complex system, the study uses a dynamic panel data model to construct a policy effectiveness identification model. The model can fully take into account the dynamic relationship of individual indicators across countries and points in time, effectively capture individual (i.e., different countries) heterogeneity, and maximize the information contained in the data without relying on too many external assumptions, so as to accurately assess the impact of policies on the number of cybercrimes.... Determine effective cybercrime response policies and then provide theoretical support for countries to formulate prevention and control policies.

(1) Dealing with Missing Data Values

The study obtained five implicit indicators for five years: 2014, 2017, 2018, 2020 and 2024.

Legal measures: this indicator measures the status of national laws and regulations to combat cybercrime and maintain cybersecurity. It includes prohibitions or minimum regulatory requirements for specific crimes, as well as definitions of rights, responsibilities and protections.

Technical measures: Without adequate technical measures and capabilities to detect and respond to incidents, Member States and their respective entities remain vulnerable to cyber risks that could undermine the advantages of digital technologies.

Organizational measures: Organizational measures are necessary for the proper implementation of national initiatives. Member States need to develop comprehensive plans with broad strategic objectives for implementation, delivery and measurement. Structures such as national agencies need to be in place to implement cybersecurity strategies and evaluate the success or failure of programs.

Capacity development: Capacity development spans legal, technical and organizational measures. Understanding cybersecurity technologies, risks, and impacts helps develop better legislation, better policies, better strategies, and better organizational roles and responsibilities. Capacity development includes the development of knowledge and skills of the base population, professionals working in cybersecurity, and experts in the field.

Collaboration: Collaboration enhances dialog and coordination to help create a more comprehensive field of cybersecurity applications. Cooperation can include joint initiatives, information sharing, training, and other activities that connect professionals, officials, and others seeking to improve cybersecurity.

These indicators provide an adequate and more objective picture of the extent to which countries are implementing policies in different areas and are introduced in this paper to calculate the effectiveness of policies in different areas.

The study planned to collect GCI intrinsic indicators from 2014 to 2024, but there were missing values in the data for that time period. After comprehensive consideration, quadratic spline interpolation was chosen to fill these missing values. The change of network security index over time should be relatively continuous and smooth in theory. The smooth function curve obtained by quadratic spline interpolation is consistent with the characteristics of the gradual change of the network security index over time and can reflect the potential trend of the data more realistically.

(2) Data Standardization

Because the total score of each index has significant differences between years, it is difficult to effectively compare and synthesize data from different years under the same dimension. For example, in 2014 and 2017, the total score of individual indicators was 1, while in 2020 and 2024, the total score of individual indicators was 20. Therefore, the raw data were standardized, and the total score of all single indicators was standardized to 100, which makes the data of different years comparable and lays a solid foundation for the subsequent model construction and statistical analysis. Fig. 4 below shows the comparison of GCI data (standardized) after the interpolation process.

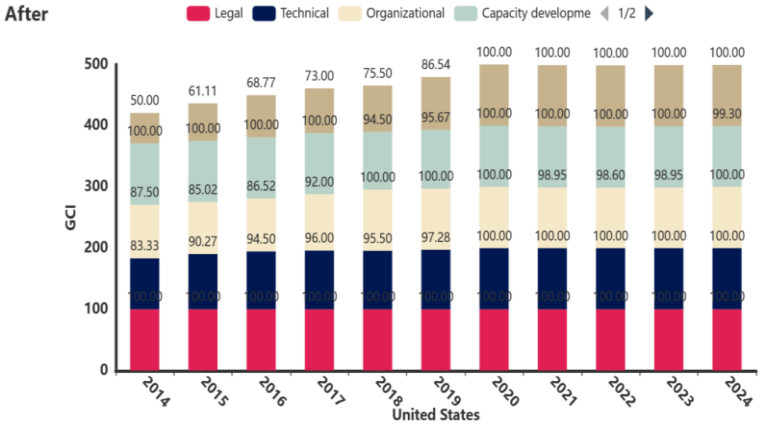

Fig. 4 Comparison of data after the quadratic spline interpolation process

3.1. Principle of Dynamic Panel Data Model (DPM)

The Dynamic Panel Data Model captures the heterogeneity of individuals (in this case, different countries/regions), the dynamics of relationships between variables, and time-series characteristics.

3.1.1 Modeling and Indicator Description

In order to take into account, the time-series nature of the data, the individual variability across countries, and the reality of the combined impact of multiple factors, and to exclude other irrelevant

but significant influences, this paper uses a combination of a dynamic panel data model and the SIR infectious disease model.

$$Crime_{\text{num } it} = \alpha + \rho \cdot Crime_{\text{num } i,t-1} + \sum_{j=1}^{6} \beta_j \cdot X_{jit} + \mu_i + \epsilon_{it} \quad (1)$$

The value of the solution is required to be:

Intercept (α reflects the base level of the crime).

Individual fixed effects μ_i (demonstrating the relative propensity of the country/region to be prone to cybercrime itself).

Coefficients of the lag term ρ (reflecting the natural rate of change in cybercrime).

CGI Coefficients each of the five indicators $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$. (describes the impact effect of the five indicators)

Other components:

Number of crimes in country i at time t $Crime_{\text{num } it}$.

Number of crimes in country i at lag time t $Crime_{\text{num } i,t-1}$.

Gross GDP coefficient β_6 (used to exclude the effect of economic development).

Random error term (in calculus) (ϵ_{it} denotes unexplained random fluctuations in the model).

3.1.2 Infectious Disease Model Fusion

In this paper, we consider the use of an SIR model to describe the spread of an epidemic. The output of this model (number of infections) is introduced as a new independent variable into the dynamic panel data model to exclude the effect of new crown epidemics on the cybercrime situation at a given time.

The infection rate is defined as:

$$I_t = \frac{I}{N} \quad (2)$$

Where I represent the number of infected individuals and N is the total population. This is then introduced into a dynamic panel data model:

$$Crime_{\text{num } it} = \alpha + \cdot \rho \cdot Crime_{\text{num } i,t-1} + \sum_{j=1}^{6} \beta_j \cdot X_{jit} + \gamma \cdot I_t + \mu_i + \epsilon_{it} \quad (3)$$

Where γ is the infection coefficient, indicating the degree of influence of the number of infected people on cybercrime.

3.2. Model Results

Table 1. Solving Result

Variable	Intercept	Lag Crime num	Legal	Technical	Organizational	Capacity development	Cooperation
Coefficient	78536.94	1.32	15464.99	-8301.78	8757.11	-21657.60	9111.54

As in table 1, final interceptions is about 80,000, the relative size of the propensity to commit cybercrime is more in the U.S. than in China, more in India, more in Germany, more in Russia, and more than in any other country, and the natural rate of growth of cybercrime is about 30% per year, and of the five metrics, capacity building has the best effect on reducing the number of cybercrimes, followed by technological upgrades, with cooperation and organization having less of an effect, and the soundness of the law likely to increase the number of cybercrimes recorded by the government by making it easier to identify and prosecute cybercrimes, thus increasing the number of cybercrimes recorded by the government.

4. Sensitivity Analysis

To ensure that the model accurately identifies the most effective indicators, this paper created simulation parameters and used the model to estimate parameter values based on the data generated. The study simulated crime data for 10 different countries from 2000 to 2019 under the same original parameters, a process that was repeated 20 times, generating a total of 100 sets of data.

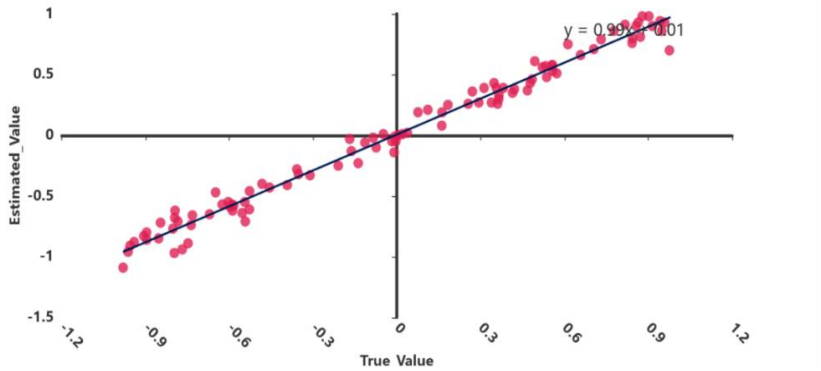

Fig. 5 Correlation analysis between raw data and calculation results

As shown in Fig. 5, based on the results of the correlation analysis, the model is able to accurately analyze the magnitude of the impact of the indicators, accurately determine whether there is a positive or negative correlation between the indicators, and successfully complete the task.

5. Conclusion

This paper uses dynamic panel data model to deeply analyze the situation related to cybercrime and provide scientific basis for global cybersecurity prevention and control. First, the distribution of global cybercrime shows obvious differences, which is influenced by social and economic development, major events and other factors, and is closely related to national security policies. Second, given the complexity of cybercrime, it is difficult to comprehensively analyze it by traditional research methods. This study introduces an innovative solution combining the dynamic panel data model and the SIR infectious disease model. The dynamic panel data model can capture the dynamic relationship of indicators in different countries and points in time, while the SIR infectious disease model can exclude the interference of new crown epidemics on the cybercrime situation, and the combination of the two can more accurately assess the impact of cybercrime-related factors. Finally, the analysis through this model combination provides a strong support for enhancing the comprehensive response capacity of global cybercrime and promotes the optimization and upgrading of cybersecurity prevention and control strategies.

References

[1] Hou L. Model estimation and selection for spatial dynamic panel data[D]. University of Science and Technology of China, 2024.DOI: 10.27517/d.cnki.gzkju.2024.000449.

[2] WU Hequn, WANG Qiang, ZHENG Zhiwan. Spatial Distribution Characteristics and Influencing Factors of the Place of Origin of Telecommunication Network Fraud Offenders[J]. Geography Research, 2023, 42(12):3219-3234.

[3] WANG Jing, LI Zheng, WANG Tao, et al. Spatial and temporal evolution and formation mechanism of child abduction and trafficking criminal activity network in China: an analysis based on successful cases of family search[J]. Journal of Zhejiang University (Science Edition),2024,51(01):64-75+89.

[4] YANG Hong, ZHANG Xiaoguang. Stochastic SIS infectious disease models on simple complex forms[J]. Journal of Mathematical Physics,2024,44(05):1392-1399.

[5] Wang Xiaolu. A review of research on China-ASEAN cooperative cybersecurity governance: progress, limitations and prospects[J]. Research on Indian Ocean Economies,2020, (05):136-152+156.DOI: 10.16717/j.cnki.53-1227/f.2020.05.007.

[6] ZHANG Y P, LU S W, LU M X, et al. A Comparative Study of Sino-US Cybersecurity Policies Based on the Three-Dimensional Framework of “Evolution-Tool-Theme” [J]. Journal of Intelligence, 2025, 44(02):124-135.