Cybersecurity Diagnosis Based on National Context

You Hao[1, a]

[1]School of Life Science, Nanjing University, Nanjing, China;

[a]2125153381yh@gmail.com

Abstract. With rapid internet advancement, strengthening cybersecurity is vital for national security. This study uses a Five-Dimensional K-means Clustering (FDKC), a Partition-based Spearman Correlation Analysis, and a TREND-enhanced AHP-EWM model to analyze cybercrime patterns and guide policy. First, five indicators—Crime Rate, Success Rate, Report Rate, Thwart Rate, and Prosecution Rate—were used in FDKC to group countries into five clusters. Results show that technologically advanced countries like the US and UK have the highest Crime Rates, while regions with weaker cybersecurity, such as Russia, the Middle East, and Africa, have higher Success Rates. Countries with strong cybersecurity frameworks, including the US, China, and Europe, show higher Report, Thwart, and Prosecution Rates. Second, integrating the Global Cybersecurity Index (GCI) and policy timelines, the Spearman model revealed that policy effectiveness depends on economic and technological context: less developed nations gain most from international cooperation, while developed countries benefit from stronger legislation and technical measures. Third, twelve demographic variables across Population Structure, Internet Access, Wealth, and Education were analyzed with the AHP-EWM model incorporating trend factors, confirming that moderately developed countries should focus on education to improve cybersecurity awareness and reduce cybercrime. Finally, sensitivity analysis confirmed the model's robustness and suitability for policy evaluation and strategic cybersecurity planning.

Keywords: Cybercrime Distribution; Cybersecurity Policy; K-means Clustering; Crime Development Index; AHP-EWM; Spearman Correlation.

1. Introduction

"There is no such thing as perfect security, only increasingly difficult security," as cybersecurity expert Eva Galperin aptly noted. In the digital age, the proliferation of internet usage and rapid technological advancements have significantly escalated the frequency, scale, and sophistication of cybercrime. This growing threat poses serious challenges not only to individual privacy and property rights but also to national political stability, economic development, and public trust. In response, governments worldwide have implemented a range of cybersecurity policies and strategies. However, the effectiveness of these measures varies substantially across countries, with some demonstrating commendable progress while others lag behind or exhibit inconsistent outcomes. This disparity highlights the pressing need for a robust and systematic evaluation framework capable of assessing policy effectiveness and uncovering structural patterns across different national contexts.

Cybercrime is a multifaceted phenomenon influenced by a complex interplay of technological, socioeconomic, and institutional factors. Understanding the dynamics of cybercrime thus requires a holistic perspective that accounts for variations in technological maturity, educational attainment, economic conditions, and policy environments. To address this need, the present study investigates three interrelated research questions: (1) Which countries exhibit notably high cybercrime rates, and how are they distributed globally? (2) How effective are different types of cybersecurity policies over time in reducing cybercrime? (3) To what extent do national demographic characteristics shape cybercrime trends and outcomes?

To identify countries with distinct cybercrime profiles, we begin by constructing five key indicators based on real-world data and the VERIS (Vocabulary for Event Recording and Incident Sharing) framework: total incident count, success rate, reporting rate, prosecution rate, and per capita rate. Using these indicators, we apply a five-dimensional K-means clustering algorithm to classify countries into groups with shared cybercrime characteristics.

To evaluate policy effectiveness, we develop a Crime Development Index (CDI) that synthesizes the five indicators into a single composite measure of cybercrime severity. We then examine the correlation between the CDI and the five pillars of the Global Cybersecurity Index (GCI)—legal, technical, organizational, capacity building, and cooperation—using a partition-based Spearman correlation analysis. This approach enables us to assess the relative impact of different policy dimensions within each cluster and track the dynamic evolution of cybercrime in relation to policy implementation timelines.

Finally, we examine the influence of demographic variables on cybercrime outcomes by constructing a customized AHP-EWM (Analytic Hierarchy Process–Entropy Weighting Method) model enhanced with a Trend Matrix. This model evaluates countries based on four demographic dimensions: population structure, internet accessibility, economic status, and education level. By correlating these demographic scores with the CDI, we identify how structural societal factors may amplify or mitigate cyber threats, providing actionable insights for designing targeted, adaptive cybersecurity strategies. Taken together, this study offers a comprehensive framework that integrates statistical modeling, policy evaluation, and demographic analysis to generate a multidimensional understanding of the global cybersecurity landscape. An overview of our methodological approach is provided in Figure 1.

2. Preliminary

2.1 Assumptions

A cybercriminal activity is only considered thwarted when it is interrupted due to external factors. The failure of a cybercrime can result from various factors, such as the perpetrator exposing themselves, internal whistleblowing within the perpetrator's team, detection by the victim organization's systems, or third-party reporting. Among these factors, only those external to the perpetrator, i.e., factors unrelated to the perpetrator, are considered as warranting the crime. If the losses incurred from a crime involve legal service fees, the case is deemed to have been ultimately prosecuted. If the discovery of a crime involves proactive human intervention, the case is classified as "reported." Proactive human intervention includes any individual, whether perpetrator or victim, who, upon recognizing the potential harm of the crime, actively reports it. A policy, no matter how perfectly conceived, is only effective when it achieves tangible results. Countries with similar national conditions and geopolitical environments exhibit comparable rhythms in the formation and refinement of cybersecurity policies. Economically and technologically advanced nations have established comprehensive national security policies earlier, while such policies are just beginning to take shape in less developed regions. This uniformity aids in simplifying the determination of policy enactment timelines. National policies can influence the demographic characteristics of a population, thereby affecting the extent of cybercrime. The data we collect is accurate. The data we have collected is consistent with common sense and accurately reflects real-world situations.

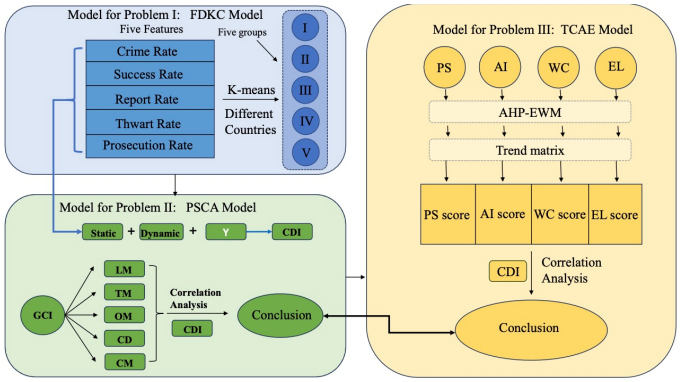


Figure 1: flow diagram of our work

2.2 Data Collection and Preprocessing

To ensure the reliability and comprehensiveness of the analysis results, we combined cybercrime distribution data from VCDB with data from other reliable sources1, standardizing this data according to the VERIS framework. For evaluating the national cybersecurity status and policies, we used the GCI indicator data from the ITU's Global Cybersecurity Index 2024 report[1]. These indicators are divided into five major pillars: Legal, Technical, Organizational, Capacity Development, and Cooperation. Data from selected countries are presented in Figure 7. For demographic characteristics, we collected indicators from the United Nations, the World Bank, and other sources for the past five years across various countries. Table 1 shows our main data sources.

Data preprocessing methods:

1. Data Cleaning: This included handling missing values and outliers. For missing values or abnormally high/low values, we filled in the missing data with the mean of other years.
2. Data Integration: We integrated the same indicators from different data sources into a cohesive dataset.

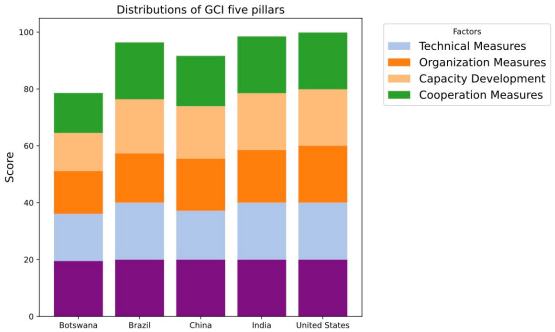


Figure 2: GCI Data Visualization

Data Sources
https://seon.io/resources/global-cybercrime-report/
https://www.twenty-four.it/services/cyber-security-services/cyber-crime-prevention/
https://data.worldbank.org/
https://globaldatalab.org/shdi/table

Table 1: main data source

Symbol	Description
x_{ij}	The data for the j-th indicator of the i-th country
$\widetilde{x_{ij}}$	Normalized x_{ij}
p_{ij}	The proportion of x_{ij} in EWM Model
$Score_i$	The comprehensive score for a certain indicators of each country
P_{static}	A static assessment value of cybercrimes
$P_{dynamic}$	A dynamic assessment value of cybercrimes

note: Other specific notations, if necessary, will be mentioned and illustrated while we're building models.

3. Method I: Five-dimensional K-means clustering

After organizing the data using the VERIS framework, we identified 94 countries with relatively complete data as the final set for clustering. We then applied the k-means clustering algorithm, treating each country as a point in a five-dimensional space and identifying the central characteristics of these clusters. The clustering results were visualized on a world map, and for each cluster, several representative countries were selected to display the distribution of the five indicators in a heatmap 3. Based on these results, we analyzed the findings in the context of real-world regional development patterns.

Group I (Dark Green):

Primarily located in Central Africa, the Middle East, Southeast Asia, and northern South America, these countries exhibit the lowest cybercrime rates, higher crime success rates, and lower rates of crime reporting, thwarting, and prosecution. As the least economically and technologically developed regions, public awareness is low, and governments lack effective policies. Consequently, cybercrimes, once initiated, are highly likely to succeed, with perpetrators rarely facing sanctions, leading to high success rates and low reporting, thwarting, and prosecution rates.

Group II (Light Green):

Comprising countries in Eastern Europe, North Africa, and western South America, this group shows low cybercrime rates and moderate levels in other indicators. Given their moderate technological and economic development, it is inferred that internet pen- etration is relatively low, making them less attractive targets for cybercriminals. These governments may have implemented somewhat effective policies, and the public demon- strates a basic awareness of cybercrime prevention.

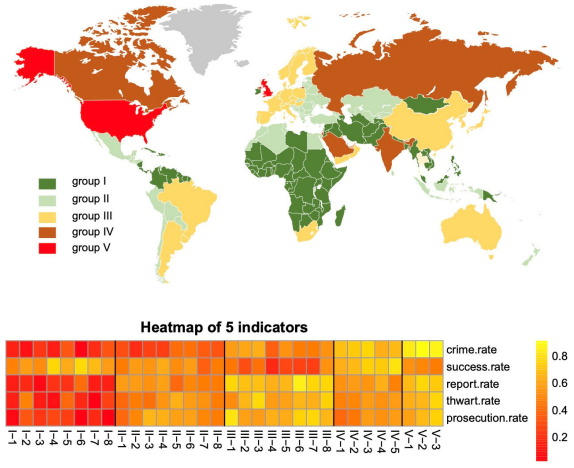


Figure 3: Cybercrime Worldwide Distribution

Group III (Yellow):

Represented by countries such as China, Australia, Japan, and parts of Western and Central Europe, this group exhibits moderate cybercrime rates, low crime success rates, and high rates of crime reporting, thwarting, and prosecution. High internet penetration and stable social conditions suggest that these governments possess strong administrative capabilities, having implemented effective policies and public awareness campaigns to combat cybercrime.

Group IV (Brown):

Including countries like Russia, India, Saudi Arabia, and Canada, this group shows high cybercrime rates and success rates, with moderate levels of crime reporting, thwart- ing, and prosecution. Despite their relatively advanced technological and economic de- velopment, these governments may lack effective measures against cybercrime, or exist- ing measures are inadequately enforced[2], resulting in a concerning cybercrime situation with significant room for improvement.

Group V (Red):

Represented by the United States, the United Kingdom, and Israel, these countries have high cybercrime rates but also high rates of crime reporting, thwarting, and prose- cution, ensuring that cybercrimes do not always succeed. As global leaders in technology, these nations host a large concentration of high-tech and financial enterprises[3], making them prime targets for cybercriminals. Advanced internet infrastructure and high penetration rates further facilitate cybercrime. However, their governments have long recognized the threat of cybercrime and established robust measures[4], while the public and corporations maintain high vigilance against such threats.

4. Method II: Partition-based Spearman Correlation Analysis

To simplify the model, we aim to create a comprehensive score that reflects the overall development of cybercrime in a country. The construction of the index involves three steps:

Step 1: To quantify the dynamic changes in cybercrime, we first established a static assessment value P_{static} based on four indicators, representing the current state of cybercrime. We posit that the crime rate most directly reflects the current state of cybercrime, followed by the success rate. In contrast, prosecution, reporting, and thwarting are considered secondary reactions occurring after the crimes. Therefore, the weight coefficients are assigned as follows: $(\beta_1\beta_2\beta_3\beta_4\beta_5)^T = (0.35, 0.2, 0.15, 0.15, 0.15)^T$.

$$Pstatic = \beta 1arate + \beta 2asuccess + \beta 3aprosecution + \beta 4athwart + \beta 5areport \quad (1)$$

The dynamic change values are then obtained by calculating the difference between
The static values over a 5-year period (2019–2024).

$$P = P^{2024} - P^{2019} \quad (2)$$

Step 2: The static value for 2024 is then combined with the dynamic change values from the past 5 years using specific weights to form the Cybercrime Development Index (CDI).

$$CDI = \lambda_{st}P_{static} + \lambda_{dy}P_{dynamic} \quad (3)$$

Step 3: We hypothesize that the longer a country has been implementing cybersecurity-related policies, the higher the expectations for its current cybercrime situation, assuming equal effectiveness of the policy. Therefore, we introduce a penalty term related to the length of time the policy has been in effect in the CDI calculation formula.

$$CDI = \lambda_{st}P_{static} + \lambda_{dy}P_{dynamic} + kY \quad (4)$$

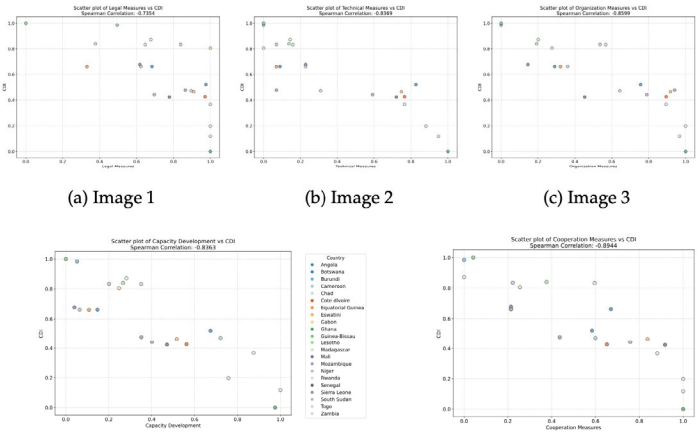
Where Y represents how long a nation's cybersecurity policy has been enacted. Due to the difficulty of identifying the exact policy formation timeline for each country and defining the precise criteria for policy formation, we adopt the follow- ing approach to determine Y and its weight based on Assumption 5: Countries within the same group are assigned a unified Y value. This is achieved by reviewing the historical development of regional cybersecurity or relevant reports to estimate the

average year (Y_0) when a comprehensive cybersecurity pol- icy framework was established for the group. The Y value is then calculated as $Y = 2024 - Y_0$. The specific timeline is as follows:

Figure 4: Policy Timeline of each Group

Step 4: P_{static}, $P_{dynamic}$, and Y are normalized individually and added together with a weight matrix assigned as $(\lambda_{st}\lambda_{dy}k)^T = (0.35, 0.55, 0.1)^T$ .. Now a larger value of CDI indicates a worse state of cybercrime in a given country.

Spearman correlation analysis, which captures non-linear relationships and is less affected by outliers, offers a more accurate reflection of the link between GCI indicators and the CDI. By examining the correlation between the five GCI pillars and CDI across five regions, we can quantitatively identify which policy factors most influence cybercrime and whether their impact is positive or negative. The absolute value of the Spearman coefficient measures the strength of the relationship, while a negative value indicates that a GCI indicator significantly suppresses CDI. Conversely, a positive value does not imply that the policy worsens cybercrime but suggests it has little to no effect. For example, the correlations for Group 1 countries between the five GCI pillars and CDI are shown in the figure below:



(a) Image 1 (b) Image 2 (c) Image 3

(d) Image 4 (e) Image 5

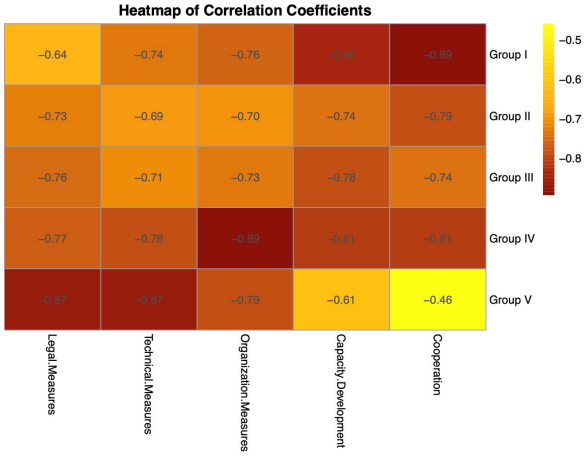
Figure 5: Overall caption for the figure.

A heatmap is used to display the Spearman correlation coefficients across all groups, providing an intuitive visualization of policy effectiveness in different regions.

Analysis of the Pattern • Group I Countries:

Group I Countries:

In this group, CM (Capacity Measures) shows a strong negative correlation with CDI, while LM (Legal Measures) has a weaker correlation. Due to limited economic and technological capacity, these countries rely heavily on international cooperation for financial and technical support, as legislation alone is insufficient to curb cybercrime. Thus, prioritizing inter-organizational and international collaboration is essential, while LM measures are less effective.



Distribution of GCI Pillars-CDI correlation in 5 Groups

Group II Countries:

In this group, negative correlations between GCI indicators and CDI are uniformly low, reflecting lower cybercrime rates and relatively effective existing policies. All policy components show moderate effectiveness, suggesting a need for comprehensive cybersecurity improvements.

Group III Countries:

In this group, the negative correlation between CD (Capacity Development) and CDI is relatively high. These countries possess advanced economies and technologies, which provide favorable conditions for cybercrime. However, their cybercrime rates remain manageable due to strong legislation, effective governance, and high

Group IV Countries:

In this group, the strong negative correlation between Organizational Measures (OM) and CDI reflects governments' limited internet control and the need for dedicated agencies and strategic planning. Due to severe cybercrime, improvements across all GCI indicators are needed. OM measures are most effective here, with other components also showing notable impact.

Group V Countries:

In this group, strong negative correlations between Technical (TM) and Legal Measures (LM) and the cybercrime index (CDI) highlight the need for advanced legislation and technical safeguards to keep pace with rapid technological growth. The weaker correlation with Capacity Measures (CM) suggests limited gains from international cooperation, given their already advanced cybersecurity infrastructures. Therefore, TM and LM are the most effective policy tools here.

5. Model III TREND-Combined AHP-EWM Model

We selected 94 countries with complete data across three dimensions: cybercrime status, Global Cybersecurity Index (GCI) scores, and demographic statistics. A comprehensive evaluation framework was constructed using the AHP-EWM model, encompassing four primary demographic indicators, each with three sub-indicators. To enhance objectivity, we further integrated Trend Matrices capturing temporal shifts in demographic characteristics. Finally, Spearman correlation analysis was employed to quantify the relationship between these demographic dimensions and cybercrime distribution, building on the methodology established in the previous section.

Indices Definition for Demographics

There are quite a large number of factors that have an influence on the different aspects of national demographics. Meanwhile, the data we collect is in a great amount as well. Therefore, for making

them distinct for further research, we finally integrate our 12 most decisive indices and classify them into four dimensions, which are SPS, AI, WC and EL, to assess the **Cybercrime-Immunity of Demographic Characteristics(CID)**. The concrete indices are shown in Table 2.

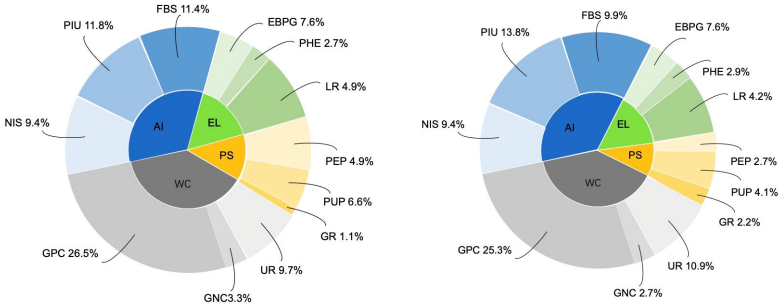
Primary Indicators	Secondary Indicator	Effect
Population Structure(PS)	Proportion of Elderly Population (PEP)	-
	Proportion of Urban Population (PUP)	+
	Gender Ratio (50% Proximity) (GR)	#
Access to Internet(AI)	Proportion of Internet Users (PIU)	-
	Number of Internet Servers per Million People (NIS)	-
	Fixed Broadband Subscriptions (FBS)	-
Wealth Condition(WC)	GDP per Capita (GPC)	+
	GINI Coefficient (GNC)	-
	Unemployment Rate (UR)	-
Education Level(EL)	Proportion of Population with Higher Education(PHE)	+
	Education Budget as a Percentage of GDP (EBPG)	+
	Literacy Rate (LR)	+

Figure 6: Table 2: The Indices of Demographics

This study adopts 12 indicators grouped under four primary dimensions—Population Structure, Internet Access, Wealth Condition, and Education Level—each classified by effect type: benefit-type ("+"), cost-type ("–"), or moderate-type ("#"). These classifications reflect whether higher, lower, or balanced values are more desirable in mitigating cybercrime risk. In Population Structure, an aging population (PEP) is a cost-type factor due to its economic burden, while urbanization (PUP) is a benefit-type, associated with better infrastructure and resilience. Gender ratio (GR) is a moderate-type, where balance signals social stability. All Internet Access indicators—percentage of users (PIU), server density (NIS), and broadband subscriptions (FBS)—are cost-type, as increased connectivity without adequate safeguards can raise cybercrime exposure. For Wealth Condition, GDP per capita (GPC) is a benefit-type indicator of national capacity, while income inequality (GNC) and unemployment (UR) are cost-type indicators linked to social strain and crime incentives. Education Level includes three benefit-type indicators: tertiary education (PHE), education spending (EBPG), and literacy rate (LR), all contributing to digital awareness and cyber resilience. These classifications are grounded in the socio-technical nature of cybercrime, where demographic balance, managed digital access, economic stability, and education all play vital roles. Indicator selection is theory-driven and empirically supported, reflecting real-world patterns consistently.

Introduce the TREND Matrix into the AHP-EWM Model

To evaluate the impact of demographic factors on cybercrime, we developed a hybrid weighting framework combining the Analytic Hierarchy Process (AHP) and Entropy Weight Method (EWM), integrating expert judgment with objective data. After standardizing indicators by type (benefit, cost, moderate), AHP was used to derive subjective weights via pairwise comparisons and consistency checks. To mitigate AHP's subjectivity, EWM was applied to assign weights based on data variability across countries. The final weights were computed by combining AHP and EWM results, with greater emphasis on expert input. These composite weights enabled calculation of a comprehensive demographic score for each country in 2023, forming the basis for analyzing demographic influences on cybercrime patterns.



Weights in Static AHP-EWM Weights in Trend AHP-EWM

Figure 7: Caption

Correlation Between Primary Indicators and CDI

Using the aforementioned evaluation model, we ultimately derived the weights of each indicator in Figure 7. By applying Spearman correlation analysis, the correlation coefficients between the scores of the 4 primary indicators and the CDI were obtained and analyzed across the 5 groups.

Analysis of the Pattern

Group I Countries: These countries have low population quality scores, reflecting poor economic and technological development. The strong positive correlation between the AI indicator and CDI suggests that the lack of comprehensive policies in these countries makes internet users highly susceptible to cybercrime. The weaker negative correlation of WC and EL indicators with CDI is due to limited internet infrastructure, where only the wealthy and highly educated have significant internet access, resulting in less pronounced negative correlations.

Group II Countries: These countries have moderate population quality scores, indicating average economic and technological levels. Most indicators, except PS, show relatively low and balanced correlations with CDI. This suggests that these countries are not major targets for cybercrime and have moderately effective policies, making CDI less sensitive to changes in these indicators.

Group III Countries: Countries in this group have high population quality scores, reflecting advanced economic and technological development. WC and EL indica- tors show strong negative correlations with CDI, while AI has a weaker correlation. This highlights the effectiveness of robust cybersecurity policies, which prevent a rapid increase in CDI despite higher internet usage. Additionally, it underscores the importance of improving personal resilience to cybercrime through education and training, aligning with previous findings.

Group IV Countries: These countries also have high population quality scores, indicating advanced economic and technological levels. The strong negative correlation between EL and CDI, combined with the weaker correlation of WC with CDI, suggests incomplete policies and limited government control over cybersecurity. As a result, individuals rely on education to improve their resilience to cybercrime. These countries need to strengthen organizational capacity, establish better regulatory frameworks, and develop long-term strategies.

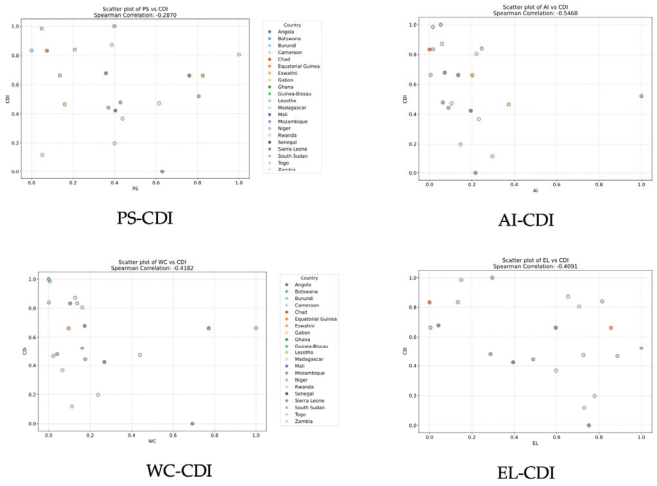
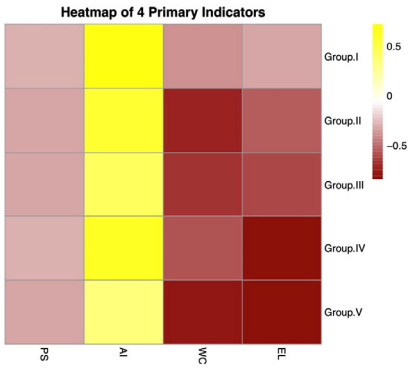


Figure 8: Overall caption for the figure.



Distribution of primary indicator-CDI correlation in 5 Groups

Group V Countries: characterized by the highest population quality scores and advanced economies, show strong negative correlations between wealth, education, and cybercrime index (CDI). This indicates that affluent and educated populations possess greater resilience to cybercrime and benefit from robust cybersecurity measures. The weaker correlation between technical measures (TM) and CDI suggests that comprehensive policies effectively prevent increased internet usage from driving cybercrime growth..

Overall Analysis: Across all groups, the PS indicator shows a consistently weak negative correlation with CDI, indicating that population structure has a limited impact on cybersecurity. This aligns with real-world observations where demographic factors have minimal causal relationships with cybercrime.

6. Sensitivity Analysis

In the TREND-Combined AHP-EWM(TCAE) Model, the integrity of original data for the 12 selected indicators critically determines both the weight allocation outcomes and subsequent coefficient calculations. To assess the robustness of our model, we conducted a comprehensive sensitivity analysis through systematic perturbation testing. This methodology involves introducing controlled variations to each indicator's annual data within the constrained scale, enabling rigorous evaluation of model responsiveness to input fluctuations while maintaining ecological validity through variation thresholds.

We introduced fluctuations of 10%, 12%, and 15% to the original data and recalculated the new weights for each indicator based on the model. These new weights were compared with the original weights, and the change ratio was calculated as shown in Figure 9.

	AHQ15%	EWM15%	ALL15%	AHQ12%	EWM12%	ALL12%	AHQ10%	EWM10%	ALL10%
PEP	0.126244	0.146304	-0.14388	-0.01966	-0.02957	0.069305	0.030052	0.032522	0.013209
PUP	-0.06629	0.135866	-0.13041	0.066718	0.079419	-0.03011	0.039438	0.014293	0.079469
GR	0.066399	-0.05133	-0.06193	0.067558	-0.06112	0.093807	0.097609	0.064358	0.054562
FBS	-0.09526	0.030909	0.031152	-0.08393	0.114623	-0.11194	0.012338	0.080602	-0.04809
PIU	0.135086	0.137121	-0.07115	0.077007	-0.03815	0.006634	-0.0443	0.096255	0.033867
NIS	-0.02705	-0.06878	0.096366	0.016616	0.070776	-0.0779	-0.05612	0.02872	0.059302
GPC	-0.12991	0.0749	0.006667	-0.02701	-0.08911	0.102575	-0.01338	0.061354	-0.0347
GNC	-0.03735	0.100472	-0.13673	-0.06285	-0.10526	-0.0179	-0.01281	-0.06029	0.005312
UR	0.095951	0.011731	-0.01187	0.082651	0.070097	-0.04681	0.080795	-0.08928	0.021299
EBPG	0.109683	-0.14749	0.109125	0.089712	0.043876	-0.09329	-0.02322	-0.07753	-0.06692
PHE	-0.04932	-0.05169	-0.01269	-0.10667	-0.07501	-0.03761	0.00042	-0.00021	0.00075
LR	-0.04233	-0.04012	-0.14742	0.031971	0.103971	-0.01895	-0.00081	-0.00009	0.00052

Figure 9: The fluctuation ratio of each indicator

Simultaneously, we plotted three-dimensional scatter plots with AHP Weight, EWM Weight, and Overall Weight(weight in TCAE) as the x-axis, y-axis, and z-axis, respectively (as shown in Figure 10). Red points represent the weights derived from the original data, while blue points represent the weights derived from the fluctuating data. Grey dashed lines connect the corresponding points for the same type of indicator.

From the figure and table, it is evident that the weight changes are small and stable, following a similar trend to the data fluctuations, with the maximum change ratio not exceeding 15%. This demonstrates the stability of our model.

7. Theory Analysis

Based on the analysis of the five groups, we derived the following theory: The focus of cybersecurity policy development should strongly align with a nation's specific conditions, including its level of economic and technological development. For underdeveloped regions, leveraging external resources is crucial. Strengthening collaboration between international and domestic security agencies, as well as between national and private organizations, can effectively curb the growth of cybercrime while also enhancing governance experience. For nations with world-leading economic and technological capabilities, even those with extensive experience in combating cybercrime and established cybersecurity frameworks, continuous improvement of legal systems and the establishment of agile, professional technical response teams remain imperative. This is because the pace of technological advancement in such countries often exceeds the speed of legal refinement, leading to the continuous emergence of new vulnerabilities. For countries with moderate levels of economic development and technological foundations, a comprehensive enhancement of cybersecurity policies is essential. Simultaneously, these nations should prioritize balanced economic growth and the development of education to improve public awareness and resilience to cyber threats.

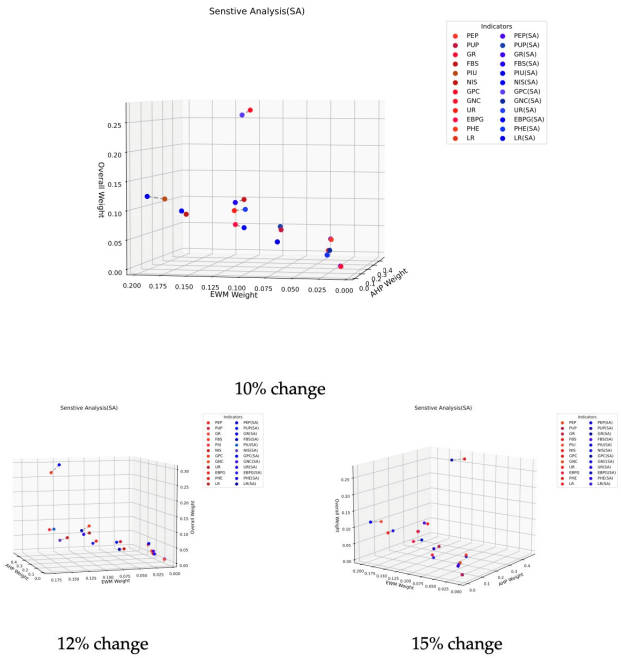


Figure 10: Disturbances make little difference to the weights

8. Conclusion

The proposed model has several strengths. It highlights the varying effectiveness of cybersecurity policies across country clusters, underscoring the need for context-specific strategies based on economic, technological, and governance factors. By combining AHP and EWM, it balances expert

judgment with objective data, integrating both static and temporal dimensions for a nuanced assessment of cybercrime trends. The model is rational, stable, and analytically powerful, effectively identifying key indicators and supporting evidence-based policymaking. However, limitations exist. Some integration coefficients rely on subjective judgment, which may introduce bias. Additionally, measuring temporal change by simple differences may miss important fluctuations, potentially oversimplifying cybercrime dynamics. Overall, the model offers a strong foundation for policy analysis, with future improvements suggested in sensitivity testing and dynamic trend modeling.

References

[1] Gajjar, V. R. & Taherdoost, H. Cybercrime on a global scale: Trends, policies, and cybersecurity strategies. In 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 668–676 (IEEE, 2024).

[2] Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M. & Foo, E. Current approaches and future directions for cyber threat intelligence sharing: A survey. Journal of Information Security and Applications 83, 103786 (2024).

[3] Oecd policy framework on digital security: Cybersecurity for prosperity .

[4] Chen, S. et al. Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications 10, 1–10 (2023).

[5] Global cybersecurity index 2024 .