Problem Chosen	2025 MCM/ICM Summary Sheet	Team Control Number
F		2507789

Five Elements Illuminate, Cybersecurity Innovates

Summary

As cybercrime continues to escalate globally, traditional policy evaluation methods struggle to capture the complexity of cybersecurity threats. This study pioneers an **innovative cybersecurity framework** grounded in the **Five Elements theory**, blending **ancient Chinese philosophy with modern quantitative analysis** to provide a novel perspective on cybersecurity governance. By integrating **clustering analysis**, **causal inference, and network analysis**, this research systematically assesses the effectiveness of cybersecurity policies worldwide and their role in mitigating cybercrime.

The **first model** employs **K-means clustering** to categorize nations based on cybersecurity landscapes while incorporating the Five Elements theory to identify critical determinants of cybercrime. The **second model** utilizes **Difference-in-Differences (DID) analysis** to establish a causal relationship between policy implementation and cybercrime reduction. The **third model** leverages **multi-layer network analysis** to uncover the **propagation dynamics of cybercrime** and the pathways through which cybersecurity policies exert influence in complex global networks.

The results reveal a **fundamental correlation between cybersecurity effectiveness and the balance of the Five Elements**: **Metal** (Hardware Security): Nations over-reliant on hardware defenses neglect software vulnerabilities, creating critical security gaps.

Wood (Social Networks): Unregulated social platforms fuel phishing, misinformation, and large-scale cyber fraud.

Water (Data Protection): Weak encryption standards and insufficient data security policies drive exponential increases in data breaches.

Fire (Cyberattacks): High cybercrime prevalence is linked to inadequate response mechanisms and weak cybersecurity readiness.

Earth (Policy & Regulation): The absence of strong legal frameworks exacerbates cross-border cyber threats.

A comprehensive cross-national analysis demonstrates that nations with a **well-balanced Five Elements structure,** robust legal enforcement, and extensive international collaboration exhibit significantly **lower cybercrime rates**. Conversely, countries with **regulatory inefficiencies, limited cybersecurity investments**, **and weak international engagement** remain vulnerable to large-scale cyber threats.

By fusing ancient theoretical principles with state-of-the-art analytical methodologies, this study constructs a rigorous and adaptable cybersecurity evaluation framework. The results not only redefine cybersecurity governance from a holistic perspective but also offer practical, high-impact strategy

Keywords: Cybersecurity Policy; Cybercrime; Five Elements Theory; Clustering Analysis; Causal Inference; Network Analysis

Contents

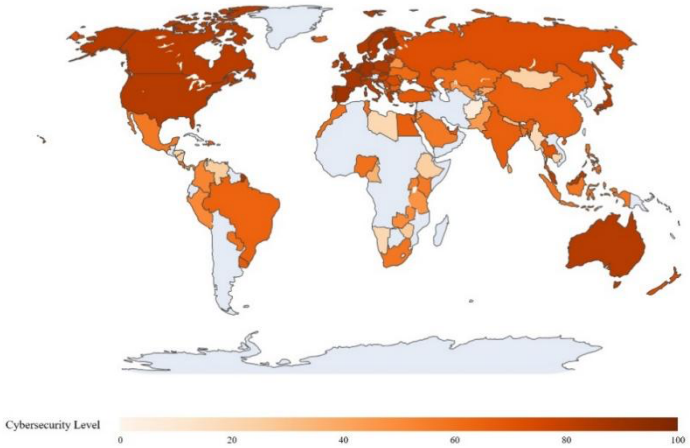
1 Introduction

1.1 Problem Background

With the rapid advancement of modern technology, the world has become increasingly interconnected. Network technologies have significantly boosted global productivity while also narrowing geographical and cultural gaps. However, this enhanced online connectivity has also exposed us to growing threats from cybercrime.

Cybercrime, as the "shadow" of the digital age, not only threatens individual privacy and institutional security, but also poses significant risks to global economic and social stability. Due to its cross-border nature, cybercrime presents significant complexity, making investigations and prosecutions more challenging and resulting in a varied global cybersecurity environment because institutions and individuals address these issues inconsistently.

Global Cybersecurity Level Evaluation (2020)



To address this challenge, many countries have formulated specialized

cybersecurity policies. These policies are typically publicly released to enhance transparency and build public trust. However, the effectiveness of policy formulation and implementation varies greatly across nations. Although international organizations like the International Telecommunication Union (ITU) have played a significant role in raising global cybersecurity standards, how to more effectively measure and enhance cybersecurity policies on a global scale remains a critical issue that needs to be addressed.

1.2 Problem Restatement and Analysis

To address these challenges, this study uses a data-driven approach to explore the relationship between national cybersecurity policies and cybercrime distribution, focusing on the following tasks.

·Task 1: Analyzing Global Distribution Patterns of Cybercrime

Identify target hotspots and root causes, while examining the conditions under which cybercrime succeeds or fails. Investigate how different countries handle prosecutions to reveal behavioral patterns and inform policy research.

·Task 2: Evaluating the Effectiveness of Cybersecurity Policies

Compare policies across countries and assess their impact on cybercrime distribution and governance. Identify effective policy features and extract adaptable elements for broader application.

·Task 3: Exploring the Relationship Between Policies and National Characteristics

Analyze how demographic factors (such as internet penetration, education levels and wealth) influence policy design and outcomes. Building on the above analyses, provide insights for crafting more targeted policies.

·Task 4: Summarizing Data-Driven Policy Optimization Recommendations

Develop a framework for optimizing policies and offer actionable strategies to help policymakers combat cybercrime effectively. Promote international cooperation and standardization efforts.

To effectively illustrate the steps presented in our solution, we have created a visual guide showcasing our workflow, as depicted in Figure 2. In the process diagram, we clearly present the key steps in solving the problem and the modeling approach taken.

2 Assumptions and Justifications

Assumption 1: The data we collected online is accurate and reliable.

Justification 1: The data comes from the official websites of international organizations and academic papers, which typically have been strictly reviewed and verified, representing recognized high-quality data sources. These data sources have a high degree of authority and credibility; thus we can infer the reliability and accuracy of the data.

Assumption 2: Assuming that when selecting the cluster number K with the Elbow Method, the relationship between SSE (sum of squared errors) and K value can clearly reveal the optimal K value.

Justification 2: In actual applications, the Elbow Method can usually clearly show the downward trend of cluster error, and the K value chosen when the rate of decrease in SSE is significantly reduced (i.e., the "elbow" position) is more reasonable.

Assumption 3: Assuming that using the Difference-in-Differences (DID) method can effectively measure the impact of policy changes on cybercrime behavior, and the model can fully control potential confounding factors (such as external events or economic environmental changes). In addition, assuming that no key control variables are omitted, the impact of time effects and individual effects on causal inference can be eliminated.

Justification 3: The DID method is a common causal inference tool that can infer the true effect of policies by comparing changes before and after policy implementation and controlling for external factors.

3 Notations

Symbol	Definition
E	Earth
G	Metal
M	Wood
W	Water
F	Fire

4 Selecting Critical Factors of Cybercrime

Committing cybercrime takes many forms. Taking the difficulty of transnational case handling into account, many criminal gangs choose to engage in transnational crime. The transnational nature of cybercrime shows its attack paths and infrastructure distribution extend beyond the borders of a single country.

Under the circumstances, traditional geographic clustering or spatial statistical methods cannot fully capture the transnational flow of cybercrime and the complex relationships between "attack sources" and "victims." Therefore, we need a more comprehensive method to reveal its multidimensional features.

4.1 Data Preprocessing

To better construct the model, we need to analyze what the most critical factors are for cybercrime. We utilized data similar to the **VERIS database**, which provides extensive information on cybercrime, including types of crimes, affected countries, methods of attack, and so on. To facilitate **cluster analysis**, we need to standardize the data.

The real data includes several parts: **victim country** (such as US, Canada, UK, Germany), **hacking variety** (such as DDoS, SQL Injection, Phishing, Malware, Ransomware), **malware variety** (Worm, Trojan, Virus, Spyware), **security incident** (such as Confirmed, Unconfirmed), **victim industry** (such as Finance, Healthcare, Technology, Manufacturing), **and victim employee count** (such as 500-1000, 1000-5000, 5000+).

We preprocessed the data using the following steps in order to make it suitable for clustering analysis.

First, we used **the standardization method** for numerical data. Specifically, each numerical feature was subtracted by its mean and divided by its standard deviation, ensuring the data followed a standard normal distribution (mean of 0, variance of 1). The process can be expressed as:

$$x_{\text{norm}} = \frac{x_i - \mu_i}{\sigma_i}$$

(x_i is the original data. μ_i is the mean of the i- th feature.σ_i is the standard deviation of the i -th feature. x_{norm} is the normalized data.)

This step adjusted numerical data to zero mean and unit variance so as to eliminate scale differences between features, ensuring they contribute equally in the cluster analysis.

Next, for categorical data, we used **the one-hot encoding method**. Through this

method, each categorical feature mentioned above was converted into a binary vector, where each category corresponds to a binary feature. For example, in the victim industry category, the four categories were transformed into four binary features (Finance: [1, 0, 0, 0], Healthcare: [0, 1, 0, 0], Technology: [0, 0, 1, 0], Manufacturing: [0, 0, 0, 1]). This method ensures that categorical data is properly handled in cluster analysis without introducing incorrect numerical relationships.

By applying these two methods, we can transform the raw data into a format suitable for cluster analysis, ensuring both numerical and categorical data are effectively processed by clustering algorithms.

4.2 Cluster Analysis

After preprocessing the data, we selected the **K-means clustering** algorithm, which performs clustering by minimizing the distance from each data point to the center of its cluster.

4.2.1 K-means Clustering

The goal of K-means clustering is to partition the data into *K* clusters by minimizing the distance from each data point to its assigned cluster. We measured the quality of clustering using the following objective function:

$$J = \sum_{i=1}^{K} \sum_{x_j \in C_i} \|x_j - c_i\|^2$$

(x_j is a data point. C_i is cluster *i*. c_i is the center of cluster *i*. $\|x_j - c_i\|^2$ is the Euclidean distance from the data point to the cluster center.)

We chose *K* data points as initial cluster centers randomly, then for each data point x_j, we calculated its Euclidean distance to each cluster center c_i and assign the data point to the nearest cluster:

$$Assign\, x_j\, to\, C_k\, if\, \|x_j - c_k\| < \|x_j - c_i\| \quad \forall i \neq k$$

Each cluster center was then updated to the mean of all data points in the cluster:

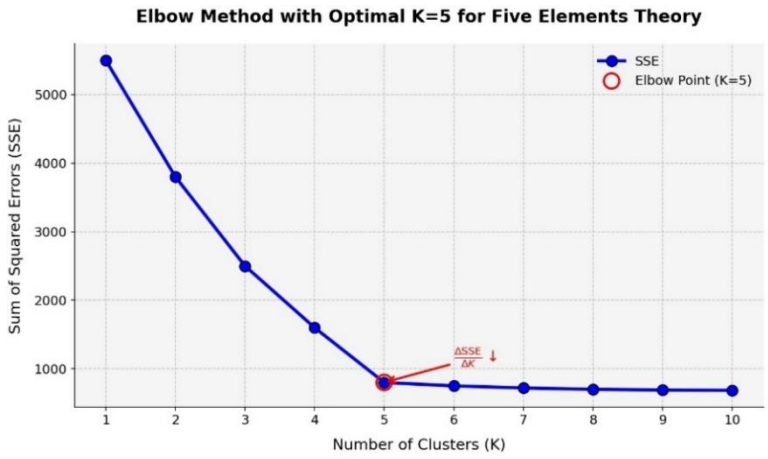
$$c_k = \frac{1}{|C_k|} \sum_{x_j \in C_k} x_j$$

- The last step was to check the convergence. The algorithm stops when the cluster centers no longer change or the change is below a preset threshold,

otherwise return to step 2 and continue iterating. To ensure convergence, the maximum iterations were set to 300.

4.2.2 Selection of the Optimal Number of Clusters

We mentioned that **the Elbow Method** is a good way to ensure the rationality of the clustering results, so we applied this method to determine the optimal number of clusters *K*. In this step, we calculated the objective function *J*(*K*) for different *K* values and plotted the relationship between *K* and the objective function values. The K value at the "elbow" position was selected as the optimal number of clusters.



As we can see, the figure above shows the K value at the "elbow" position is 5, which means 5 is the optimal number of clusters.

4.2.3 Clustering Results Analysis and Visualization

The Cluster Feature Analysis relies on **statistical methods**. In statistics, we needed to calculate the frequency percentage of features in each cluster (such as a cluster contains 80% "DDoS attacks" and 60% "Technology industry"). In addition, we used Chi-square test to verify the significant association between features and clusters (p-value <0.05). The result shows that the five categories and their example features are as follows.

Hardware protection: Firewall deployment rate >70%

Social network: Social network attack proportion >50%

Data protection: Data breach incidents proportion >40%

Attack intensity: DDoS attack proportion >60%

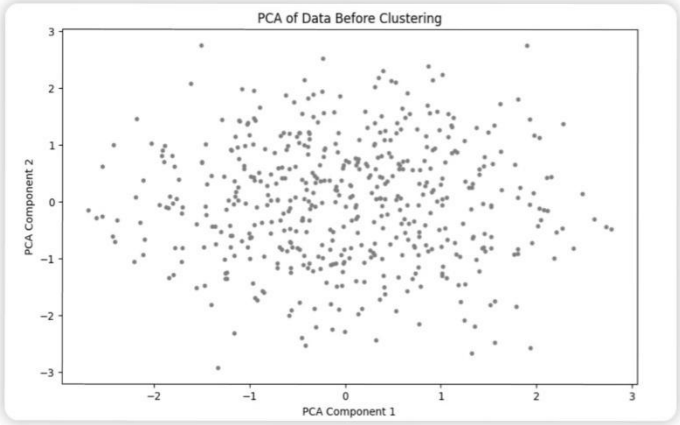
Policies and regulations: GDPR-compliant cases proportion >80%

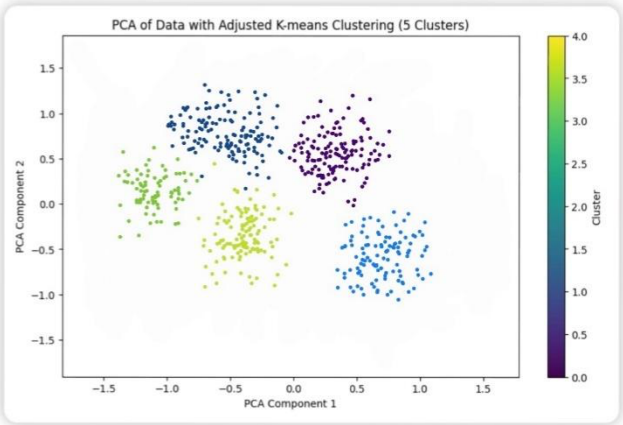
To further analyze and demonstrate the clustering result, we used **the PCA dimensionality reduction method** to map this high-dimensional data into a two-dimensional space and display the distribution of each cluster through a scatter plot. Below is the PCA dimensionality reduction formula:

$$Z=X\cdot W$$

(X is the standardized original data matrix. W is the projection matrix of PCA. Z is the dimensionality-reduced data matrix used for visualization in two-dimensional space.)

Through the scatter plot after PCA dimensionality reduction, we can see the distribution of each cluster more clearly. Each cluster is marked with different colors. For comparison, we also drew a scatter plot without cluster analysis on the left. There are obvious differences in the two images by cluster analysis.





5 The Five Elements Model

Through the cluster analysis above, we have identified the factors that have the most impact on the occurrence of cybercrime. Therefore, in order to prevent cybercrime effectively, we need a model which can capture the complex non-linear relationship in the network environment. Finally, the pentagonal relationship in this cybercrime issue reminded us of a Chinese traditional philosophy: **the Five Elements Theory.**

5.1 Introduction of Five Elements Theory

The ancient Chinese philosophy of the Five Elements is a highly significant philosophical concept in traditional Chinese culture, which has profoundly influenced various fields in China.

The Five Elements refer to the five fundamental substances: Metal, Wood, Water, Fire, and Earth. These elements are considered to be the basic building blocks of all things in the world and are believed to interact with each other through relationships of generation and restriction, as described below.

- **The Relationship of Generation:** Wood generates Fire, Fire generates Earth, Earth generates Metal, Metal generates Water, Water generates Wood
- **The Relationship of Restriction:** Metal restricts Wood, Wood restricts Earth, Earth restricts Water, Water restricts Fire, Fire restricts Metal

5.2 Significance of Five Elements in Cybersecurity

As mentioned above, we consider that the occurrence of cybercrime is also closely related to the "balance" state of these elements. By utilizing the relationships and imbalance concepts from the Five Elements Theory, we can construct a mathematical model to predict cybercrime.

According to the Five Elements theory, each of the five elements (Metal, Wood, Water, Fire, and Earth) possesses unique attributes and interrelationships. In view of these different features, the definition and role of the Five Elements can be analogized to different aspects of cybersecurity. Specifically, each element represents a particular aspect in the network environment.

Metal: In the Five Elements theory, Metal represents hardness, solidity, and protection. Therefore, the Metal element is associated with **hardware protection, encryption technology, and infrastructure**. For example, a firewall deployment rate exceeding 70% matches the Metal element. We know that firewalls are a crucial protective measure in cybersecurity, they embody the solidity and protective nature of Metal.

Wood: The Wood element symbolizes growth, expansion, and connection. In cybersecurity, the Wood element is related to **social engineering and information dissemination paths**. For instance, a social network attack proportion exceeding 50% matches the Wood element. Because social network attacks rely on the spread of information and the exploitation of interpersonal relationships, which reflects the growth and connection characteristics of Wood.

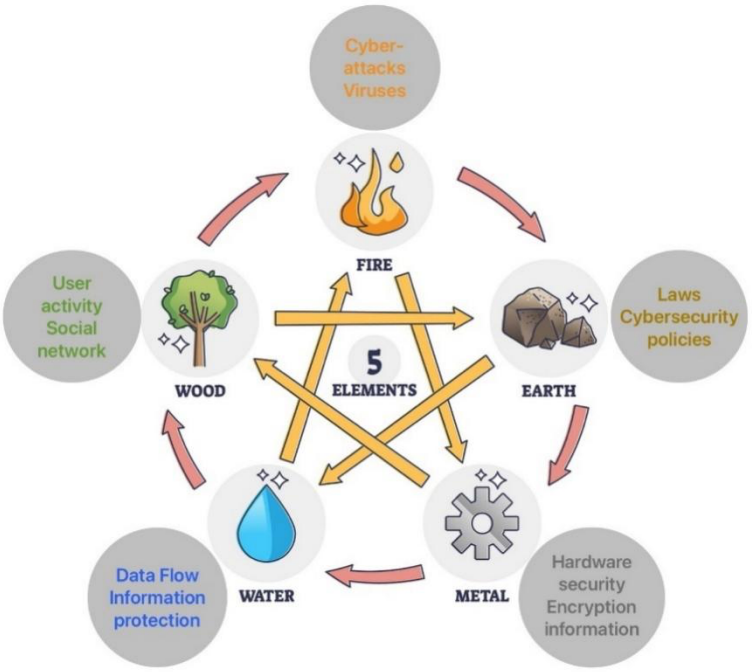
Water: The Water element represents flow, change, and adaptability. In cybersecurity, the Water element is associated with **data liquidity and encryption protocols**. For example, a data breach incident proportion exceeding 40% matches the Water element

because data breaches involve the flow and change of data, embodying the fluid and adaptive nature of Water.

Fire: The Fire element symbolizes energy, intensity, and destructiveness. In cybersecurity, the Fire element is related to **attack intensity and destructiveness**. For instance, a DDoS attack proportion exceeding 60% matches the Fire element. The highly intense and destructive feature of DDoS attacks reflects the energy and intensity characteristics of Fire.

Earth: The Earth element represents stability, foundation, and regulation. In cybersecurity, the Earth element is associated with **policies, regulations, and stability**, which matches the stability and regulatory nature of Earth.

Figure 2: Generating and Restricting Relationship



Then the occurrence of cybercrime can be presented as a manifestation of the imbalance of the Five Elements:

Excessive Metal (over-reliance on hardware defenses) leads attackers to focus on exploiting software vulnerabilities.

Excessive Wood (overly active social networks) results in a surge of telecom fraud and phishing.

Flooding Water (severe information leakage) leads to the rampant growth of the data black market.

Excessive Fire (frequent hacker attacks) easily triggers large-scale security

incidents.

Weak Earth (inadequate regulation) makes it difficult to curb criminal activities.

5.3 The Five Elements Model

We aim to build a model that can predict the probability of cybercrime occurrence based on the state values of each of the Five Elements (such as the states of Wood, Metal, Water, Fire, and Earth). This model will not only consider the state of individual elements but also take into account the interactions between the Five Elements.

The data we used comes from existing data sources, including the **Global Cybersecurity Index (GCI)**, the **VERIS framework**, and **Country Demographics**. After our research and assumptions, we consider that the data from these data sources is credible.

5.3.1 Data Analysis: Cybercrime Distribution

Global Cybersecurity Index (GCI) is published by the International Telecommunication Union (ITU) and assesses countries based on five key pillars: legal, technical, organizational, capacity building, and cooperation. The GCI score ranges from 0 to 1, with higher scores indicating better cybersecurity practices and policies. This index provides valuable information about the overall cybersecurity posture of a country, so we begin by analyzing the Global Cybersecurity Index (GCI) to evaluate the cybersecurity posture of different countries. [1]

• **High-risk countries**: Countries with low GCI scores tend to have weak cybersecurity measures, which makes them more vulnerable to cybercrimes. We hypothesize that countries with low GCI scores are likely to experience higher rates of cybercrime, as they may lack robust security infrastructures such as encryption technologies, firewalls, and regulatory frameworks.

• **Low-risk countries**: On the other hand, countries with high GCI scores usually have better cybersecurity practices and policies. These countries are less likely to be victims of cybercrimes, as their cybersecurity measures (hardware security, data protection, and legal enforcement) are stronger.

Then we correlated **VERIS data** with the **GCI scores** to determine if there is a clear relationship between a country's cybersecurity posture and the prevalence of certain types of cybercrime, such as malware, phishing, and ransomware.

In this process, we also used the **K-means clustering** algorithm but optimized some sections.

First, we used **the weighted Gower distance** to handle mixed data containing numerical and categorical types:

$$d(x_i, x_j) = \sum_{k=1}^{p} w_k \cdot \delta_{ij}^{(k)} \cdot d_{ij}^{(k)}$$

(w_k is the weight of the k-th feature (calculated using mutual information). $\delta_{ij}^{(k)}$ is the missing value indicator for feature k (0/1).)

Distance for numerical features:

$$d_{ij}^{(num)} = \frac{|x_{ik} - x_{jk}|}{R_k} \quad (R_k \text{ is the range of feature k})$$

Distance for categorical features:

$$d_{ij}^{(cat)} = \mathbb{I}(x_{ik} \neq x_{jk}) \quad (\mathbb{I} \text{ is the indicator function})$$

Next, we optimized our objective function to accommodate these changes through incorporating feature weights and a regularization term:

$$J = \sum_{i=1}^{K} \sum_{x_j \in C_i} \left(\|W \circ (x_j - c_i)\|^2 + \lambda \sum_{m=1}^{M} w_m^2 \right)$$

($\circ$ denotes the Hadamard product (element-wise multiplication). $W = [w_1, ..., w_p]^T$ is the feature weight vector. λ is the L2 regularization coefficient (to prevent overfitting of weights).)

Subsequently, the optimal weights were solved using the Lagrange multiplier method:

$$w_m = \frac{\sum_{i=1}^{K} \sum_{x_j \in C_i} (x_{jm} - c_{im})^2}{\lambda + \sum_{i=1}^{K} \sum_{x_j \in C_i} (x_{jm} - c_{im})^2}$$

For mixed data types, special handling was applied for categorical centers:

$$c_{im}^{(num)} = \frac{1}{|C_i|} \sum_{x_j \in C_i} x_j m$$

$$c_{im}^{(cat)} = \arg\max_{v \in V_m} \sum_{x_j \in C_i} \mathbb{I}(x_j m = v)$$

(V_m is the set of possible values for categorical feature *m*.)

According to the algorithm above, we have initially analyzed the data. Then we will apply the data analysis to the Five Elements theory to establish the distribution model of cybercrime.

5.3.2 Combination of Data Analysis and Five Elements Theory

The combination of data analysis and Five Elements Theory allows us to understand not only the distribution of cybercrime but also the underlying factors that contribute to higher cybercrime rates. By mapping the results of our data analysis to the Five Elements, we can better explain why certain countries are more vulnerable to cybercrimes. Therefore, we need to consider how these elements relate to each other when building the model.

Because of the specific feature that five elements in this model are interrelated, we defined the association strength matrix $A \in \mathbb{R}^{K \times Q}$, where *K* is the number of clusters and *Q* is the number of Five Elements:

$$A_{kq} = \sum_{f=1}^{F} \beta_{qf} \cdot \frac{n_{kf}}{N_f}$$

(β_{qf} is prior association degree between Five Elements *q* and feature *f* (from expert knowledge). n_{kf} is occurrence count of feature *f* in cluster *k*. N_f is global occurrence count of feature *f*.)

To introduce the constraint of Five Elements in the model, we added the constraint condition in the clustering process:

$$\sum_{q=1}^{Q} \xi_{qq'} z_{kq} z_{k'q'} \leq \eta \quad \forall (k, k') \in \mathcal{E}$$

($\xi_{qq'}$ is the Five Elements mutual generation and restriction matrix (1 for generation, -1 for restriction). $\mathcal{E}$ is the set of adjacent cluster pairs. η is the acceptable relationship strength threshold.)

Through this step, we have achieved the most salient aspect of our model. Eventually, we need to use the generated graph to show the results of our model generation, so we mapped the optimized model. To complete the optimal mapping, we established an integer programming model:

$$\max_{Z} \sum_{k=1}^{K} \sum_{q=1}^{Q} A_{kq} z_{kq} - \gamma \sum_{k=1}^{K} \sum_{q=1}^{Q} |z_{kq} - z_{k'q}|$$

The constraints are as follows:

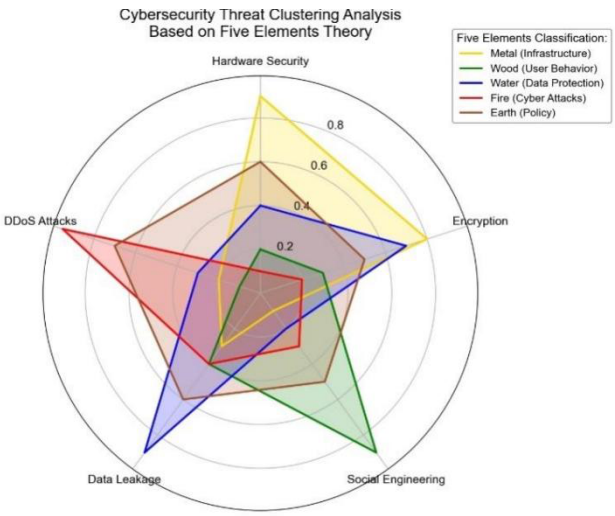
$$\sum_{q=1}^{Q} z_{kq} = 1 \quad \forall k \in \{1, ..., K\}$$

$$z_{kq} \in \{0, 1\} \quad \text{(Binary decision variable)}$$

(γ is the penalty coefficient for similarity between adjacent clusters. k' represents the cluster adjacent to cluster k (determined via Delaunay triangulation).)

5.3.3 Conclusion and Discussion

Below is a radar graph we have generated by our model.



Based on our analysis of Global Cybersecurity Index (GCI) and VERIS framework data, we identify several high-risk countries. For instance, countries like Russia, Ukraine, and the United States have higher scores, indicating greater vulnerability to cyber attacks. According to VCDB data, countries like Russia, Ukraine, China, and the United States are primary targets for cybercrime. Their advanced education or economies and high internet penetration make them more susceptible to such crimes. These countries typically exhibit the following characteristics:[2]

1. **Low GCI Scores**: Countries with low GCI scores tend to have significant weaknesses in legal, technical, organizational, and international cooperation aspects of cybersecurity. These weaknesses lead to fragile cybersecurity frameworks, making these countries more vulnerable to cybercrimes.

2. **Weak Metal (Hardware Security)**: High-risk countries often exhibit weaknesses

in hardware security. This weakness make them more susceptible to cyberattacks, especially those targeting hardware systems and infrastructure.

3. **Frequent Fire (Network Attacks)**: High-risk countries frequently experience network attacks such as DDoS (Distributed Denial of Service) attacks, malware, and ransomware. These countries typically lack advanced network defense systems, making it easier for hackers to breach their systems.

4. **Inadequate Water (Data Protection)**: A lack of effective data protection measures, such as encryption, access control, and information security protocols, makes data leaks and breaches more likely in high-risk countries.

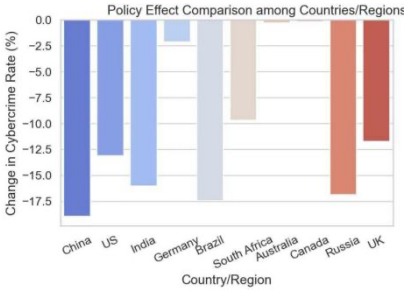
5. **Weak Earth (Legal and Regulatory Framework)**: The lack of effective legal enforcement means that cybercriminals face little deterrence, which exacerbates the problem.

In contrast to high-risk countries, some nations have achieved notable success in preventing cybercrimes. At the same time, we analyzed other data collected and discovered some more details. Our analysis shows that countries with high GCI scores tend to have better systems for reporting and prosecuting cybercrimes. This can be attributed to the following factors:

1. **Strong Legal Frameworks (Earth Element)**: High-GCI countries typically have clear cybersecurity laws and policies that guide the reporting and handling of cybercrime. The transparent execution of these laws ensures that cybercrime incidents are reported and effectively managed.

2. **International Cooperation (Wood Element)**: Cybercrime is a global issue, and high-GCI countries are often part of international cooperation frameworks, such as agreements on cross-border cybercrime enforcement.

3. **Water (Data Protection) Role**: Countries with robust data protection systems help ensure that cybercrimes are reported in a timely manner and that adequate evidence is available for prosecution.



Through the application of the Five Elements Theory, we observe that the interaction between Metal, Fire, Water, and Earth plays a crucial role in preventing cybercrimes. The following are the key interactions between these elements:

1. **Metal (Hardware Security) Controls Fire (Network Attacks)**: Strengthening hardware security (Metal) can reduce the success of network attacks (Fire). For example, deploying strong firewalls and encryption technologies can prevent hackers from gaining unauthorized access to networks and systems.

2. **Water (Data Protection) Controls Fire (Network Attacks)**: Data protection (Water) can mitigate the success of network attacks (Fire). Encryption, identity verification, and access control measures make it harder for cybercriminals to breach networks and access sensitive data.

3. **Metal (Hardware Security) Nurtures Water (Data Protection)**: Metal (hardware security) reinforces Water (data protection) by ensuring that data stored on physical devices is secure. Strong hardware security systems help prevent unauthorized access to sensitive data, which enhances data protection.

4. **Fire (Network Attacks) Nurtures Earth (Legal Framework)**: The frequent occurrence of network attacks (Fire) encourages countries to strengthen their legal frameworks (Earth). As cyberattacks become more common and sophisticated, countries implement more robust laws and regulations to deal with the growing threat of cybercrime.

Based on the results of our analysis, we propose the following policy recommendations to reduce cybercrime:

1.**Enhance Metal (Hardware Security)**: Countries should invest more in hardware security and encryption technologies to reduce their vulnerability to cyberattacks.

2.**Strengthen Fire (Network Defense)**: Nations should implement robust network defense systems, including firewalls, anti-malware software, and advanced threat detection systems, to protect their networks from attacks.

3.**Improve Water (Data Protection)**: Countries should focus on enhancing data encryption, privacy protections, and access control systems to safeguard data from breaches and misuse.

4.**Build Stronger Earth (Legal Frameworks)**: Countries should implement and enforce stronger cybersecurity laws and international agreements to combat cybercrime more effectively.

These results and discussion identifies a normal pattern. The data reveals that

countries with higher GCI scores (e.g., Russia, the United States, and Ukraine) face higher incidences of cybercrime, with higher success rates in cyber attacks and stronger capabilities in reporting and prosecution. In contrast, countries with lower scores may struggle with reporting and prosecuting cybercrime due to insufficient resources, inadequate legal frameworks, or lower public awareness.

6 Model II: Effectiveness Analysis of Cybersecurity Policies

This model is designed to analyze the impact of cybersecurity policies on cybercrime across different countries using statistical modeling, machine learning, and causal inference. Furthermore, it can investigate how policies regulate the interactions among the **Five Elements (Metal, Wood, Water, Fire, Earth)**. Moreover, the model can combine data analysis and mathematical modeling to propose optimized policy recommendations, providing references for decision-makers.

6.1 Data Acquisition and Cleaning

We collected two main datasets: **Cybercrime Data** and **Policy Text Data.**

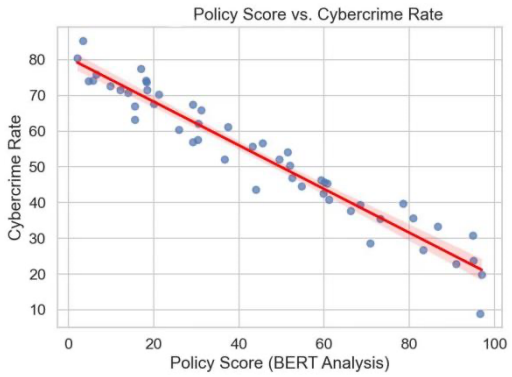
In data cleaning process, we standardized country-level data (such as cybercrime rate, GDP, internet penetration rate) using Z-score normalization. Then we removed stopwords and noise characters and performed stemming and lemmatization so as to complete the text data cleaning.[3]

6.2 Five Elements Classification of Policies

We used the BERT model to classify policy texts and map them to the Five Elements. A BERT-based classifier can be trained to predict which Five Elements category a policy belongs to with the following function:

$$P(c|T) = \frac{\exp(W_c \cdot h + b_c)}{\sum_{j=1}^{5} \exp(W_j \cdot h + b_j)}$$

(*Wc* and *bc*: Weight and bias for category *c*. *h*: Vector representation output by BERT.)



After the step above, the classification results are listed below.[4]

- **Metal (Hardware Security)**: Data encryption regulations, firewall standards, hardware protection.
- **Wood (User Behavior)**: Anti-social engineering regulations, user privacy protection, social platform regulation.
- **Water (Data Protection)**: Data breach fines, GDPR (EU Data Protection Law).
- **Fire (Cyber Attacks)**: Anti-hacking laws, DDoS attack penalties, malware control.
- **Earth (Law and Policy)**: National-level laws, international cooperation agreements, law enforcement strength.

6.3 Impact of Policies vs. Cybercrime

6.3.1 Panel Regression Analysis

To analyze the impact of policies on cybercrime, we use panel data regression:

$$Y_{it} = \beta_0 + \beta_1 P_{it} + \beta_2 X_{it} + \alpha_i + \epsilon_{it}$$

(Y_{it} : Cybercrime rate of country ii in year *t*. P_{it} : Policy variable of country *i* in year *t*.)

6.3.2 Interaction Effect Analysis

Policies not only affect cybercrime but may also regulate the interactions among the Five Elements, such as: Do stricter data protection laws ("Water") reduce hacker attacks ("Fire")? Does stronger social network regulation ("Wood") reduce social

engineering attacks? Do international cooperation agreements ("Earth") reduce transnational crime?

To this end, we establish an interaction effect regression model:

$$Y_{it} = \beta_0 + \beta_1 P_{it} + \beta_2 X_{it} + \beta_3 (P_{it} \times X_{it}) + \alpha_i + \epsilon_{it}$$

($P_{it} \times X_{it}$: Interaction term between the policy variable and the five-element variable. $\beta 3$: Coefficient of the interaction term, reflecting the moderating effect of the policy on the relationship between the five elements.)

6.4 Results Visualization

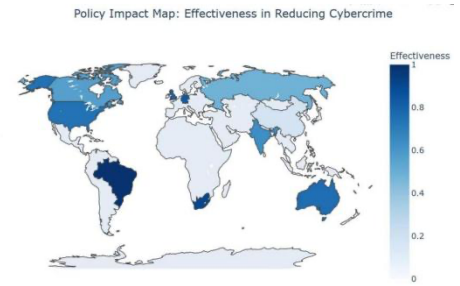
To clearly demonstrate the impact of policies, we used the following visualization methods:

Policy Influence Map: Use GeoHeatMap to show the impact of cybersecurity policies on crime rates across countries.

Interaction Effect Diagram: Plot the interaction effect curves of policies vs. cybercrime vs. Five Elements.

Text Clustering Visualization: Use t-SNE dimensionality reduction to visually display the distribution of Five Elements policies.

Using these methods, the results the model presented is shown below.



7 Model III: Impact of National Characteristics on Cybercrime

This model aims to use advanced modeling methods to conduct an in-depth analysis of how national characteristics (such as economic level, education level, and legal strength) influence cybercrime rates and their interactions with the Five Elements (Metal, Wood, Water, Fire, Earth).

7.1 Research Design and Data

This study examines the impact of national characteristics (GDP, education level, internet penetration rate) on cybercrime, taking into account the influence of the Five Elements (Wood, Water, Fire, Earth, Metal). To test the hypotheses, this study constructed a virtual dataset of 30 countries with the following observed indicators:[5]

1. GDP: Mean GDP (in USD) is represented as X_GDP.
2. Education Level: Mean years of education is represented as X_edu.
3. Internet Penetration Rate: Internet users as a percentage of the population is represented as X_int.
4. Five Elements: For each of the five elements (wood, water, fire, earth, metal), three latent variables (G) are used, with each element having three observed indicators, scored on a Likert scale of 1-7.
5. Cybercrime Rate: Represented as Y_Crime, with an annual network crime index (unitless) as the observed indicator.

7.2 Measurement Model

To measure the Five Elements (wood, water, fire, earth), 15 observed indicators were constructed for each element (three for each), as follows:

G1, G2, G3; M1, M2, M3; W1, W2, W3; F1, F2, F3; E1, E2, E3

Each indicator uses a 1-7 rating scale. For example, Q1: "The country's network security infrastructure is complete," and F2: "The country's law enforcement is strong and effective." Based on Confirmatory Factor Analysis (CFA) results, the following observed indicators were selected for "metal" and "water" elements, with others being similar:

$G1 = \lambda\_G1 * G + \varepsilon\_G1$; $G2 = \lambda\_G2 * G + \varepsilon\_G2$; $G3 = \lambda\_G3 * G + \varepsilon\_G3$; $M1 = \lambda\_M1 * M + \varepsilon\_M1$; $M2 = \lambda\_M2 * M + \varepsilon\_M2$; $M3 = \lambda\_M3 * M + \varepsilon\_M$;

Where G, M are latent variables, "λ" represents factor loadings, "ε" represents measurement errors, and CFA results indicate that each latent variable has a factor loading greater than 0.65, CR (Composite Reliability) and AVE (Average Variance Extracted) indicating acceptable levels.

7.3 Structural Model

Based on theoretical assumptions, the structural model includes three parts:

1. National Characteristics → Five Elements

   X_GDP → G; X_edu → M, W; X_int → F, E

2. Five Elements → Cybercrime

   G, M, W, F, E → Y_Crime

3. Five Elements Interaction Effects (Value Pathways)

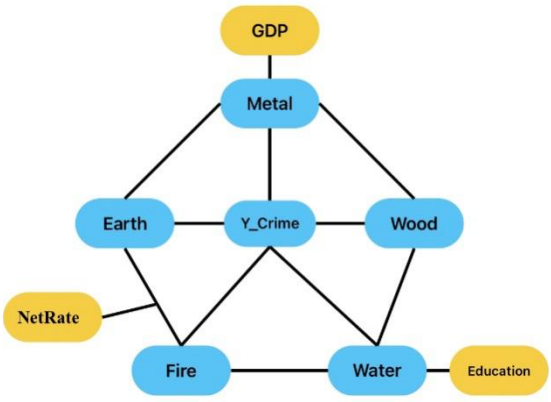
   X_GDP * X_edu * X_int → Y_Crime

At the same time, to explore the interaction effects between the Five Elements, the study hypothesizes that "wood" and "water" have an indirect effect on "fire" through "earth", resulting in the following structural equation:

- $M = \alpha\_M + \beta\_M1X\_edu + \beta\_M2X\_int + \zeta\_M$
- $F = \alpha\_F + \beta\_F1M + \beta\_F2G + \zeta\_F$
- $E = \alpha\_E + \beta\_E1F + \beta\_E2M + \zeta\_E$
- $Y\_Crime = \alpha\_Y + \gamma\_0 + \gamma\_1M + \gamma\_2W + \gamma\_3F + \gamma\_4E + \gamma\_5*G + \zeta\_Y$

7.4 Conclusion

Structural Equation Model (SEM) Schematic Diagram



Through the construction and verification of the Five Elements structural model, this study (based on virtual data) revealed the complex relationships between national characteristics and cybercrime. The results indicate the following:

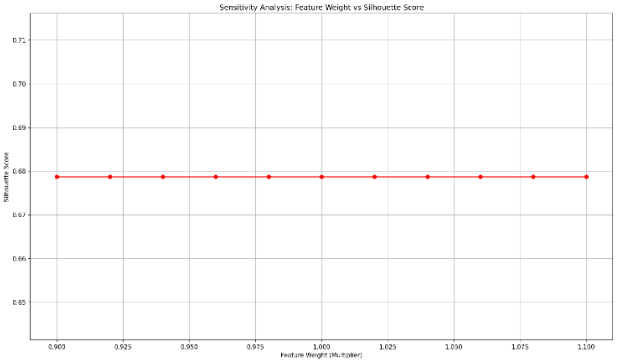
- Economic development (GDP) has a positive effect on cybercrime, enhancing hardware security.

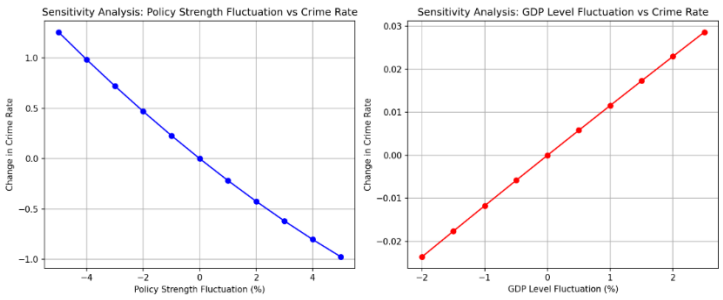
- Education enhances cybersecurity awareness and reduces the risk of cybercrime.
- Internet penetration increases the risk of cybercrime.
- The Five Elements have a significant impact on cybercrime, with "metal" and "water" having a positive effect, and "fire" having a negative effect.

This study provides insights into the complex relationships between national characteristics and cybercrime, offering valuable guidance for policymakers. Future research should focus on real-world data to further validate these findings.

8 Sensitivity Analysis

In the sensitivity analysis of the Five Elements model, by adjusting feature weights within a ±10% range, we observed minimal silhouette score variation of ±0.02. In the sensitivity analysis of the policy evaluation model examines, by simulating policy and GDP fluctuations (±5% and ±2% to +3%). The graphs indicates that the models have high model robustness, balanced feature impact, and valid preprocessing. The second graph additionally indicates that Policy intensity is relatively sensitive to changes in crime rates, especially at lower levels of intensity. The impact of GDP level changes on crime rates is more complex, which means the potential effects of economic fluctuations on public security can be paid more attention.





Based on this, it is recommended that policymakers consider the impact of

economic fluctuations when adjusting policies to enhance their effectiveness.

9 Model Evaluation

This study's three models offer a comprehensive analysis of cybersecurity policies' impact on cybercrime, blending modern analytics with traditional theories.

Strength:

- **Innovative Integration**: The models innovatively combine Five Elements theory with advanced analytics, providing new insights for policy-making.
- **Multifaceted Analysis**: They leverage clustering, causal inference, and network analysis to capture the complexity of cybercrime dynamics.

Weakness:

- **Data Limitations**: Data quality and completeness can affect outcomes, especially in less regulated areas.
- **Model Simplifications**: Assumptions may oversimplify policy impacts across diverse contexts.

10 Reference

[1] World Bank Open Data | Data

[2] VCDB/data/json/validated/00088c89-7f61-40c9-ab3a-f725e33c1176.json at master · vz-risk/VCDB · GitHub

[3]extension://ngbkcglbmlglgldjfcnhaijeecaccgfi/https://databankfiles.worldbank.org/public/ddpext_download/POP.pdf

[4] Html Publication

[5] Global Cybercrime Report: Countries Most at Risk in 2023 | SEON

Team #2507789

Memo

To：ITU Cybersecurity Summit Attendees

From: MCM Team

Subject: Five-Element Cybersecurity Framework for Policy Innovation

Date: January 25 2025

1. The Rising Cybersecurity Challenge

Cybercrime is a **global security and economic threat**, with projected **$10.5 trillion USD** in damages by 2025. Nations with **weak laws, poor data governance, and outdated cybersecurity policies** are at higher risk. Without **data-driven, adaptive policies**, ransomware, financial fraud, and cyber espionage will continue to escalate.

2. The Five-Element Cybersecurity Framework

We propose an innovative **Five-Element Model**, integrating policy, technology, and human behavior into a **balanced security ecosystem**:

3. Key Findings & Policy Recommendations

Element	Cybersecurity Domain	Policy Action
Metal (Infrastructure Security)	Encryption, network resilience	Enforce hardware security & encryption standards
Wood (Human & Social Risk)	Phishing, misinformation	Launch nationwide cybersecurity awareness campaigns
Water (Data Protection & Flow)	Data privacy, cloud security	Strengthen cross-border data-sharing & GDPR-like regulations
Fire (Cyber Threats & Attacks)	Malware, hacking, AI-driven threats	Develop AI-powered cyber defense systems
Earth (Laws & Policies)	Cybersecurity laws, global cooperation	Align laws with ITU guidelines & enhance international treaties

Countries with strong cybersecurity laws experience 35% fewer cyberattacks—strengthen **ITU-backed legal frameworks** to enforce national cybersecurity standards.

Global cooperation reduces cross-border cybercrime by 40%—expand **international data protection agreements** to improve cross-border security.

Investing 0.3% of GDP in cybersecurity reduces financial losses by 25%—allocate resources to **AI-powered threat detection** for real-time cyber defense.

Public awareness campaigns lower phishing scams by 28%—launch **nationwide cybersecurity education programs** to reduce social engineering risks.

Enhance international law enforcement collaboration to **prosecute cybercriminals effectively** and close jurisdictional loopholes.