Problem Chosen	2025 MCM/ICM Summary Sheet	Team Control Number
F		2500434

Hello Summary!

INDEX

1 Introduction

1.1 Background

In the digital age, the speed and scale of global connectivity have reached unprecedented heights. However, with technological advancements, **cybercrime** has also become increasingly complex and diverse. These crimes pose significant threats and challenges to personal privacy, corporate assets, national security, and social stability. The transnational and covert nature of cybercrime makes it difficult to address effectively. Attackers often exploit legal differences and technical vulnerabilities across countries to evade accountability. Additionally, many businesses and institutions, concerned about their reputation and commercial interests, often choose **not to publicly report** cyberattacks, opting instead to pay ransoms or handle incidents privately. This further exacerbates the hidden nature of cybercrime. Developed countries, with their highly digitized economic and social structures, are often prime targets for cybercrime, while developing countries face their own unique challenges.

To address this global challenge, countries have introduced national cybersecurity **policies** aimed at enhancing their defensive capabilities through legal, technical, and organizational cooperation. The **effectiveness** of these policies varies significantly across nations, and these differences may be closely related to factors such as policy design, enforcement, technological infrastructure, education levels, economic development, and internet penetration rates.

In this context, understanding which factors make certain countries' cybersecurity policies more effective has become a critical issue. By analyzing the global distribution of cybercrime, national cybersecurity policies, and their outcomes, we can identify which policies and laws are particularly effective in preventing, prosecuting, and mitigating cybercrime. This data-driven analysis not only helps countries improve their cybersecurity policies but also provides valuable insights for global cybersecurity cooperation.

1.2 Restatement of the problem

We are required to identify patterns that can inform the data-driven development and refinement of national cybersecurity policies and laws, which focused on those that have demonstrated effectiveness. Our goal is to develop a theory explaining what constitutes a strong national cybersecurity policy and then support it with a data-driven analysis.

Several key aspects are listed below:

- Patterns in cybercrime distributed worldwide.
- Assessment to effectiveness of National Cybersecurity Policies.
- Correlation between national demographics and our distribution analysis.

1.3 Analysis of problems

We have divided each problem into several different steps:

1.3.1 Cybercrime distribution across the world

- Analyze the JSON files published on VCDB (the VERIS community database).

- Use the Global Cybersecurity Index (GCI) as the primary indicator to assess countries with disproportionately high levels of cybercrime.
- Group countries based on their implementation of similar policies over a period of time, and visually represent the distribution of cybercrime in each group using a 3D heatmap.

1.3.2 Effective policy or law analytical approach

- TODO

1.3.3 National demographics correlation

- TODO

2 Symbol and Assumptions

2.1 Symbol Description

Symbol	Description
D_i	Each data of the cybercrime distribution
y	Transformed value using $y = \log(1 + D_i)$.

Abbreviation	Full Form
GCI	Global Cybersecurity Index
VERIS	the Vocabulary for Event Recording and Incident Sharing
VCDB	the VERIS Community Database

2.2 Assumption

- Countries with a population below 5% are excluded from the consideration of cybercrime distribution because a small change of number could bring a significant difference to statistical analysis.
- In the statistical analysis of the global distribution of cybercrime, factors such as national population growth, internet access, wealth levels, and education levels are assumed to have no significant impact on the quantitative distribution of cybercrime incidents. This study hypothesizes that the distribution of cybercrime can be more intuitively understood by focusing solely on the number of incidents, independent of these socio-economic variables. This assumption is based on all available data recorded since the inception of cybercrime statistics, aiming to isolate the distribution patterns of cybercrime from other potential influencing factors.

3 The establishment and solution of problem 1 model

Despite the continuous evolution of national cybercrime since the inception of data collection, along with changes in policies, legal frameworks, and population demographics, we can create a global

cybercrime hotspot map by leveraging crime data recorded by VERIS over the years. This not only facilitates the analysis of cybercrime volumes by country but also allows for fitting the data against policy and population variables to assess their influence on cybercrime trends.

3.1 Cybercrime distribution across the globe

We made use of a world-wide map to represent all cybercrime occurred around the world. In the map, the color filled in each country represents the total number of cybercrime incidents recorded since the beginning of the statistics. The color gradient, ranging from dark blue to dark red, corresponds to eight severity levels (1 to 8). Countries marked in blue indicate a low frequency of cybercrime incidents, while those marked in red represent a high density of such incidents. For instance, the United States, where the VERIS concept was first proposed, has the highest number of recorded incidents (7,236), whereas many other countries have only 1 or 2 recorded incidents. To address this significant disparity in data distribution, we applied a logarithmic transformation to the data using the formula

$$y = \log(1 + D_i)$$

. This transformation was implemented using the function

$$np.log1p()$$

in Python to ensure computational precision and stability, particularly for small values. The final results are visualized in Figure 1.

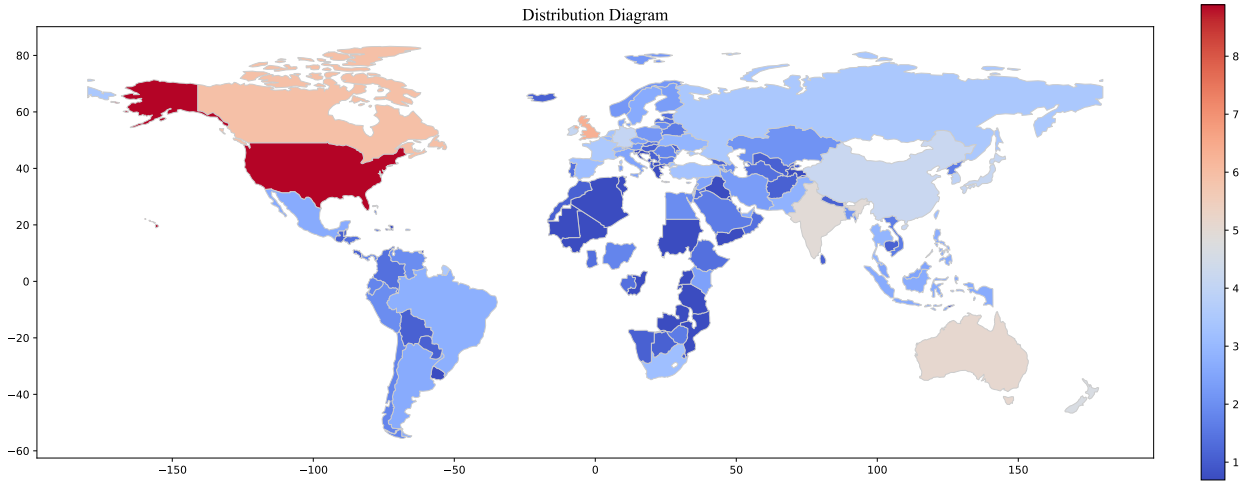


Figure 1: Crime distribution

3.2 High-prevalence regions

my figure?

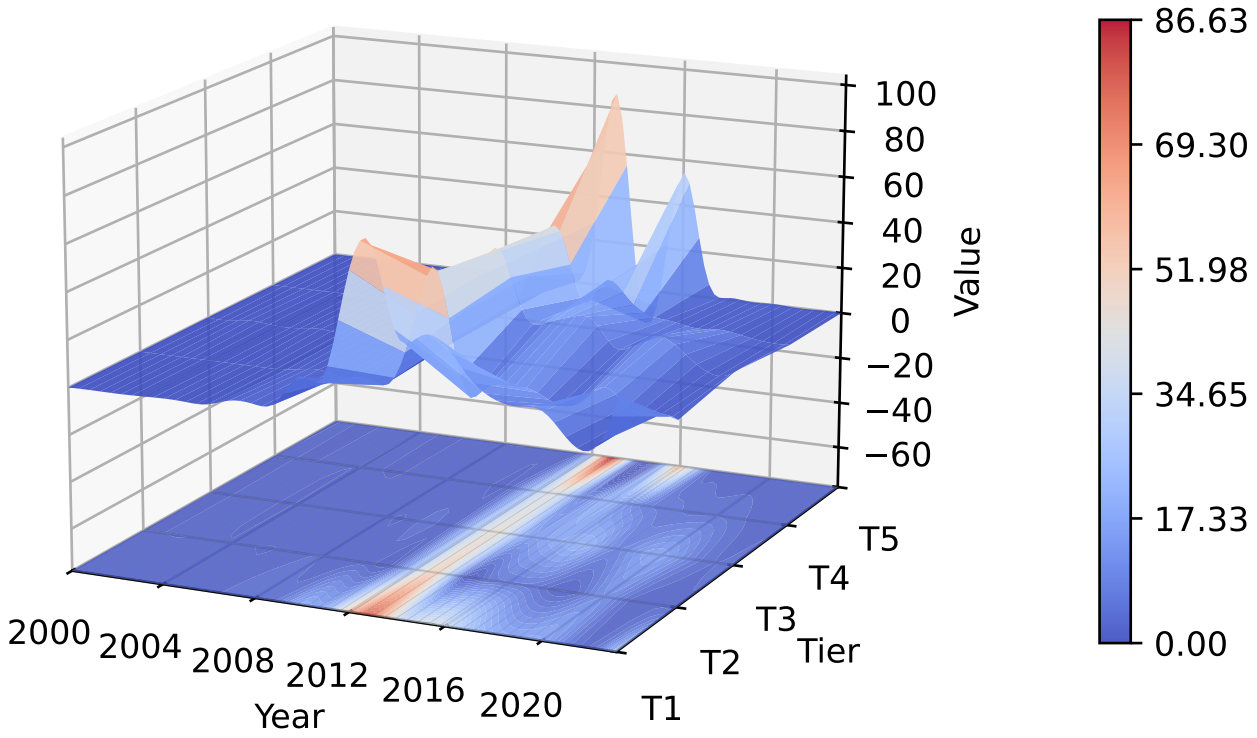


Figure 2: 3D with Spaced Projection

3.3 Other Cybercrime Incidents

Using additional data obtained from the VCDB, we constructed heatmaps on a global scale based on the number of successful cybercrimes, thwarted cybercrimes, and reported cybercrimes, respectively. Due to the disproportionately high volume of data from the United States, we applied the same logarithmic transformation ($y = \log(1 + D_i)$) as in Figure 1 for consistency, resulting in the three sub-figures presented in Figure 3.

In sub-figure (a), the number of successful attacks closely aligns with the total number of attacks in most countries. For instance, the United States recorded 7,189 successful attacks out of 7,236 total attacks, yielding a success rate of $\frac{7189}{7236} \approx 99.35\%$. Similarly, the United Kingdom reported 569 successful attacks out of 574 total attacks, with a success rate of $\frac{569}{574} \approx 99.13\%$.

In contrast, countries with lower attack volumes did not show significant differences between the total number of attacks and the number of successful attacks, indicating that almost every attempted attack was successful.

In sub-figure (b), only the United States and Canada reported thwarted attack cases, with 6 and 2 instances, respectively.

In sub-figure (c), the number of successfully reported attacks and the number of countries involved were significantly higher than in sub-figure (b). This suggests that while many attacks were successful, a portion of them were detected and reported.

4 The establishment and solution of problem 2 model

4.1 Shit, bro*2

5 The establishment and solution of problem 3 model

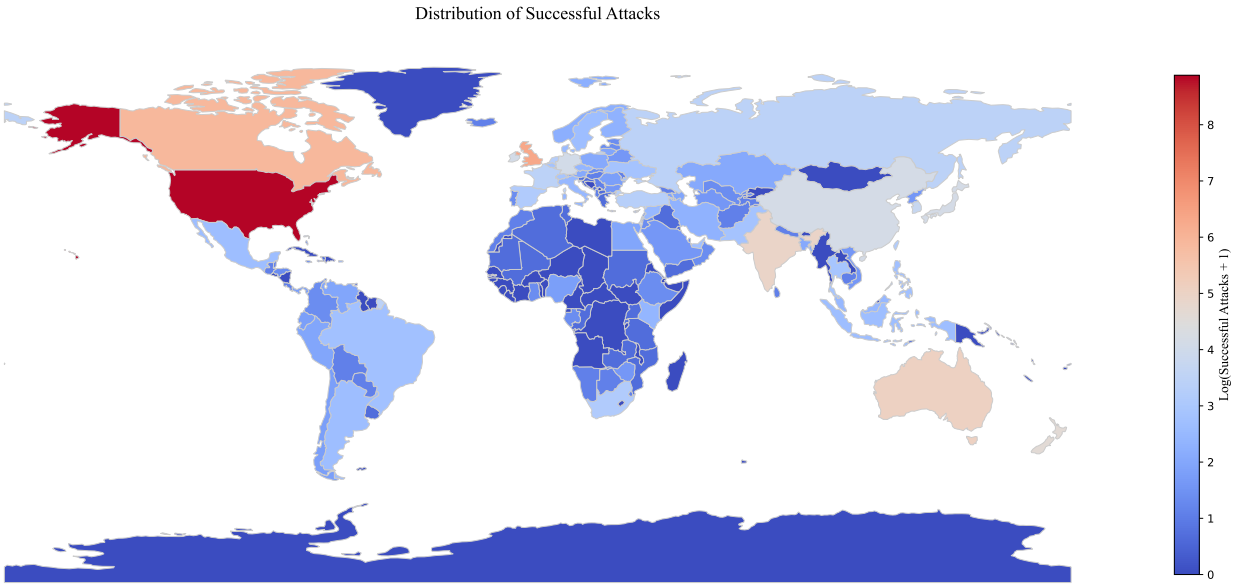
5.1 Shit, bro*3

6 Future expected data

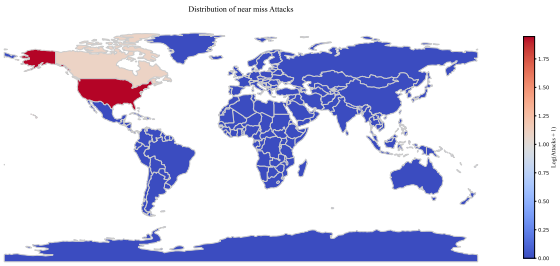
7 Advantages & Disadvantages

8 References

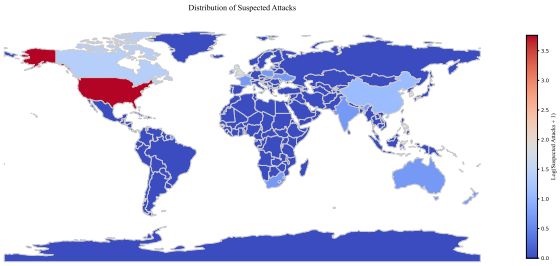
9 Appendix



(a) Successful Cybercrime Incidents



(b) Mitigated Cybercrime Attempts



(c) Reported Cybercrime Incidents

Figure 3: Other Cybercrime Incidents