Judges' Commentary: Cyber Strong

Luke Castle
Mathematics
North Carolina State University
Raleigh, NC

Phillipp Dau
Account Executive
north.io GmbH
Hamburg, Germany

Kira Graves
Director
Critical Thinking Enterprise
US Army Training and Doctrine Command
Leavenworth, KS

Bethany Kubik
Mathematics and Data Science
Duluth Public Schools
Duluth, MN

Jessica Libertini
Mathematical Sciences
US Military Academy
West Point, NY
jessica.libertini@westpoint.edu

Winnie Nakiyingi
Statistics
African Institute for Mathematical Sciences
Kigali, Rwanda

Eleanor Abernethy Ollhoff
Mathematics
Bonn, Germany

Troy Siemers
Applied Mathematics
Virginia Military Institute
Lexington, VA

Introduction

This year, the ICM® Policy Problem asked teams to develop a theory about the efficacy of national cybersecurity policies by analyzing data related to cybercrime and the introduction of policies. This problem is timely, since individual nations and the global community are seeking to improve their ability to deter, detect, and prosecute cybercrime during an era of global connectivity.

The UMAP Journal 46 (3) (2025) 303–328.

Judges' Criteria

This year's interdisciplinary panel of final judges consisted of mathematicians, scientists, and policy analysts from three continents. In opening discussions, the panelists shared what they had noticed in triage. Their observations led to the development of a set of important factors that were heavily considered in final judging. These factors included:

- Executive Summary
- Visualizations and Written Exposition
- Actionable Findings and Policy Memo
- Assumptions and Limitations
- Data Treatment and Data Processing
- Model Selection, Analytical Approach, and Connections between the Model and the Real World
- Appropriate Use of AI
- Creativity

We discuss each factor in more detail below, and in some categories, provide examples from team submissions.

Executive Summary

A previous commentary on the importance of the executive summary can be found in Libertini et al. [2018]. Most importantly, the executive summary is not simply an abstract! It must inspire the reader to want to read the rest of the paper. Within a single page, the executive summary should concisely describe the set-up/motivation of the problem, give a convincing overview of the team's methods, and provide the most important findings—not just as a list of numbers but as a recommendation to the reader of what is important.

We reproduce two examples of a good executive summary.

Executive Summary by Finalist Team 2505930 from Dalian University of Technology:

> The cross-regional and anonymous nature of cybercrime has exacerbated the vulnerability of individuals and organizations, while also complicating the formulation of effective legal and policy responses by governments. This study aims to develop a theoretical model to identify effective cybersecurity policies and laws. The research is divided into three main tasks:
>
> **Spatiotemporal Distribution Analysis of Cybercrime:** By analyzing **9,912** cybercrime reports from the VCDB database, we examine the spatiotemporal patterns of cybercrime incidents. We focus on the period from 2000 to 2023 (99.2% of the reports), and analyze nine representative countries and regions (90.49% of the reports). Using data on population, the

Global Cybersecurity Index, and cybercrime report frequency, we perform a **k-means** clustering analysis, categorizing these countries into three distinct groups based on economic conditions and internet environment characteristics: **technology-driven**, **economically transitioning**, and **densely populated**.

Evaluating the Effectiveness of Legal and Policy Frameworks: We apply an **ARIMA model** to compare the cybercrime incident rates post-enforcement in the nine major countries and regions with the predicted incident rates in the absence of these laws. By incorporating national characteristics and specific legal provisions, we summarize the effective and ineffective policy patterns for cybercrime governance in different national contexts. The results show **significant differences** in the effectiveness of legal and policy frameworks across various types of countries.

Enhancing and Validating the Theoretical Model Using Demographic Characteristics: To further refine and validate our theoretical model, we conduct a **stepwise linear regression** analysis using **19,927** data points related to factors such as internet infrastructure, basic education, and development, and their correlation with cybercrime frequency. These results validate the accuracy of our model and **show the root causes: Economy and Education**.

Finally, we perform sensitivity analysis to validate the proposed model. A memorandum detailing our data-driven findings is submitted to national leaders attending the upcoming ITU Cybersecurity Summit. The memorandum presents our conclusions: **maintaining long-term consistent cybercrime laws and policies**, and establishing targeted legal frameworks tailored to the **specific conditions of countries** with varying levels of economic development and internet infrastructure, is the most effective and necessary approach to combating cybercrime.

Executive Summary by Meritorious Team 2520503 from Ningbo University:

In recent years, the transnational and complex nature of cybercrime has posed serious challenges to global cybersecurity. To assist countries in enhancing their cybersecurity defense capabilities, ITU has actively developed international standards and assessment tools. Based on their standards, we analyze the effectiveness of national cybersecurity policies and laws through datadriven methods, aiming to provide a scientific basis for policy formulation and optimization.

To describe the distribution of cybercrime, we constructed a **National Cybercrime Index** using four indicators: incidence rate, success rate, reporting rate, and prosecution rate. We employed the **AHP** in conjunction with **the Entropy Weight Method** and **the Delphi Method** to calculate the coefficients for these four indicators, which were found to be **0.4**, **0.25**, **0.2**, and **0.15**, respectively. After substituting the specific data of various countries, we drew a distribution map. Upon comparison, we found that countries with advanced economic development and higher internet penetration rates are more likely to be high targets for cybercrime attacks. Moreover, countries with robust legal frameworks exhibit superior performance in terms of cybercrime reporting and prosecution rates.

To identify the effective categories of cybersecurity policies, we first employed **Natural Language Processing** to extract policy keywords from various countries. Then, we assessed the policy effectiveness from two dimensions: the impact on the home country and neighboring countries. For the former, we used the **PSM-DID method**, and for the latter, we applied **the Spatial Lag Model**. We categorized the effectiveness of specific policies based on these analyses. Our findings indicate that perfecting the legal framework and safeguarding critical information infrastructure are the most potent measures against cybercrime. Additionally, countries can enhance their cybersecurity capabilities through international cooperation and technological development, although the effectiveness of these measures is subject to a certain degree of latency.

To analyze the impact of demographic characteristics on cybercrime, we initially used the Pearson correlation coefficient to identify specific features with high correlation. Subsequently, we applied **the Regression-Forest Model**, which showed that for every one-unit increase in education years, the arrest rate would decrease by **4.25%** and the prosecution rate would decrease by **18.9%**. This indicates that higher education levels can significantly improve cybersecurity conditions. Additionally, for every 1% increase in internet access rate, the criminal offense rate would rise by **0.38%**; and for every 1% increase in the unemployment rate, the crime rate would increase by **0.72%**. Therefore, countries should also focus on strengthening cybersecurity legal oversight and alleviating socio-economic inequalities to reduce the risk of cybercrime.

Finally, a sensitivity analysis is performed. We find that as the fluctuations in the objective function value are rational as the parameters are modified, thereby substantiating the validity and reliability of the model. It is anticipated that our model will offer scientific support for the formulation and refinement of global cybersecurity policies, contributing to the establishment of a more secure cyberspace.

Visualizations and Written Exposition

In addition to a well-crafted executive summary, the judging panel appreciates papers that benefit from clear communication. Superior communication includes visualizations that help make a complex finding or approach more accessible, as well as strong expository writing that outlines modeling choices, their justifications, the findings, and the interpretation of the findings. With only 98 hours, it may seem natural to focus on the mathematics and the modeling; but if the explanation of the work is not clear, then great work can be overlooked. Therefore, it is important that teams consider not only how they will solve the problem but how they will convey their work.

Actionable Findings and Policy Memo

An important objective of the ICM Policy Problem is to challenge teams to move beyond the "what is the best thing to do" and to start to consider "is the proposed work possible?" and "who will do it?". It is important that the plan be actionable, meaning teams have identified the actions that some entity can control, not just the desired outcomes. For example, "reducing cyberincidents by 20%" is not an actionable plan but a goal. Some actions to support that goal might be passing new legislation or increasing funding for training to help citizens reduce their risk of falling prey to cyber scams. The judges appreciate when teams leverage existing measures of the efficacy of similar plans in other contexts to then draw inferences about how successful they could expect an action to be towards their target goals.

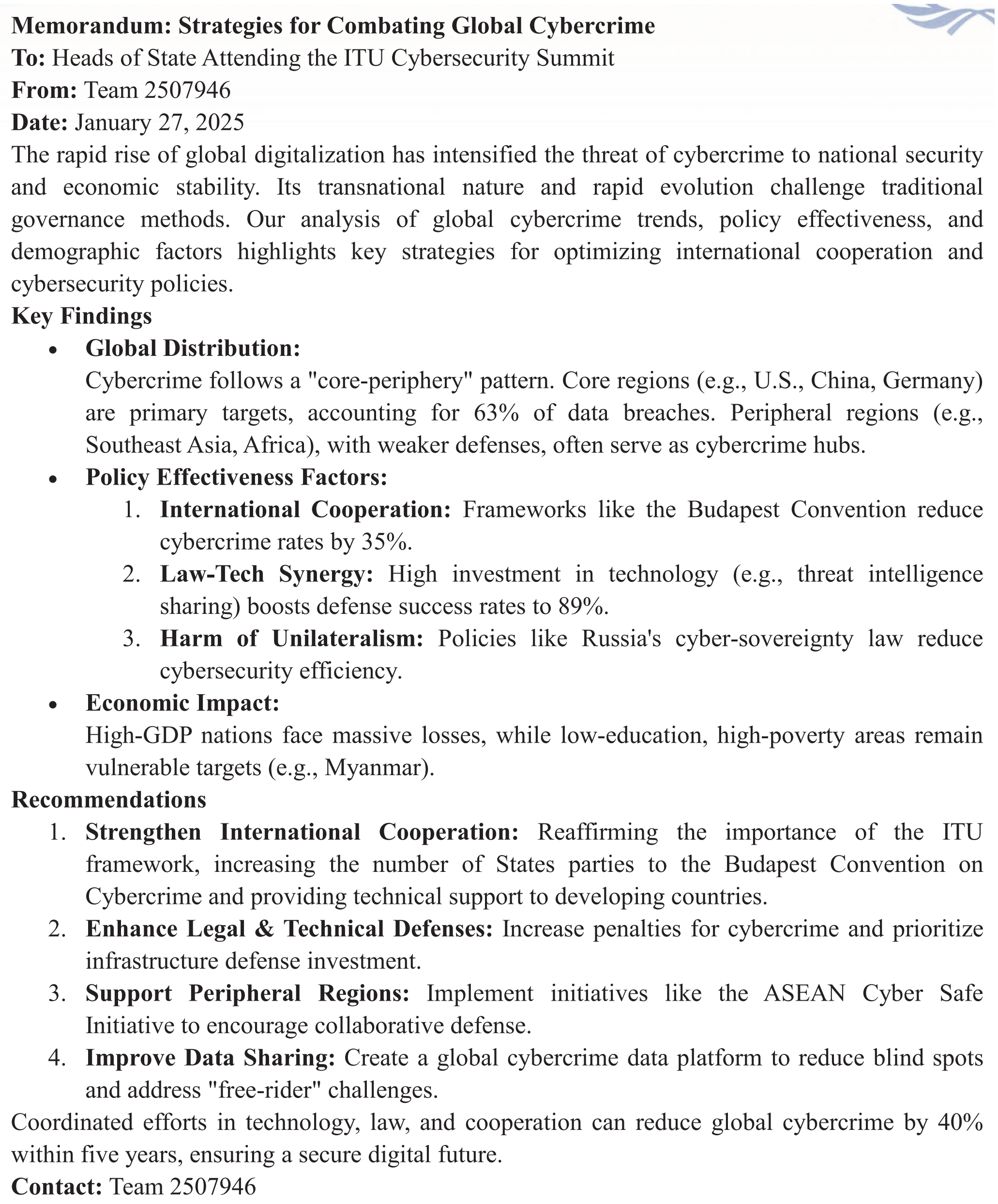
Much like the executive summary, a well-written one-page memo for policy makers is an essential part of the ICM Policy Problem and frames the key take-aways. The memo aims at translating the technical as well as mathematical modeling insights into actionable policies for a non-technical audience (e.g., national leaders, policy makers). It can be challenging for teams to draft a concise and straightforward memo. Often the memo is confused with a traditional abstract and focuses on the methods (how the tasks were addressed) rather than on data-driven and evidence-based policy recommendations—such as what insights were gleaned and what they mean, what action steps should be taken, and what outcomes might be expected based on whether those action steps are implemented.

A sound one-page memo is vital component to break down complex mathematical modeling and data analysis into digestible insights that inform policy-making and help derive actionable initiatives to tackle real-world problems.

The judging panel identified three good examples, each with different strengths:

- The memo by Finalist Team 2522757 from Shanghai International Studies University was very specific and well organized, with quantitative take-aways.
- Finalist Team 2507946 from Harbin Engineering University broke down guidance for geographically different countries in an easy-to-understand way.
- Outstanding Team 2517199 from the University of Electronic Science Technology of China focused on how quality of the data mattered for data-driven policies.

We exhibit these exemplary memos in **Figures 1–3** on pp. 308–310.



Memorandum: Strategies for Combating Global Cybercrime
To: Heads of State Attending the ITU Cybersecurity Summit
From: Team 2507946
Date: January 27, 2025

The rapid rise of global digitalization has intensified the threat of cybercrime to national security and economic stability. Its transnational nature and rapid evolution challenge traditional governance methods. Our analysis of global cybercrime trends, policy effectiveness, and demographic factors highlights key strategies for optimizing international cooperation and cybersecurity policies.

Key Findings

- **Global Distribution:**
  Cybercrime follows a "core-periphery" pattern. Core regions (e.g., U.S., China, Germany) are primary targets, accounting for 63% of data breaches. Peripheral regions (e.g., Southeast Asia, Africa), with weaker defenses, often serve as cybercrime hubs.
- **Policy Effectiveness Factors:**
  1. **International Cooperation:** Frameworks like the Budapest Convention reduce cybercrime rates by 35%.
  2. **Law-Tech Synergy:** High investment in technology (e.g., threat intelligence sharing) boosts defense success rates to 89%.
  3. **Harm of Unilateralism:** Policies like Russia's cyber-sovereignty law reduce cybersecurity efficiency.
- **Economic Impact:**
  High-GDP nations face massive losses, while low-education, high-poverty areas remain vulnerable targets (e.g., Myanmar).

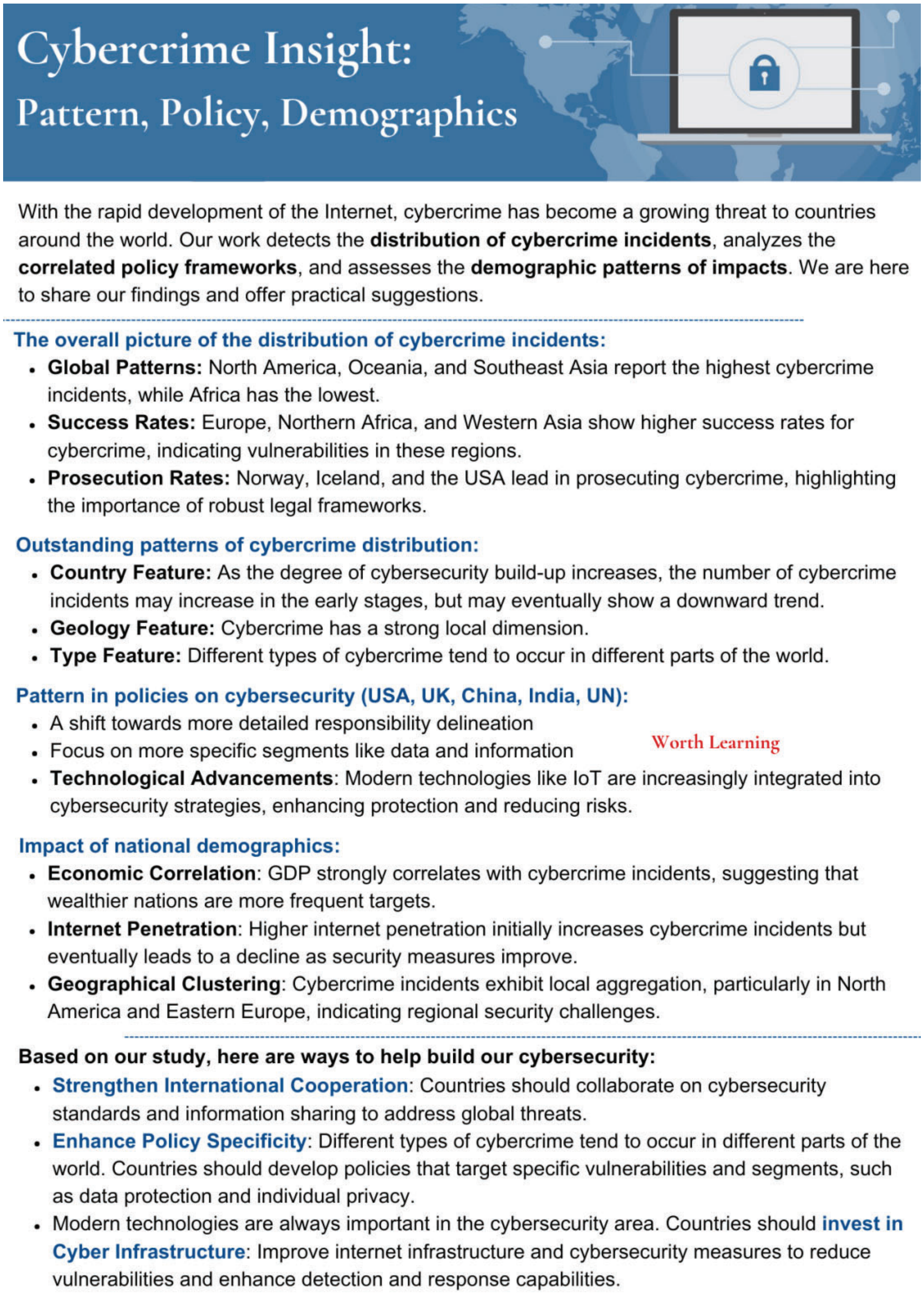
Recommendations

1. **Strengthen International Cooperation:** Reaffirming the importance of the ITU framework, increasing the number of States parties to the Budapest Convention on Cybercrime and providing technical support to developing countries.
2. **Enhance Legal & Technical Defenses:** Increase penalties for cybercrime and prioritize infrastructure defense investment.
3. **Support Peripheral Regions:** Implement initiatives like the ASEAN Cyber Safe Initiative to encourage collaborative defense.
4. **Improve Data Sharing:** Create a global cybercrime data platform to reduce blind spots and address "free-rider" challenges.

Coordinated efforts in technology, law, and cooperation can reduce global cybercrime by 40% within five years, ensuring a secure digital future.

Contact: Team 2507946

Figure 1. Memo by Finalist Team 2507946 from Harbin Engineering University. It provided actionable policy recommendations (i.e., “strengthen international cooperation, enhance legal & technical defenses, support peripheral regions, improve data sharing”). While we wished that the memo had been a bit more nuanced in its recommendations, it highlighted the effectiveness of different policies with clear statistical effects (e.g., that technology investments can increase defense success rates by up to 89%). The memo included the important information that policy makers need in order to understand the return on investment of different policies to select the best option and to guide an evidence-based decision making.



Cybercrime Insight:

Pattern, Policy, Demographics

With the rapid development of the Internet, cybercrime has become a growing threat to countries around the world. Our work detects the **distribution of cybercrime incidents**, analyzes the **correlated policy frameworks**, and assesses the **demographic patterns of impacts**. We are here to share our findings and offer practical suggestions.

The overall picture of the distribution of cybercrime incidents:

- **Global Patterns:** North America, Oceania, and Southeast Asia report the highest cybercrime incidents, while Africa has the lowest.
- **Success Rates:** Europe, Northern Africa, and Western Asia show higher success rates for cybercrime, indicating vulnerabilities in these regions.
- **Prosecution Rates:** Norway, Iceland, and the USA lead in prosecuting cybercrime, highlighting the importance of robust legal frameworks.

Outstanding patterns of cybercrime distribution:

- **Country Feature:** As the degree of cybersecurity build-up increases, the number of cybercrime incidents may increase in the early stages, but may eventually show a downward trend.
- **Geology Feature:** Cybercrime has a strong local dimension.
- **Type Feature:** Different types of cybercrime tend to occur in different parts of the world.

Pattern in policies on cybersecurity (USA, UK, China, India, UN):

- A shift towards more detailed responsibility delineation
- Focus on more specific segments like data and information

Worth Learning

- **Technological Advancements**: Modern technologies like IoT are increasingly integrated into cybersecurity strategies, enhancing protection and reducing risks.

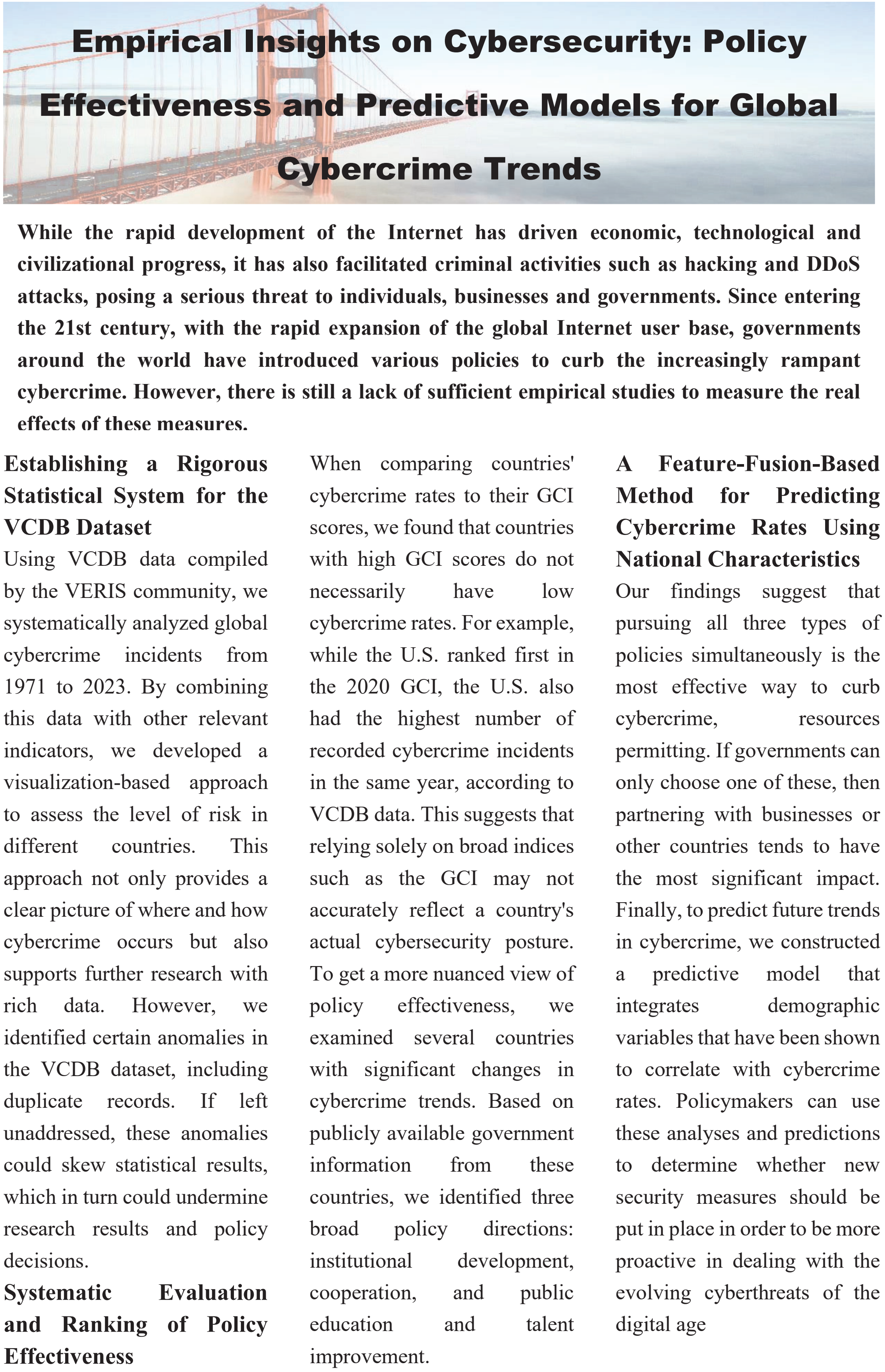
Impact of national demographics:

- **Economic Correlation**: GDP strongly correlates with cybercrime incidents, suggesting that wealthier nations are more frequent targets.
- **Internet Penetration**: Higher internet penetration initially increases cybercrime incidents but eventually leads to a decline as security measures improve.
- **Geographical Clustering**: Cybercrime incidents exhibit local aggregation, particularly in North America and Eastern Europe, indicating regional security challenges.

Based on our study, here are ways to help build our cybersecurity:

- **Strengthen International Cooperation**: Countries should collaborate on cybersecurity standards and information sharing to address global threats.
- **Enhance Policy Specificity**: Different types of cybercrime tend to occur in different parts of the world. Countries should develop policies that target specific vulnerabilities and segments, such as data protection and individual privacy.
- Modern technologies are always important in the cybersecurity area. Countries should **invest in Cyber Infrastructure**: Improve internet infrastructure and cybersecurity measures to reduce vulnerabilities and enhance detection and response capabilities.

Figure 2. Memo by Finalist Team 2522757 from Shanghai International Studies University. A major judging criterion is that submissions reflect on the practical application of the modeling insights. This clearly structured memo highlighted both the patterns in the distribution of cybercrime as well as the patterns in cybersecurity policies around the globe. While the policy recommendations remained rather broad, the memo reflected on the geographic differences in the prevalent types of crime. We appreciated how this team's memo focused on policies that were targeted to specific local challenges as well as regional conditions, as opposed to one-size-fits-all generic initiatives.



Empirical Insights on Cybersecurity: Policy Effectiveness and Predictive Models for Global Cybercrime Trends

While the rapid development of the Internet has driven economic, technological and civilizational progress, it has also facilitated criminal activities such as hacking and DDoS attacks, posing a serious threat to individuals, businesses and governments. Since entering the 21st century, with the rapid expansion of the global Internet user base, governments around the world have introduced various policies to curb the increasingly rampant cybercrime. However, there is still a lack of sufficient empirical studies to measure the real effects of these measures.

Establishing a Rigorous Statistical System for the VCDB Dataset

Using VCDB data compiled by the VERIS community, we systematically analyzed global cybercrime incidents from 1971 to 2023. By combining this data with other relevant indicators, we developed a visualization-based approach to assess the level of risk in different countries. This approach not only provides a clear picture of where and how cybercrime occurs but also supports further research with rich data. However, we identified certain anomalies in the VCDB dataset, including duplicate records. If left unaddressed, these anomalies could skew statistical results, which in turn could undermine research results and policy decisions.

Systematic Evaluation and Ranking of Policy Effectiveness

When comparing countries' cybercrime rates to their GCI scores, we found that countries with high GCI scores do not necessarily have low cybercrime rates. For example, while the U.S. ranked first in the 2020 GCI, the U.S. also had the highest number of recorded cybercrime incidents in the same year, according to VCDB data. This suggests that relying solely on broad indices such as the GCI may not accurately reflect a country's actual cybersecurity posture. To get a more nuanced view of policy effectiveness, we examined several countries with significant changes in cybercrime trends. Based on publicly available government information from these countries, we identified three broad policy directions: institutional development, cooperation, and public education and talent improvement.

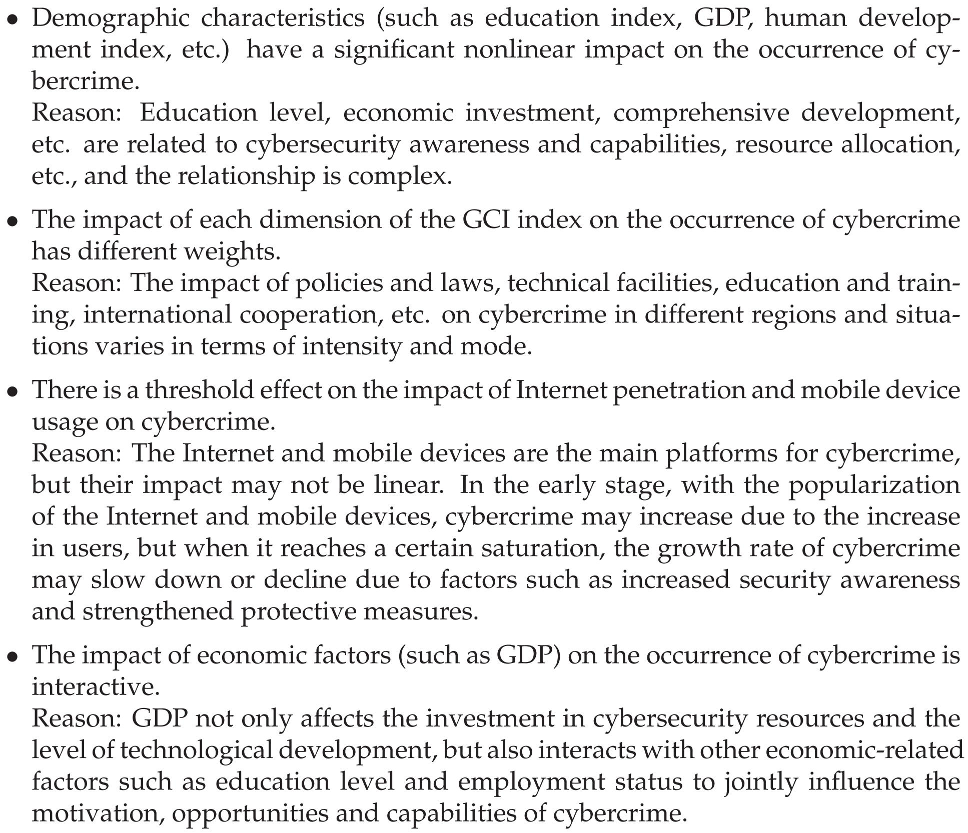
A Feature-Fusion-Based Method for Predicting Cybercrime Rates Using National Characteristics

Our findings suggest that pursuing all three types of policies simultaneously is the most effective way to curb cybercrime, resources permitting. If governments can only choose one of these, then partnering with businesses or other countries tends to have the most significant impact. Finally, to predict future trends in cybercrime, we constructed a predictive model that integrates demographic variables that have been shown to correlate with cybercrime rates. Policymakers can use these analyses and predictions to determine whether new security measures should be put in place in order to be more proactive in dealing with the evolving cyberthreats of the digital age

Figure 3. Memo by Outstanding Team 2517199 from the University of Electronic Science Technology of China. Data-driven decision making requires good and reliable data. The memo focused on data integrity and highlighted potential limitations of the VERIS Community Database (VCDB). Anomalies (e.g., duplicate data records) found were discussed in the memo. This is a great example of how important rigorous data collection and validation are for evidence-based policy making.

Assumptions and Limitations

Making assumptions is key to solving any modeling problem, and it involves an intentional balance between creating a model that is usable (sufficiently simplified to be solvable) and a model that is useful (sufficiently complex that the problem is not assumed away). For each assumption that is made, teams should be able to justify both (a) why the assumption is necessary for the model, and (b) why the assumption is reasonable. The submission from Outstanding Team 2504223 from Xi'an University of Technology addressed their assumptions well, as shown in **Figure 4**.

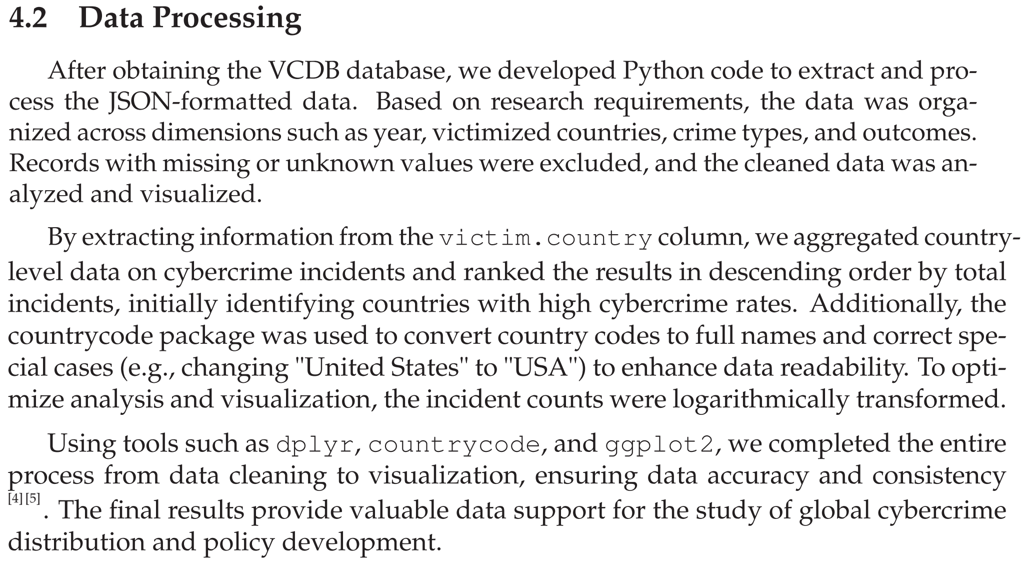


- Demographic characteristics (such as education index, GDP, human development index, etc.) have a significant nonlinear impact on the occurrence of cybercrime.
  Reason: Education level, economic investment, comprehensive development, etc. are related to cybersecurity awareness and capabilities, resource allocation, etc., and the relationship is complex.
- The impact of each dimension of the GCI index on the occurrence of cybercrime has different weights.
  Reason: The impact of policies and laws, technical facilities, education and training, international cooperation, etc. on cybercrime in different regions and situations varies in terms of intensity and mode.
- There is a threshold effect on the impact of Internet penetration and mobile device usage on cybercrime.
  Reason: The Internet and mobile devices are the main platforms for cybercrime, but their impact may not be linear. In the early stage, with the popularization of the Internet and mobile devices, cybercrime may increase due to the increase in users, but when it reaches a certain saturation, the growth rate of cybercrime may slow down or decline due to factors such as increased security awareness and strengthened protective measures.
- The impact of economic factors (such as GDP) on the occurrence of cybercrime is interactive.
  Reason: GDP not only affects the investment in cybersecurity resources and the level of technological development, but also interacts with other economic-related factors such as education level and employment status to jointly influence the motivation, opportunities and capabilities of cybercrime.

Figure 4. Assumptions and justifications by Outstanding Team 2504223 from Xi'an University of Technology.

Data Treatment and Data Processing

This year's problem required teams to identify and harvest their own data. Deciding what data to use, how to clean it, and how use it were discriminators in final judging. Many papers did pieces of this well, although some teams did a better job explaining their work than others. Outstanding Team 2521039 from China Agricultural University did an excellent job of discussing their data processing, providing transparent documentation of their use of Python and their selection of Python packages for both processing and visualization. This documentation, shown in **Figure 5**, made their work easy to follow and replicate.



4.2 Data Processing

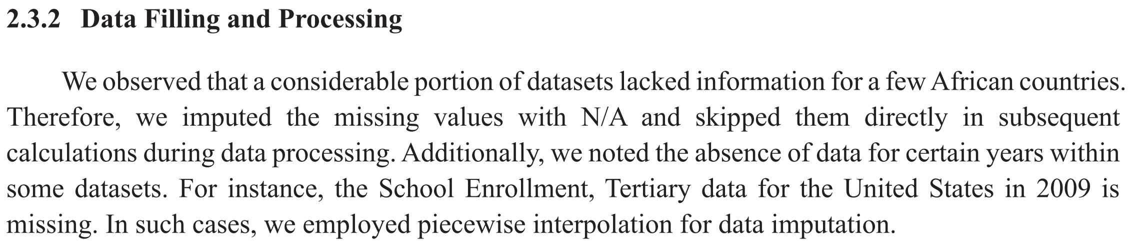
After obtaining the VCDB database, we developed Python code to extract and process the JSON-formatted data. Based on research requirements, the data was organized across dimensions such as year, victimized countries, crime types, and outcomes. Records with missing or unknown values were excluded, and the cleaned data was analyzed and visualized.

By extracting information from the `victim.country` column, we aggregated country-level data on cybercrime incidents and ranked the results in descending order by total incidents, initially identifying countries with high cybercrime rates. Additionally, the countrycode package was used to convert country codes to full names and correct special cases (e.g., changing "United States" to "USA") to enhance data readability. To optimize analysis and visualization, the incident counts were logarithmically transformed.

Using tools such as `dplyr`, `countrycode`, and `ggplot2`, we completed the entire process from data cleaning to visualization, ensuring data accuracy and consistency [4][5]. The final results provide valuable data support for the study of global cybercrime distribution and policy development.

Figure 5. Explanation of data treatment approach by Outstanding Team 2521039 from China Agricultural University.

Similarly, Finalist Team 2514761 from the University of the Chinese Academy of Social Sciences provided a clear explanation of their data treatment approach (see **Figure 6**).



2.3.2 Data Filling and Processing

We observed that a considerable portion of datasets lacked information for a few African countries. Therefore, we imputed the missing values with N/A and skipped them directly in subsequent calculations during data processing. Additionally, we noted the absence of data for certain years within some datasets. For instance, the School Enrollment, Tertiary data for the United States in 2009 is missing. In such cases, we employed piecewise interpolation for data imputation.

Figure 6. Explanation of data treatment approach by Finalist Team 2514761 from the University of the Chinese Academy of Social Sciences.

Model Selection, Analytical Approach, and Connections Between the Model and the Real World

One of the features of mathematical modeling is that there is rarely a single correct model. Different models allow the modeler to ask different types of questions, engaging in a dialog between the modeler, the models, and the insights that the model provides about the real world. However, some models and analytical approaches are more appropriate than others. Occasionally, the judges see a model selected without much justification of how that modeling choice is well suited to explore the most important and interesting aspects of the problem. Also, the judges sometimes see teams try a large and diverse set of models without any justification for why so many models were necessary.

As noted elsewhere in this commentary, clear expository writing is valuable because it helps convey both the main ideas and the nuances of each modeling choice. The judges take notice of how each team draws a connection between something of interest in the real world, and how that thing (as well as the things that could influence it) are represented in a model.

Outstanding Team 2504223 from Xi'an University of Technology offers a good example of a team that justified their modeling choices and how those choices built a connection between their models and the real world. This team was awarded Outstanding in part for their connection between the model and the real world, as discussed in the overview of their paper later in this commentary.

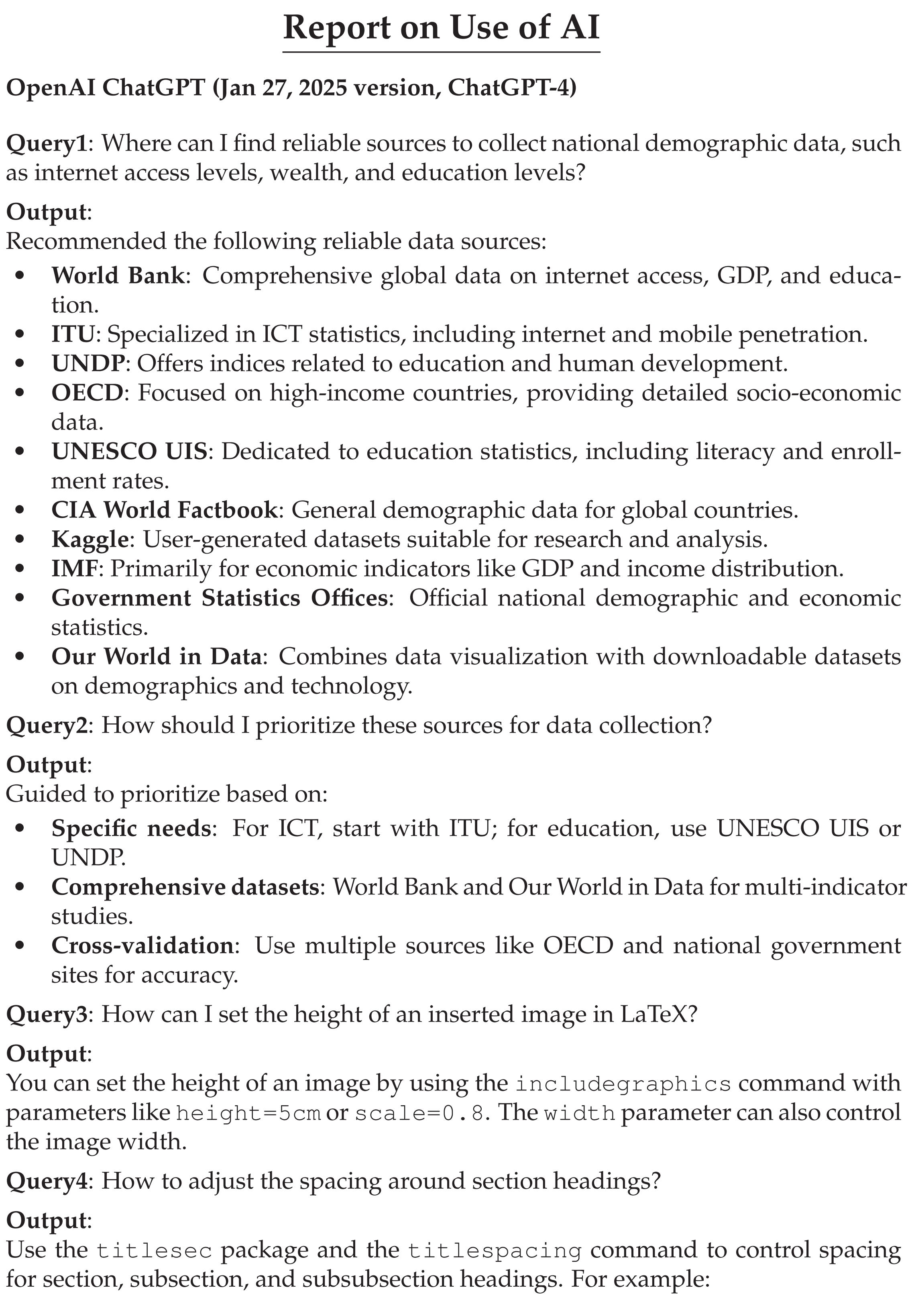
Appropriate Use of AI

We were curious to see how teams would leverage machine learning and/or AI to support their work. Some teams used AI to help them scrape government websites and to collect and classify different legislative or enforcement policies. We were particularly impressed with how Outstanding Team 2521039 from China Agricultural University leveraged AI. Beyond the required AI report of the inputs and outputs, the team provided comments on their experiences, as well as their perceptions about the limitations that they believed that they had encountered in their use of AI. We reproduce their AI report in **Figures 7–8** on pp. 314–315.

Creativity

We close this section with perhaps the most intangible, yet highly valuable, aspects of good modeling: creativity. The modeling and design processes are naturally aligned, with iterative cycles of divergent thinking and convergent thinking. In phases of divergent thinking, modelers are brainstorming all the ways a part of the problem could be defined, addressed, and/or modeled. And in phases of convergent thinking, modelers are taking the best aspects from the brainstorm, bringing them together, figuring out how to interpret a solution in the context of the real world, and producing a meaningful report for a stakeholder. So, even when one approach to any part of the problem seems like the most obvious choice, we (who are all experienced modelers) appreciate the rich perspectives that an alternative approach can bring. Therefore, each year, the judges look forward to seeing a diverse set of inspired and creative solutions.

This year, two particular papers stood out for their creative approaches. Outstanding Team 2507789 from the University of Electronic Science and Technology of China explored cybersecurity through a systemic lens inspired by the Five Elements philosophy. That philosophy served as a common thread throughout the entire paper, helping readers connect a diverse set of ideas and digest information more easily. More detail is in the section on that paper later in this commentary.



Report on Use of AI

OpenAI ChatGPT (Jan 27, 2025 version, ChatGPT-4)

Query1: Where can I find reliable sources to collect national demographic data, such as internet access levels, wealth, and education levels?

Output:
Recommended the following reliable data sources:

- **World Bank**: Comprehensive global data on internet access, GDP, and education.
- **ITU**: Specialized in ICT statistics, including internet and mobile penetration.
- **UNDP**: Offers indices related to education and human development.
- **OECD**: Focused on high-income countries, providing detailed socio-economic data.
- **UNESCO UIS**: Dedicated to education statistics, including literacy and enrollment rates.
- **CIA World Factbook**: General demographic data for global countries.
- **Kaggle**: User-generated datasets suitable for research and analysis.
- **IMF**: Primarily for economic indicators like GDP and income distribution.
- **Government Statistics Offices**: Official national demographic and economic statistics.
- **Our World in Data**: Combines data visualization with downloadable datasets on demographics and technology.

Query2: How should I prioritize these sources for data collection?

Output:
Guided to prioritize based on:

- **Specific needs**: For ICT, start with ITU; for education, use UNESCO UIS or UNDP.
- **Comprehensive datasets**: World Bank and Our World in Data for multi-indicator studies.
- **Cross-validation**: Use multiple sources like OECD and national government sites for accuracy.

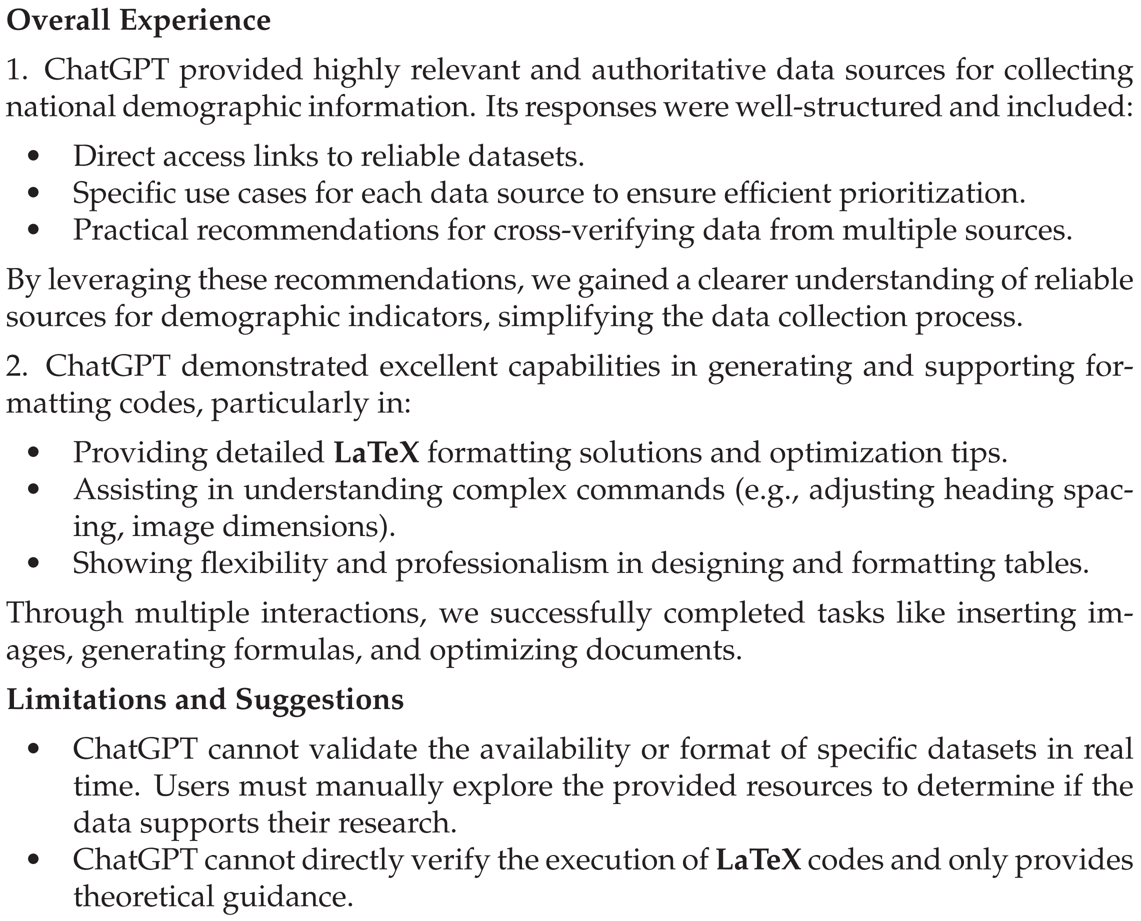
Query3: How can I set the height of an inserted image in LaTeX?

Output:
You can set the height of an image by using the `includegraphics` command with parameters like `height=5cm` or `scale=0.8`. The `width` parameter can also control the image width.

Query4: How to adjust the spacing around section headings?

Output:
Use the `titlesec` package and the `titlespacing` command to control spacing for section, subsection, and subsubsection headings. For example:

Figure 7. Explanation of AI usage by Outstanding Team 2521039 from China Agricultural University.



Overall Experience

1. ChatGPT provided highly relevant and authoritative data sources for collecting national demographic information. Its responses were well-structured and included:

- Direct access links to reliable datasets.
- Specific use cases for each data source to ensure efficient prioritization.
- Practical recommendations for cross-verifying data from multiple sources.

By leveraging these recommendations, we gained a clearer understanding of reliable sources for demographic indicators, simplifying the data collection process.

2. ChatGPT demonstrated excellent capabilities in generating and supporting formatting codes, particularly in:

- Providing detailed **LaTeX** formatting solutions and optimization tips.
- Assisting in understanding complex commands (e.g., adjusting heading spacing, image dimensions).
- Showing flexibility and professionalism in designing and formatting tables.

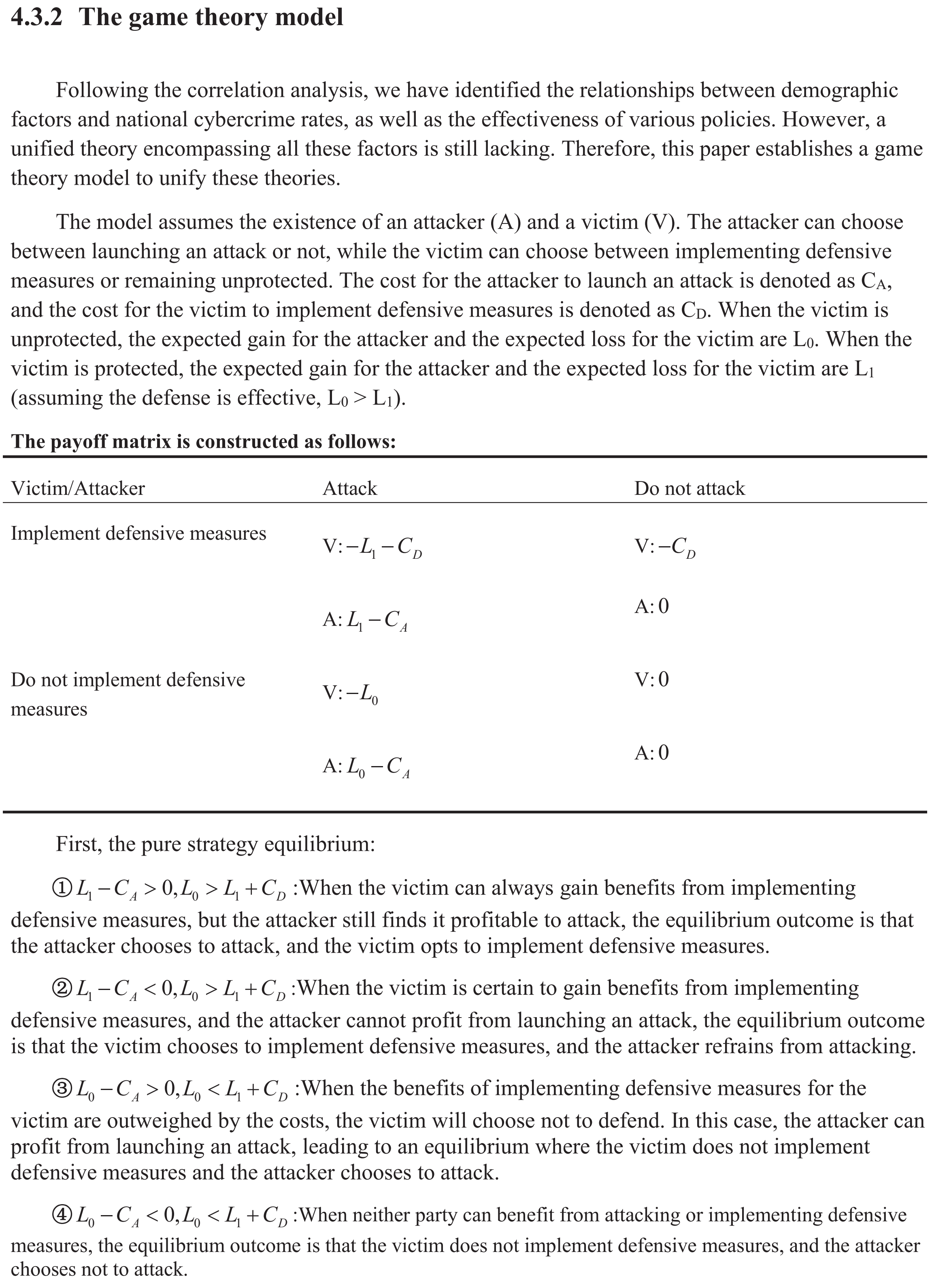
Through multiple interactions, we successfully completed tasks like inserting images, generating formulas, and optimizing documents.

Limitations and Suggestions

- ChatGPT cannot validate the availability or format of specific datasets in real time. Users must manually explore the provided resources to determine if the data supports their research.
- ChatGPT cannot directly verify the execution of **LaTeX** codes and only provides theoretical guidance.

Figure 8. Continuation of explanation of AI usage by Outstanding Team 2521039 from China Agricultural University.

While the Outstanding Team 2507789 from the University of Electronic Science and Technology of China applied their creativity in how to frame the problem, Finalist Team 2511753 from Renmin University of China applied their creativity in their selection of a mathematical model. They created a game theory model with an attacker and a victim, together with cost/loss-based strategies. The outputs of this game theory model provided the motivation for the team's broader policy recommendations. We reproduce details of their model in **Figures 9–11** on pp. 316–318.



4.3.2 The game theory model

Following the correlation analysis, we have identified the relationships between demographic factors and national cybercrime rates, as well as the effectiveness of various policies. However, a unified theory encompassing all these factors is still lacking. Therefore, this paper establishes a game theory model to unify these theories.

The model assumes the existence of an attacker (A) and a victim (V). The attacker can choose between launching an attack or not, while the victim can choose between implementing defensive measures or remaining unprotected. The cost for the attacker to launch an attack is denoted as C_A, and the cost for the victim to implement defensive measures is denoted as C_D. When the victim is unprotected, the expected gain for the attacker and the expected loss for the victim are L_0. When the victim is protected, the expected gain for the attacker and the expected loss for the victim are L_1 (assuming the defense is effective, $L_0 > L_1$).

The payoff matrix is constructed as follows:

Victim/Attacker	Attack	Do not attack
Implement defensive measures	V: $-L_1-C_D$ A: L_1-C_A	V: $-C_D$ A: 0
Do not implement defensive measures	V: $-L_0$ A: L_0-C_A	V: 0 A: 0

First, the pure strategy equilibrium:

① $L_1-C_A>0, L_0>L_1+C_D$:When the victim can always gain benefits from implementing defensive measures, but the attacker still finds it profitable to attack, the equilibrium outcome is that the attacker chooses to attack, and the victim opts to implement defensive measures.

② $L_1-C_A<0, L_0>L_1+C_D$:When the victim is certain to gain benefits from implementing defensive measures, and the attacker cannot profit from launching an attack, the equilibrium outcome is that the victim chooses to implement defensive measures, and the attacker refrains from attacking.

③ $L_0-C_A>0, L_0<L_1+C_D$:When the benefits of implementing defensive measures for the victim are outweighed by the costs, the victim will choose not to defend. In this case, the attacker can profit from launching an attack, leading to an equilibrium where the victim does not implement defensive measures and the attacker chooses to attack.

④ $L_0-C_A<0, L_0<L_1+C_D$:When neither party can benefit from attacking or implementing defensive measures, the equilibrium outcome is that the victim does not implement defensive measures, and the attacker chooses not to attack.

Figure 9. Game theory approach by Finalist Team 2511753 from Renmin University of China.

⑤ $L_0 \geq C_A \geq L_1, L_0 \geq L_1 + C_D$ **:**The model will result in a mixed strategy equilibrium, where the probability of the attacker choosing to attack is $p*$,the probability of the victim implementing defensive measures is $q*$ 。

$$p* = \frac{C_D}{L_0 - L_1}, q* = \frac{L_0 - C_A}{L_0 - L_1} \tag{1}$$

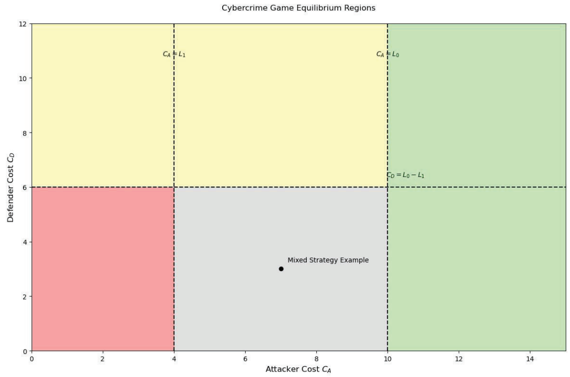


Fig14.Regional map of game model

Based on the results, it can be concluded that the reduction in cyberattacks is typically driven by the following three factors working together:

A decrease in the potential gains from attacks (i.e., L_0 and L_1), an increase in the cost of attacks (C_A), and a reduction in the cost of defense (C_D).

From these results, we can interpret the policy impacts discussed in Issue 2:

Capacity development is the most critical, as it enhances security awareness while simultaneously increasing C_A (attack cost) and reducing C_D (defense cost), thereby incentivizing attackers to abandon attacks and encouraging victims to implement defenses.

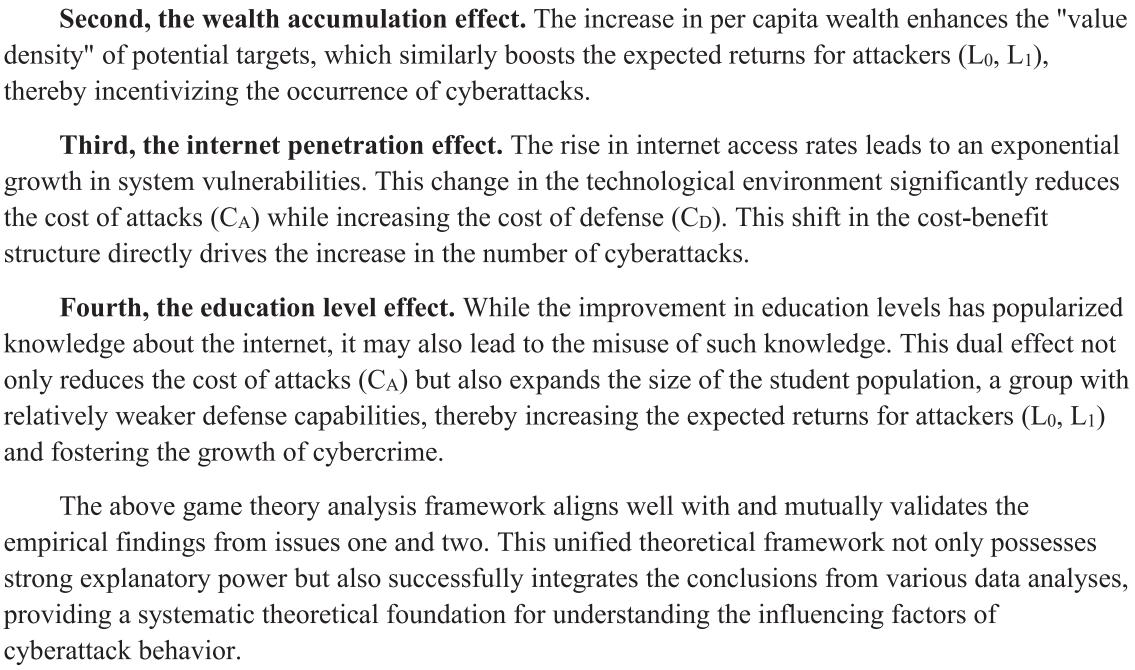
Legal and technical measures are of secondary importance, as they only provide one-sided incentives. Legal measures increase the cost for attackers through strict penalties but do not compensate victims for their losses. Technical detection methods merely reduce the attackers' potential gains (L_0, L_1) and do not serve as a strong incentive for defenders.

Cooperation and organizational efforts are the least effective. While such collaborative and organizational behaviors may lower defense costs (C_D) through shared defensive measures, they also create systemic risks. The shared responsibility among collaborators increases the overall risk exposure, thereby potentially raising the attackers' expected gains (L_0, L_1).

From a game theory perspective, the mechanisms by which Demographic factors influence cyberattack behavior can be analyzed through the following four dimensions:

First, the population expansion effect. The growth of the population base directly increases the number of potential attack targets, significantly raising the expected returns for attackers (L_0, L_1), thereby leading to a higher frequency of cyberattacks in populous countries.

Figure 10. Continuation of game theory approach by Finalist Team 2511753 from Renmin University of China.



Second, the wealth accumulation effect. The increase in per capita wealth enhances the "value density" of potential targets, which similarly boosts the expected returns for attackers (L_0, L_1), thereby incentivizing the occurrence of cyberattacks.

Third, the internet penetration effect. The rise in internet access rates leads to an exponential growth in system vulnerabilities. This change in the technological environment significantly reduces the cost of attacks (C_A) while increasing the cost of defense (C_D). This shift in the cost-benefit structure directly drives the increase in the number of cyberattacks.

Fourth, the education level effect. While the improvement in education levels has popularized knowledge about the internet, it may also lead to the misuse of such knowledge. This dual effect not only reduces the cost of attacks (C_A) but also expands the size of the student population, a group with relatively weaker defense capabilities, thereby increasing the expected returns for attackers (L_0, L_1) and fostering the growth of cybercrime.

The above game theory analysis framework aligns well with and mutually validates the empirical findings from issues one and two. This unified theoretical framework not only possesses strong explanatory power but also successfully integrates the conclusions from various data analyses, providing a systematic theoretical foundation for understanding the influencing factors of cyberattack behavior.

Figure 11. Further continuation of game theory approach by Finalist Team 2511753 from Renmin University of China.

Discussion of the Outstanding Papers

With less than 100 hours to work on the problem and produce the report, no team's submission is ever perfect. However, after multiple rounds of rich deliberations, five papers rose to the top and were selected as Outstanding papers. Each is discussed briefly below.

Team 2507789
University of Electronic Science and Technology of China
"Five Elements Illuminate, Cybersecurity Innovates"

We unanimously recognized this work as exceptionally creative. The team used the "Five Elements Theory," an ancient Chinese philosophy, as an allegory for a modern-day innovative cybersecurity framework. In taking this approach, the team used an overarching story format as a vehicle to effectively explain their data analysis, modeling, and findings. The impact of the storytelling was profound, drawing stakeholders into the plot and making the thread of the data analysis rich and meaningful.

In addition to its creative approach, we noted many strengths in this paper, including its visualizations. **Figure 12** shows how this team translated the Five Elements Theory into the elements of modern-day cybersecurity.

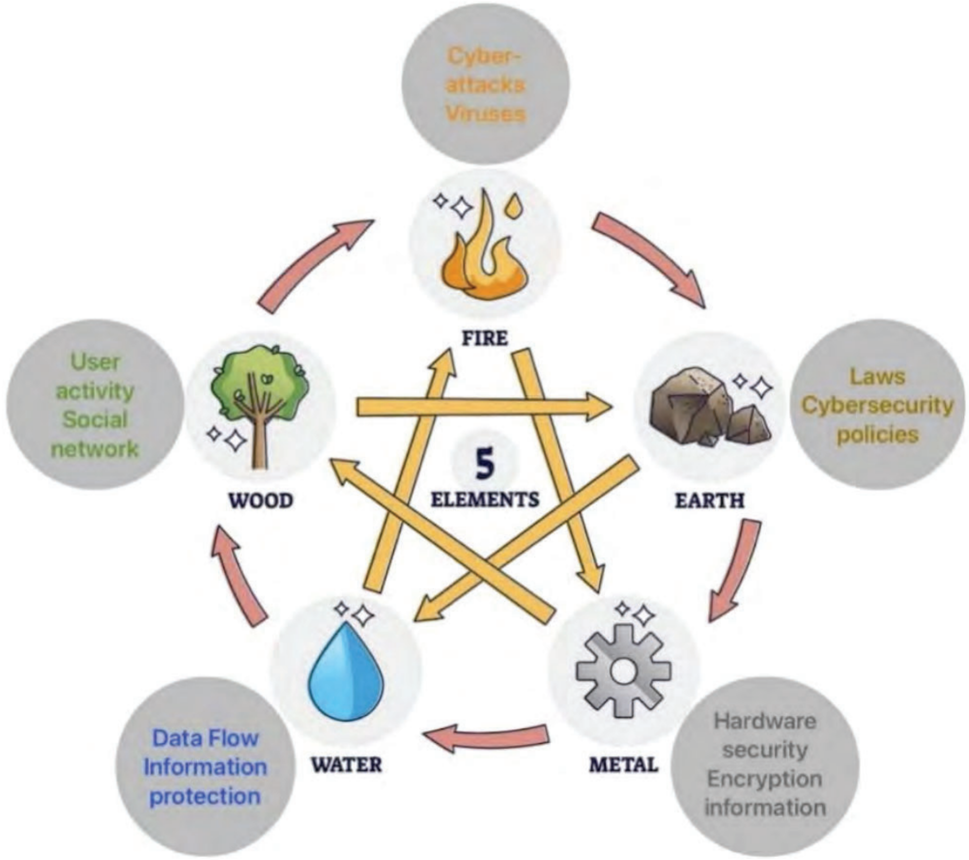


Figure 12. Visualization of cybersecurity issues through a Five Elements framework, by Outstanding Team 2507789 from the University of Electronic Science and Technology of China.

The judges applaud the use of simple, clear visuals that artfully and powerfully help narrate the data storyline. Most of the visualizations were simple, uncongested, and easy to read and interpret, including their visualization showing the power of their PCA dimensionality reduction in **Figure** 13.

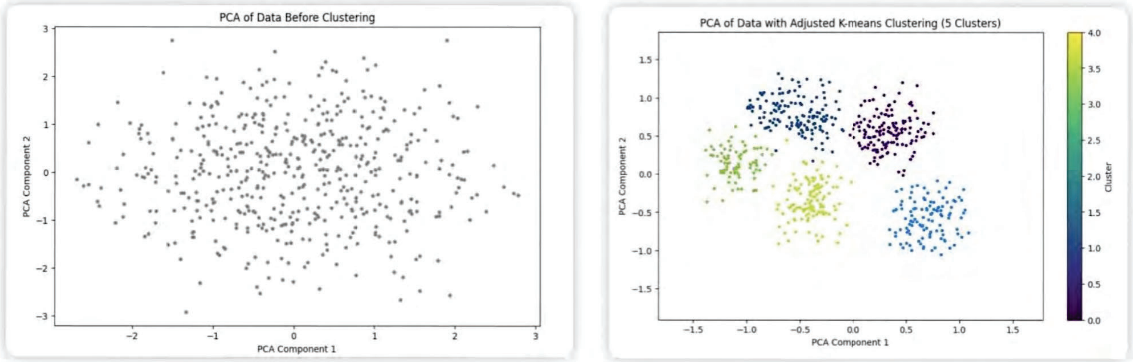


Figure 13. PCA before and after clustering, by Outstanding Team 2507789 from the University of Electronic Science and Technology of China.

The team provided reasonable assumptions regarding the validity of their data sources. They discussed the results and implications of their analysis methods, including the Elbow Method and the difference-in-differences (DiD) method. The summary and memorandum were both well written, although the memorandum might have been even stronger if it had shifted the focus more towards highlighting the team's actionable recommendations, allowing the Five Elements theory to be the delivery vehicle for the findings, not the other way around. The team provided solid, actionable solutions to address emerging cybersecurity challenges. This success was enabled by their deep dive into the detail of cybercrime types, uncovered through the data analysis.

Overall, this paper delivered a compelling solution and leveraged a creative use of Chinese philosophy to clearly convey the team's ideas. In addition to being recognized as an Outstanding paper, it received the Pareto Award for their demonstration of the human element and complexity in their modeling approach, and the team were further awarded a COMAP Scholarship.

Team 2513705
Beijing Normal University
"Cracking the Cyber-Puzzle: KDMF in Action"

This paper cleverly navigated cybercrime distribution and policy effectiveness on a global scale through their KDMF model (**k**-means clustering, **d**ifference-in-differences, **m**aximal information coefficient, and **f**actor analysis) model. This team's work exemplified many outstanding features, including a strong analysis based on well-justified assumptions, a deft exploration of messy data, and a cohesive narrative that connected multiple models. Their nuanced approach yielded a compelling story and clear, actionable policy recommendations.

The team's solution consisted of three primary components: characterizing the global distribution of cybercrime, investigating the effects of policy intervention, and modeling the influence of demographic factors on the total cybercrimes. Each of these tasks involved multiple related or intertwined models. For example, the authors used k-means clustering together with geographic heatmaps of their data to categorize nations as either prepared and resilient, moderately prepared, or high-risk and vulnerable, relative to cyberattacks. Additionally, their difference-in-differences (DiD) model relied on six policy themes identified by the team's topic modeling. Lastly, the team used complementary results from the maximal information coefficient and factor analysis methods to demonstrate strong correlations between cybercrime and total internet users, mobile-broadband subscriptions, and GDP. Overall, we were consistently impressed with the authors' awareness of the strengths and limitations of their work and thoughtful justifications of each modeling decision.

The creativity expressed by the authors in their data handling truly was a standout aspect of this paper. In particular, the team essentially created their own dataset of cybersecurity policy topics using the Latent Dirichlet Allocation model. From this, they distilled policy topics into broader themes, such as cybercrime legislation, data protection and privacy, and obligations of network operators. These themes were well-reasoned and demonstrated a strong effort to contextualize the data realistically within the given scenario. Ultimately, these themes served as the policy impact parameters in the DiD model, offering insights that informed actionable policy recommendations in the team's memo.

We noted some minor concerns with data visualization in this paper. A few graphs felt congested or poorly labeled, making the clustering results somewhat difficult to understand. However, it was clear from these visualizations that the team engaged deeply with a noisy data set. Furthermore, they expertly handled ambiguous and statistically insignificant results in their policy impact analysis, offering thoughtful explanations and well-reasoned discussions.

To conclude, this team delighted us with their creative modeling and pragmatic policy suggestions. They navigated a complex data set skillfully and carefully, and they thoughtfully considered the subtleties of cybercrime policy making. We also noted the team's responsible use of AI to clarify data and improve visualizations. The team's clever modeling, ability to engage with noisy data, and practical insights in their policy suggestions earned them the rank of Outstanding, as well as the INFORMS Award.

Team 252103
China Agricultural University
"The Global Cybersecurity Chessboard: Decoding Crime Distribution and Policy Effectiveness"

This submission was selected as Outstanding due to the way that the team responsibly handled large amounts of data to draw meaningful inferences about the impacts of cyberpolicies. The scope of their work was facilitated by the team's efficient use of Python to process and analyze their data, and this scope was amplified by the strong connection between the team's data analysis approaches and applications to the real world. The submission had an effective executive summary with clear, concise, and direct ties to the actual results of the work, which helped set a strong tone for the rest of the paper. The team demonstrated a clear interpretation of each part of the problem, seeking to understand the global distribution of cybercrime, assess the effectiveness of cybersecurity policies, and explore the key factors influencing the global distribution of cybercrime.

The team's use of Python resulted in a technical but also clear data-processing pipeline, which offered a great example of transparency in the choice of models considered. The team used simple regression models (the Hierarchical Interaction Scoring Regression Model (HISR) and the Log-Enhanced Quadratic Regression Model (LEQR)), which were well-suited choices for the problem and were executed clearly.

Two other noteworthy strengths of this paper were the data visualization and the policy memo. The data visualizations were clear, and they were further supported by thorough exposition that explored key takeaways as well as explanations around any notable exceptions to the general trend. What made the visualizations so good was not the graphs themselves but the strong writing that supported each one. Each graph and its accompanying text were clean, informative, and enhanced our understanding of the analysis done and its implications. The clear exposition extended beyond the visualizations, supporting the translation from quantitative results into effective policy recommendations that were featured in the paper and in the policy memo. The memo included specific, actionable recommendations that made a compelling case for decision-makers.

Although the work was well written and the analysis thoughtfully presented, there could have been a deeper exploration of, or more discussion on, the limitations of the chosen models and methods. Nevertheless, these are opportunities for refinement rather than shortcomings.

In recognition of their use of mathematical modeling, computational approach, thoughtful analysis, and policy relevance, this team was also awarded the prestigious SIAM Award to honor the strength and quality of their work, in addition to being selected as an Outstanding paper.

Team 2504223
Xi'an University of Technology
"Changing rules on the Virtual Battlefield"

This paper stood out due to its thoughtful treatment of assumptions and its justifications for the connections between the real world and the team's models. While some teams assumed away some of the interplay between factors to apply common statistical models to this problem, this paper embraced the complexities and interdependencies inherent in the problem and selected models capable of handling these complexities. The team also leveraged AI wisely by using nonlinear programming (NLP) to accelerate their exploration of numerous national policies, allowing them to cluster and focus their analysis. For their efforts, this team was selected for the AMS Award.

Specifically, one of the team's assumptions focused on the interdependency between economic factors (such as GDP) and cybersecurity. They also noted that in addition to GDP affecting both the level of technology and available resources for investment in cybersecurity, there are other interdependencies relating to education level and employment status, which impact motivations, opportunities, and capabilities of cybercrime.

To address these complexities, the team explored the impacts of existing policies in situ. After sorting countries into victim and/or attacking countries and mining data related to the potential efficacy of each type of policy in each of these settings, the team built a clever series of difference-in-differences (DiD) analyses to extract meaningful inferences about the relative efficacy of each type of policy. The results of their analysis are illustrated in **Figure** 14. By using a more empirical model, the team's paper inherently drew clear connections between the model and the real world, leading to recommendations that directly flowed from their findings.

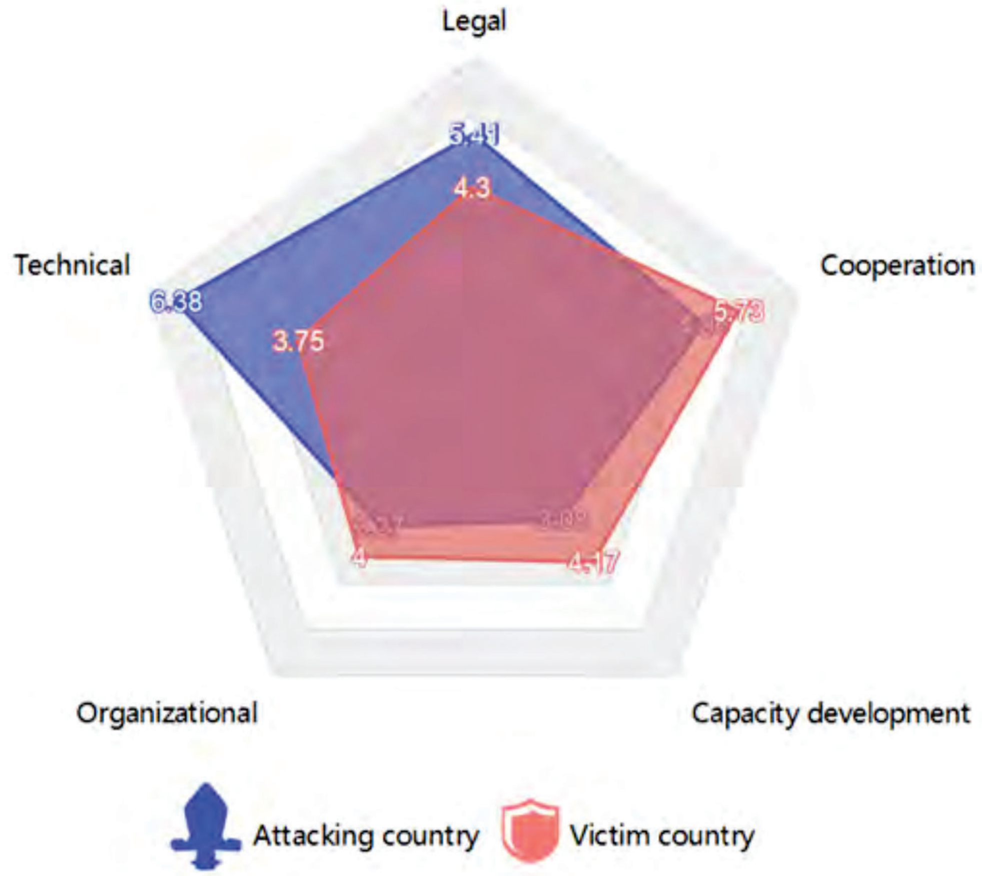


Figure 14. Policy effect radar plot, by Outstanding Team 2504223 from Xi'an University of Technology.

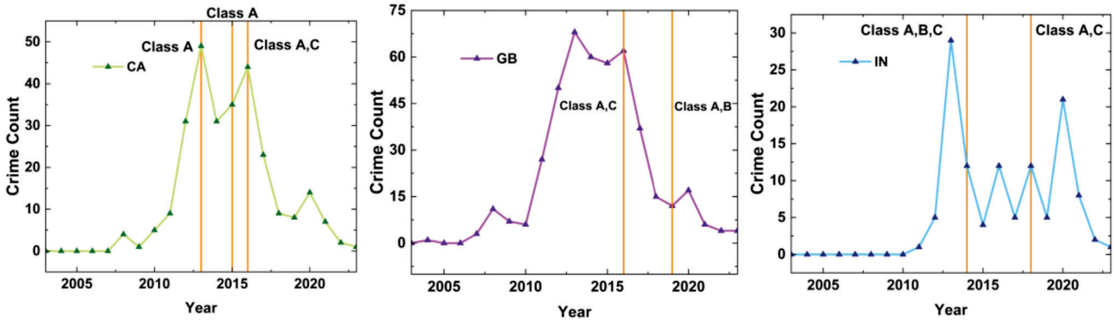
While the memo had room for improvement in how the team's findings could be more dynamically conveyed to a non-technical audience, the modeling itself was excellent. We applaud this team for its ability to incorporate complexity in their work.

Team 2517199
University of Electronic Science and Technology of China
"Data-Driven Policy Effectiveness Evaluation and Country-Specific Characteristic Based Cybercrime Prediction"

Some unique details of this paper helped it rise to the top, including its treatment of the data, its predictive and temporal approach, and the clarity of the exposition of its rationale.

We appreciated this team's treatment of the data and their attention to detail. They were one of very few teams to call attention to anomalies, such as duplicate data, in the VCDB Database. The treatment and processing of the data was clearly explained and justified. In their policy memo, they even recommended the need to clean up the VCDB Database to prevent errors in future research.

We also valued the team's well-reasoned problem-solving approach. The team started their work by exploring four different types of cybercrimes and strains before identifying countries with changes in their cybersecurity statistics in each of these four dimensions. They dug into the policies that may have driven those changes, by overlaying policy changes with relevant time series data, as shown in **Figure 15**. Then the team built a statistically informed prediction model, leveraging a relatively new approach to transformer models called TimeXer.



(a) Canada (b) Great Britian (c) India

Figure 15. Times series data for cyberincidents with policy changes, by Outstanding Team 2517199 from the University of Electronic Science and Technology of China.

Many teams did excellent modeling. However, this team's work was easy to celebrate because they used their report to reflect on their thinking—not just the what and the how, but the why behind their modeling decisions. While the executive summary was incomplete (it pointed to findings in the body of the report instead of giving the bottom line up front) and the memo was not formatted well, the rest of the report tied ideas together clearly, and the memo provided actionable findings tied to the analysis. Ultimately, we selected this paper as Outstanding for the combination of the team's attention to detail, their sound modeling approach, and their clear exposition of the rationale behind their modeling decisions.

Concluding Remarks

This year, teams from around the world leveraged tried and true approaches as well as emergent and nascent capabilities, such as generative AI, large language models, and natural language processing, to scrape, sift through, and make sense of large amounts of data related to cybersecurity. The problem was challenging and very open-ended, and teams took a wide range of approaches from the problem definition to the model selection. We celebrated this diversity of approaches as well as the clarity of writing as teams connected their ideas, modeling choices, and model outputs to the real world. We also appreciated creativity—both in terms of how the problem was addressed (the models that a team selected) as well as how the work was communicated (the use of metaphor, story, and visualizations).

Reference

Libertini, Jessica, Troy J. Siemers, and Diana M. Thomas. 2018. Executive summary. *The UMAP Journal* 39 (4): 427–432.

About the Authors

Luke Castle earned his Ph.D. in mathematics at North Carolina State University, where he now is a teaching assistant professor. He first got involved in the ICM in 2019 as a postdoctoral fellow at Virginia Military Institute, serving as triage judge, triage coordinator, and final judge for the competition. His current interests revolve around redesigning service courses to meaningfully showcase the broad applicability of mathematics.

Philipp M. Dau earned his Ph.D. in Criminology and Geography from Ghent University and has researched and studied at Cambridge University, Leipzig University, Umeå University, Arizona State University, Complutense University of Madrid, and the University of Kiel. His professional experience includes public sector consulting, agile product management in software development, and transport-related security. He has been an ICM triage judge for five years and has been a final judge since 2022. His academic and professional interests range from policing, security, and economic geography to evidence-based management and strategic leadership.

Kira Graves retired from the US Army Training and Doctrine Command in September 2023. Dr. Graves is currently engaged with several non-profit organizations, corporations, and institutions of higher learning.

Bethany Kubik is a math interventionist at a middle school. She earned her Ph.D. in mathematics from North Dakota State University with a focus on homological algebra. She has taught in the mathematics departments at North Dakota State University, the US Military Academy, the University of Minnesota Duluth, and Lake Superior College. Bethany has been a triage judge for the ICM since 2017 and has been on the final judging panel many times.

Jessica Libertini has formal training in mathematics, engineering, international relations, and science diplomacy. She enjoys developing analytic frameworks and participatory methodologies to support teams that are multidisciplinary, multicultural, and multidimensional as they try to understand and address complex global challenges. Her career has spanned industry, government, and academia, and she is currently on the faculty at the US Military Academy at West Point.

Winnie Nakiyingi is the Research and Academic Coordinator at the AIMS Research and Innovation Centre in Rwanda, a role that intersects research, academics, and science communication. She also is a Statistics Consultant for Axiom-DK, where she provides data analysis services in humanitarian work. Driven by a passion for empowering African women and girls in STEM, Winnie founded Words That Count, an organization that aims to present various career paths within the STEM spectrum to young girls mapping their careers in STEM. Her other passion is bridging the gap between natural and social sciences through collaborations among policymakers, diplomats, and scientists/researchers. She has made several appearances in Science Diplomacy, for example, the United Nations General Assembly (UNGA78) Science Summit, the INGSA Conference in Kigali, and the Malta Conference Foundation for Science Diplomacy, among others.

Eleanor Ollhoff studied at the University of Tennessee and has a background in undergraduate mathematics instruction and pedagogy as well as in pure mathematics (low-dimensional topology and differential geometry). She has taught at Appalachian State University, the University of Tennessee, and the US Military Academy. She has been a triage judge for the ICM since 2014, and she has been on the final judging panel for several of the recent past years.

Troy Siemers has a Ph.D. in mathematics from the University of Virginia. He is a professor and head of the Applied Mathematics department at the Virginia Military Institute. He has broad interests and has published with colleagues on interdisciplinary projects in chemistry, physics, economics, psychology, and applied mathematics. His current research includes game-theoretic modeling and the data presentation of historical data from late-1700s colonial America.