2025 ICM
Problem F: Cyber Strong?

Background:
More and more of our world has become connected through the wonders of modern technology. While this online connectedness has increased global productivity and made the world smaller, it has also increased our individual and collective vulnerability via **cybercrime**. Cybercrime is difficult to counter for a variety of reasons. Many **cybersecurity incidents** cross national borders, complicating issues of jurisdiction for both the investigation and the prosecution of these crimes. Additionally, many institutions, such as investment firms, are unwilling to report a hack, preferring to quietly pay a ransom demand than to let their clients and potential clients know that they were the victim of a security breach. To address the growing cost and risk of cybercrime, many countries have developed national cybersecurity policies, publicly available on their government websites. The International Telecommunication Union (ITU) is the specialized agency of the United Nations focused on information and communication technology; as such, they play a leading role in setting international standards, facilitating international cooperation, and developing assessments to help measure the status of global and national **cybersecurity**.

Requirements:
In this problem, you are asked to help identify patterns that could inform the data-driven development and refinement of national cybersecurity policies and laws based on those that have demonstrated effectiveness. Develop a theory for what makes a strong national cybersecurity policy and present a data-driven analysis to support your theory. In developing and validating your theory, things you may wish to consider include:

- How is cybercrime distributed across the globe? Which countries are disproportionately high targets of cybercrimes, where are cybercrimes successful, where are cybercrimes thwarted, where are cybercrimes reported, where are cybercrimes prosecuted? Do you notice any patterns?
- As you explore the published national security policies of various countries and compare these with the distribution of cybercrimes, what patterns emerge that would help you identify parts of a policy or law that are particularly effective (or particularly ineffective) in addressing cybercrime (through prevention, prosecution, or other mitigation efforts)? Depending on your analytical approach, it may be relevant to consider when each policy was adopted.

- What national demographics (e.g., access to internet, wealth, education levels, etc.) correlate with your cybercrime distribution analysis? And how might these support (or conflate with) your theory?

Based on the quantity, quality, and reliability of the data you collected and used for your analysis, share any limitations and/or concerns that national policy makers should consider when relying on your work to develop and/or refine their national cybersecurity policies.

Your work should not seek to create a new measure of cybersecurity, as there are existing measures such as ITU's Global Cybersecurity Index (GCI),[1] which assigns a score to each country based on their level of cybersecurity as assessed through five pillars: legal, technical, organizational, capacity building, and cooperation. Instead, you have been asked to seek meaningful patterns in the effectiveness of national cybersecurity policies and/or laws with respect to the national contexts in which those policies were enacted. The GCI or similar existing research may be useful in validating your work. Additional resources that could be useful include websites that collect cybercrime data, particularly those leveraging the VERIS framework, which attempts to standardize how cybercrime data is collected and reported,[2] including the VERIS Community Database (VCDB).[3] You are encouraged to find other data sources but be mindful of the veracity and completeness of those sources.

Share Your Insights:
Use your work to create a 1-page memo to country leaders (nontechnical policy experts) attending an upcoming ITU Summit on Cybersecurity. This memo should provide a nontechnical overview of your work, including a summary of the objective and context, your theory, and the most pressing findings that would be relevant to this audience of national policy-makers.

Your PDF solution of no more than 25 pages total should include:

- One-page summary sheet.
- Table of Contents.
- Your complete solution.
- One-page memo.
- Reference List.
- AI Use Report (If used does not count toward the 25-page limit.)

Note: There is no specific required minimum page length for a complete ICM submission. You may use up to 25 total pages for all your solution work and any additional information you want to include (for example: drawings, diagrams, calculations, tables). Partial solutions are accepted. We permit the careful use of AI such as ChatGPT, although it is not necessary to create a solution to this problem. If you choose to utilize a generative AI, you must follow the COMAP AI use policy. This will result in an additional AI use report that you must add to the end of your PDF solution file and does not count toward the 25 total page limit for your solution.

NEW MCM/ICM: Online Submission Process

The purpose of this article is to assist and guide students and advisors participating in MCM/ICM. In the article, COMAP, provides information about the new online submission process using the new online submission page https://forms.comap.org/241335097294056. You will need your team's control number, advisor id number and your problem choice to complete your submission.

References

[1] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[2] https://verisframework.org/index.html

[3] https://verisframework.org/vcdb.html

Glossary

(The following definitions are derived from definitions provided by multiple International Organizations, including ISO, ITU, and INTERPOL.)

Cybercrime: Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/or networks.

Cybersecurity Incident: A single (or a series of) unwanted or unexpected computer security events that have a significant probability of compromising business operations and threatening cybersecurity.

Cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizational and individual assets.