2025 ICM

问题 F：网络强国?

背景介绍

借助现代科技的神奇力量，我们的世界越来越紧密地联系在一起。虽然这种网络连接提高了全球生产力，使世界变得更小但也增加了我们个人和集体在**网络犯罪**方面的脆弱性。由于种种原因，网络犯罪很难打击。许多**网络安全事件**跨越国界，使调查和起诉这些罪行的管辖权问题变得更加复杂。此外，许多机构（如投资公司）不愿意报告黑客攻击，宁愿悄悄地支付赎金，也不愿让客户和潜在客户知道他们是安全漏洞的受害者。为了应对日益增长的网络犯罪成本和风险，许多国家制定了国家网络安全政策，并在政府网站上公开发布。国际电信联盟（ITU）是联合国专注于信息和通信技术的专门机构；因此，他们在制定国际标准、促进国际合作以及开展评估以帮助衡量全球和国家**网络安全**状况方面发挥着主导作用。

要求：

在这个问题中，要求您帮助确定一些模式，以便在已证明有效的国家网络安全政策和法律的基础上，以数据为导向制定和完善这些政策和法律。请就如何制定强有力的国家网络安全政策提出一个理论，并提交一份数据驱动的分析报告以支持您的理论。在制定和验证您的理论时，您可能需要考虑的事项包括

- 网络犯罪在全球的分布情况如何？哪些国家
  网络犯罪的高发区、网络犯罪的得逞区、网络犯罪的挫败区、网络犯罪的报案区、网络犯罪的

网络犯罪被起诉吗？您是否注意到任何模式？

- 在探索各国已公布的国家安全政策并将其与网络犯罪的分布情况进行比较时，您会发现哪些模式可以帮助您确定政策或法律中在解决网络犯罪（通过预防、起诉或其他缓解措施）方面特别有效（或特别无效）的部分？
  根据您的分析方法，可能需要考虑每项政策的通过时间。

- 哪些国家的人口统计数据（如互联网接入、财富、教育水平等）与您的网络犯罪分布分析相关？这些因素如何支持（或与）您的理论相混淆？

根据您收集和用于分析的数据的数量、质量和可靠性，分享国家政策制定者在依赖您的工作制定和/或完善国家网络安全政策时应考虑的任何限制和/或问题。

你们的工作不应寻求创建一个新的网络安全衡量标准，因为现有的衡量标准包括国际电联的全球网络安全指数(GCI)，[1]该指数根据每个国家的网络安全水平，通过法律、技术、组织、能力建设和合作五大支柱进行评估，给每个国家打分。而不是要求你们根据国家网络安全政策和/或法律的颁布背景，寻找这些政策和/或法律的有效性方面有意义的模式。GCI 或类似的现有研究可能有助于验证您的工作。其他有用的资源包括收集网络犯罪数据的网站，特别是那些利用 VERIS 框架的网站，该框架试图规范网络犯罪数据的收集和报告方式，[2] 包括 VERIS 社区数据库 (VCDB)

分享您的见解：
用您的工作成果为出席即将召开的国际电信联盟网络安全峰会的国家领导人（非技术政策专家）撰写一份 1 页的备忘录。该备忘录应对您的工作进行非技术性概述，包括目标和背景概述、您的理论以及与国家政策制定者听众相关的最紧迫的发现。

您的 PDF 解决方案总页数不超过 25 页，其中应包括

- 一页摘要表。
- 目录
- 您的完整解决方案
- 一页备忘录。
- 参考书目。
- 人工智能使用报告（如已使用，则不计入 25 页限制。）

注意：对于提交的完整 ICM 文档，没有具体的最低页数要求。你可以用最多 25 页的篇幅来撰写你的所有解决方案以及你想包含的任何其他信息（例如：图纸、图表、计

算、表格）。我们接受部分解决方案。我们允许谨慎使用 ChatGPT 等人工智能，但没有必要为这一问题创建解决方案。如果您选择使用生成式人工智能，则必须遵守 COMAP 人工智能使用政策。这将导致一份额外的人工智能使用报告，您必须将其添加到 PDF 解决方案文件的末尾，并且不计入解决方案的 25 页总页数限制中。

~~新材料管理办法/国际化学品管理大会：在~~线提交程序

本文旨在为参加 MCM/ICM 的学生和指导教师提供帮助和指导。在文章中，COMAP 提供了有关使用新的在线提交页面 https://forms.comap.org/241335097294056 的新在线提交流程的信息。您将需要您所在团队的控制编号、指导教师 ID 编号和您的问题选择来完成提交。

参考资料

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

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

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

术语表

(以下定义源自多个国际组织提供的定义，包括国际标准化组织、国际电联和国际刑警组织）。

网络犯罪网络犯罪包括利用数字设备和/或网络进行的各种犯罪活动。

网络安全事件：单个（或一系列）不希望发生或意想不到的计算机安全事件，这些事件极有可能危及业务运营并威胁网络安全。

网络安全：网络安全是工具、政策、安全概念、安全保障措施、准则、风险管理方法、行动、培训、最佳实践、保证和技术的集合，可用于保护网络环境以及组织和个人资产。