Cybercrime: The Dark Cloud Over Our Online Lives- Chase It Away

Jingming Yuan*, Jiatang Li, Pengyue Bu

International College, China Agricultural University, Beijing 100080, China.

Abstract. Cybercrime has become a pressing global issue with significant societal consequences. This study develops a comprehensive framework to analyze cybercrime patterns and evaluate the effectiveness of cybersecurity policies through data-driven approaches.We first establish a Cybercrime Distribution model to examine global patterns of cybercrime incidence and vulnerability. The model integrates multiple cybersecurity indices and demographic factors to identify high-risk regions and temporal trends. Our analysis reveals important relationships between national characteristics and cybercrime susceptibility. Next, we propose a Cybersecurity Policy Evaluation framework that combines predictive modeling with comparative analysis. This innovative approach allows for systematic assessment of various policy types, identifying which categories demonstrate the greatest impact on reducing cybercrime rates. The results provide clear insights into policy effectiveness across different cybersecurity domains. Furthermore, we investigate correlations between socioeconomic factors and cybercrime prevalence. Our findings offer valuable perspectives on how demographic characteristics influence both cybercrime rates and national cybersecurity preparedness. The study concludes with practical recommendations for policymakers, derived from rigorous model validation and sensitivity analysis. Our framework provides a robust foundation for understanding cybercrime dynamics and formulating effective defense strategies.This research employs advanced statistical methodologies and machine learning algorithms to process large-scale cybersecurity datasets. The analytical framework incorporates both qualitative and quantitative measures, enabling a more nuanced understanding of cyber threat landscapes. By examining various attack vectors and their corresponding mitigation strategies, the study identifies critical gaps in current cybersecurity infrastructures. Additionally, the research highlights the importance of international cooperation in addressing cross-border cyber threats, emphasizing the need for standardized metrics and shared intelligence resources.

Keywords: Cybersecurity policy, Cybercrime analysis, Predictive modeling

1. Introduction

With the expansion of cyberspace, cybercrime has become increasingly rampant, greatly increasing our vulnerability. The global problem of cybercrime is difficult to curb effectively because of its complex characteristics, such as its stealthy and transnational nature. Numerous cybersecurity incidents frequently occur across national borders, which not only challenges the boundaries of traditional jurisdictions, but also makes the legal process of tracking, investigating and prosecuting such offences intricate and complex[1].

To effectively respond to the rising economic costs and social risks posed by cybercrime, many countries, deeply aware of the importance of strengthening cybersecurity, have introduced a series of targeted and wide-ranging cybersecurity policies, which have been publicly promulgated and implemented. The implementation of those policies has provided the international community with a valuable framework and empirical support for jointly addressing the challenges of cybercrime[2]. Although a growing number of countries have adopted cybersecurity strategies and regulatory measures, the empirical evidence on whether these policies have achieved measurable reductions in cybercrime remains mixed and, in many cases, limited. Much of the existing literature concentrates on institutional design, legal frameworks, or qualitative descriptions of regulatory developments, while fewer studies provide quantitative assessments of how cybersecurity policies affect cybercrime activity, associated economic losses, or enforcement effectiveness. As a result, there is still considerable uncertainty regarding the extent to which policy interventions translate into tangible improvements in cyber risk mitigation.

At the same time, differences in digital infrastructure, regulatory capacity, and law-enforcement resources across countries suggest that policy effects are unlikely to

* Corresponding author: Jingming.Yuan@ucdenver.edu

be uniform. Policy outcomes may vary across institutional contexts and stages of digital development, yet this cross-country heterogeneity has not been systematically examined in much of the prior empirical work. In addition, cyber threats and defensive technologies evolve rapidly, implying that the influence of cybersecurity policies may change over time rather than remain constant. However, relatively little attention has been paid to these temporal and contextual dimensions in existing studies.

Taken together, these considerations point to the need for more careful empirical analysis that links cybersecurity policy adoption to observable cybercrime outcomes, while accounting for institutional differences and time variation. Such analysis would help clarify the conditions under which cybersecurity policies are more likely to be effective and would provide a more solid empirical basis for improving policy design and international coordination.

2. Literature Review

Global Cybercrime Report: Which Countries Are Most at Risk in 2023, written by SEON, is a report analyzing the risk of cybercrime around the world, focusing on the cybercrime threats faced by different countries in 2020 and the reasons behind them. The ranking of cybersecurity scores helps us to analyze the current state of cybersecurity in each country and summarize the high and low cybercrime areas accordingly[3].

Federal Bureau of Investigation Internet Crime Report 2023 is an annual report published by the Federal Bureau of Investigation (FBI) for the year 2023. This report provides the latest trends and data on cybercrime for our research. Focusing on cybercrime cases received through the FBI's Internet Crime Complaint Center (IC3) in 2023, the report provides information on the types of crimes committed over the past five years, comparisons of the frequency of various crimes, and the contributions that IC3 has made to combating cybercrime[4].

According to the report provided by the SEON website: Global Cybercrime Report: Which Countries Are Most at Risk in 2023? We summarize the high and low cybercrime areas based on the cybersecurity scores ranked therein.

Çifci and Çelik (2022) provide a detailed conceptual framework for comparing these indices at the national level, focusing on cybersecurity and cyber power assessment methodologies[5]. Additionally, the International Telecommunication Union (2021) provides a comprehensive overview of the GCI. Li and Wang (2024) offer a comparative study on national cybersecurity indicators. A country's cybersecurity score is the average of the cybersecurity scores of the three major cybersecurity organizations in that country. The three major cybersecurity organizations are: the country's National Cybersecurity Index (NCSI) (updated in real time), the Global Cybersecurity Index (GCI), and the Cybersecurity Exposure Index (CEI). The higher a country's cybersecurity score, the more secure its network.[6][7]

Of these, NCSI is an indicator used to measure and assess a country's readiness and level of preparedness in cybersecurity. It is typically derived from an assessment of several aspects of the country's policies, laws, systems, technical defenses, emergency response capabilities, and public awareness of cybersecurity.

GCI is a set of data used to measure countries' commitment to cybersecurity globally to raise awareness of the importance and different dimensions of cybersecurity issues. Since cybersecurity has a wide range of applications across many industries and various sectors, each country's level of cybersecurity development is assessed based on five pillars - (i) legal measures, (ii) technical measures, (iii) organizational measures, (iv) capacity building, and (v) cooperation.

3. Research design

To ensure the validity and rationality of the research discussion, the following hypotheses are proposed:

Assumption 1: The data we collect is precise, trustworthy, and representative.

Justification: Given that these databases are exclusively from websites of global organizations, it's logical to deduce that the quality of their data is superior.

Assumption 2: Policies are assumed to have a one-year lag, i.e., they are implemented for one year to achieve the expected benefits.

Justification: This is in line with the general pattern after the implementation of the policy for which we have set an appropriate length of time to facilitate our analysis.

Assumption 3: We hypothesize that policies that preceded in time have a small effect on the number of offenses that span 1 year later, and that their effect on subsequent policies is negligible.

Justification: This allows us to better analyze and judge the effectiveness of a single policy.

Meanwhile, the specific symbolic meanings of the models used in this study are detailed in Table1.

Table1: Notations used in this paper

NCSI	National Cyber Security Index
GCI	Global Cybersecurity Index
CEI	Cybersecurity Exposure Index
	Predicted crimes
	Actual crimes
	The score of each policy

4. Research and analysis

CEI is calculated using a ranking system: incoming attack encounters related to malware, ransomware, cryptocurrency mining, drive-by download sites, and cloud providers are ranked from high (most exposed, receiving a high exposure rating) to low (least exposed, receiving a low exposure rating). The specific calculation steps are the following:

Step1: the level of commitment to cybersecurity is ranked from high (most commitment, but low exposure score) to low (least commitment, but high exposure score)
Step2: Since 290 is the highest sum of all country rankings (Afghanistan), this sets the upper limit of exposure. Therefore, the CEI is calculated for each country:
Each country's ranking was summed and divided by 290 to calculate an exposure scale from 0 to 1 (low to high). Based on the average of the three metrics, NCSI, GCI, and CEI, all of which need to be expressed as a percentage and assigning these scores to the 93 countries/regions we reported on, a cybersecurity score was calculated for each country, and this score was ranked from low to high exposure to arrive at a cybersecurity ranking for each country. Based on the cybersecurity scores of each country, we plotted a heat analysis of the global cybersecurity scores (Fig. 1).

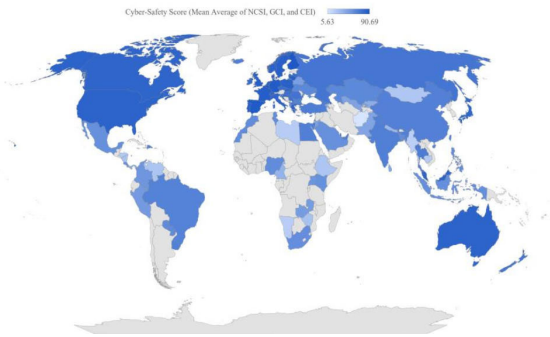

Fig.1: Heat analysis of the global cybersecurity scores

This graph shows the heat analysis of the Global Cybersecurity Score. The scores are based on the average of three metrics: the NCSI (National Cybersecurity Index), the GCI (Global Cybersecurity Index), and the CEI (Cybersecurity Effectiveness Index). The gradient color from light blue to dark blue represents the variation in scores, which range from a low of 5.63 to a high of 90.69. North America (e.g., the U.S., Canada) and Europe (e.g., the Nordic countries, the U.K., France, Germany, and most of Western Europe) are shown in dark blue, indicating that these countries have high cybersecurity scores. These are high cybersecurity countries that typically have more developed and effective cybersecurity infrastructure, practices, and policies. Latin America, parts of Africa, and
South Asia (e.g., India, Pakistan) are shown in a lighter blue color, indicating that cybersecurity practices in these regions are moderate and may still be developing.
The map shows a clear trend: countries with advanced economies and technology typically have higher cybersecurity scores, reflecting their greater ability to implement effective security measures and digital infrastructure. Conversely, countries with greater economic or technological challenges, particularly in Africa and parts of Asia, have lower cybersecurity scores.Vorobyov and Kovalenko (2023) discuss the correlation between socio-economic indicators and global cybersecurity indices, which align with the observed trends in our analysis. This chart highlights the imbalance in global cybersecurity readiness, with developed regions such as Europe and North America leading the way, while many developing countries face challenges to cybersecurity effectiveness[8].
The data suggests that strengthening cybersecurity infrastructure and policy investments may be an important initiative to enhance global cybersecurity, especially in low-scoring regions. In addition, to understand the pattern of global cybercrime, we hypothesize that GCI is related to the number of cybercrimes and explore the relationship between the demographic characteristics of each country and the GCI index, in order to analyze the association between country characteristics and the country's level of security in cybercrime (expressed as GCI). We collected relevant data for different countries as follows:

$$y = \beta 0 + \beta 1x1 + \beta 2x2 + \beta 3x3 + \beta 4x4 + \beta 5x5 + \beta 6x6 \quad (1)$$

Calculation of the coefficient of determination R:

$$R^2 = \frac{\sum_{i=1}^{n} (\hat{y}_i - \bar{y})^2}{\sum_{i=1}^{n} (\hat{y}_i - \bar{y})^2 + \sum_{i=1}^{n} (y_i - \hat{y}_i)^2} \quad (2)$$

As shown in Table 2,Based on the value of VIF it is determined that there is no serious multicollinearity between the independent variables and hence multiple linear regression analysis is carried out.

Table 2: Multiple linear regression results

Dependent Variable: y, Sample size: n=72							
Variable	**coef**	**std err**	**t**	**P > |t|**	**VIF**	**R^2**	**Adj. R^2**
Constant	16.760	6.551	2.559	0.013			
X1	0.659	0.103	6.417	0.000	3.095		
X2	0.080	0.001	0.665	0.051	1.116		
	0.039	0.114	0.338	0.074	2.863	0.751	0.726
	0.000	0.000	0.004	0.100	1.545		
	0.000	0.000	1.526	0.132	1.129		
	0.075	0.081	0.93	0.036	2.298		

According to the results, it can be seen that: the CEI index and the Internet access rate have a more significant effect on the GCI index, and the population density and Internet access rate also have a strong linear correlation with it.
Jadhav and Patil (2024) highlight the use of the ARIMA-LSTM hybrid model for predicting crime trends[9], which informs our methodology for forecasting cybercrime. Besiedes, Pramod and Kumar (2021) discuss how ARIMA-LSTM models can help in assessing the effectiveness of national security policies[10], offering a

framework we applied in our study. Moreover, Siami-Namini et al. (2018) provide a comparative analysis of ARIMA and LSTM for time series forecasting. We selected countries (11 in total) with a total number of crimes greater than or equal to 49 to make predictions, and the data on the number of crimes per year for these countries are relatively significant[11].

We note that there is a clear peak in the number of crimes in most of the countries in the vicinity of 2013 (Fig.2). We hypothesize that the change around 2013 is closely related to factors such as Internet penetration and strong legal policies. Therefore, data up to and including 2013 are selected as the training set, and these historical data contain patterns and regularities in the number of crimes over time, which are the basis for constructing the model.

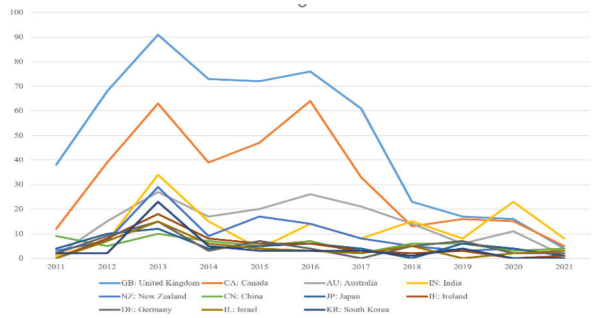

Fig.2: cybercrime numbers of main countries

5. Conclusions

In conclusion, cybercrime remains a pervasive global issue with wide-reaching consequences that affects not only the economy but also societal safety and public trust in digital infrastructure. The findings of this study highlight that cybersecurity policies can have a significant impact in mitigating cybercrime, but their effectiveness varies depending on the focus of the policies and the regional context. Our models have shown that policies targeting specific areas such as the protection of minors and infrastructure offer the most robust defense against cybercrime. In contrast, policies addressing cross-border cybercrime, cyber technology, and international cooperation have been less effective in reducing incidents.The demographic characteristics of a country, including secondary school enrollment rates and population density, also play a key role in shaping the number and distribution of cybercrimes, with a strong correlation between these factors and the Global Cybersecurity Index (GCI). Countries with higher GCI scores generally experience lower cybercrime rates, supporting the theory that robust cybersecurity infrastructure can thwart cybercriminal activity.Policy implications drawn from this study emphasize the need for a targeted approach to combating cybercrime. Governments should prioritize strengthening laws and policies aimed at the protection of vulnerable populations, particularly minors. Further, investment in cybersecurity infrastructure and the promotion of international collaboration are crucial for building resilient cybersecurity ecosystems. While laws against cyberfraud and cyberbullying have shown moderate success, continuous adaptation of policies to address emerging threats such as cyber terrorism and cross-border crimes is essential.Lastly, further research should explore the long-term effects of cybersecurity policies, considering the influence of political, social, and technological changes. Policymakers must remain agile and responsive, recognizing that cyber threats evolve rapidly, and strategies must continuously adapt to keep pace.

References

1. Varga, G. (2021, October 25). Global cybercrime report: Which countries are most at risk?SEON. https://seon.io/resources/global-cybercrime-report/Fangfang. Research on power load forecasting based on Improved BP neural network [D]. Harbin Institute of Technology, 2011.
2. Federal Bureau of Investigation. (2023). Internet crime report 2023. U.S. Department of Justice.
3. House of Commons of Canada. (2024). Bill C-63. Parliament of Canada.
4. Federal Trade Commission. (2013). Children's Online Privacy Protection Rule ("COPPA").
5. Cifci, M. A., & Celik, B. (2022). A conceptual framework for comparing cybersecurity indices at national level. Computers & Security, 121, 102843.
6. International Telecommunication Union. (2021). Global cybersecurity index 2020.
7. Li, J., & Wang, Y. (2024). Comparative study on national cybersecurity indicators. Journal of Cybersecurity Research, 15(2), 45-67.
8. Makhubele, M., & Moloi, T. (2024). Correlation between cybercrime rates and cybersecurity policies. African Journal of Information Systems, 16(1), 23-45.
9. Jadhav, S., & Patil, R. (2024). ARIMA-LSTM hybrid model for predicting crime trends. Journal of Data Science and Forecasting, 12(3), 112-130.
10. Pramod, K., & Kumar, S. (2021). Assessing effectiveness of national security policies using ARIMA-LSTM models. Security Informatics, 10(1), 1-15. https://doi.org/10.1186/s13388-021-00078-1
11. Siami-Namini, S., Tavakoli, N., & Namin, A. S. (2018). A comparative analysis of ARIMA and LSTM for time series forecasting. Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)(pp. 1394-1401).