

Article Analysis: “Exploring the Global Geography of Cybercrime and its driving forces.”

Carla Belfiore

July 21, 2024

The article I chose to examine, titled “Exploring the Global Geography of Cybercrime and its Driving Forces,” is a scholarly article that analyzes how technical advancements in ICTs (information and communication technology) connect with all those societal, political, and economic factors to determine cybercriminality. It analyzes the geographical dispensation of cybercrime as well as the driving forces that contribute to its global spreading. In addition, it also discusses how social inequalities, norms, structures, politics, economic differences, and prosperity all impact cybercriminality and victimization.

Furthermore, the publication goes through the different social science principles such as determinism, objectivity, relativism, and parsimony. In the article, the principle of determinism is very present. In fact, it demonstrates how events like cybercrime, for example, are determined by preceding factors. This is made possible by analyzing the socioeconomic, political, technological, and geographical factors that contribute to the dispensation of cybercrime. Technological infrastructure, for example, shows how countries with more advanced technological infrastructure experience higher rates of cybercrime. Objectivity is another key principle presented in the article. As a result, it promotes objectivity by showing data, facts, and research without subjective or prejudicial insights. The aim of the article is to merely provide insights on the globalization of cybercrime, sticking to factual evidence. Relativism in the concept of cybercrime, for example, can be used to understand how cultural, economic, and framework differences influence perceptions and ways of responding to cybercrime. The article also presents parsimony. Like this principle suggests, the information provided is rather simple and straight-forward. It gives a clear understanding of the factors that influence cybercrime.

To add to all this, it also relates to topics discussed in class, like the use of different research methods, victimization, social science principles, economics, sociology, and criminology. They play a huge role in understanding the realm of cybercrime. Like we’ve seen previously, the economic conditions of a place vary a lot, and this impacts the prevalence of cybercrime. Unemployment, poverty, and income inequality are all aspects to take into consideration. They are all aspects that incentivize cybercriminals to commit illegal actions in exchange for monetary gains. The economic factor is also really important for organizations and societies that can’t invest in good preventative measures, making them more susceptible to the phenomenon of cybercrime. Sociology is also crucial. The study of cultural norms, community dynamics, and human behavior are all contributing factors. The social context, for example, says a lot about the reasons that drive cybercrime activities. Another important factor is the study of criminal behavior. Criminology

allows specialists to get inside the mind of a criminal and analyze what types of events push them to act unethically.

In addition, the article focuses on research questions based on identifying and analyzing socioeconomic factors that propel cybercrime across the globe. Questions such as the impact of social, economic, and cybersecurity factors that influence the popularity of cybercrime. Also, hypotheses propose that in places where corruption is more prominent, the phenomenon of cybercrime is more prevalent due to the decrease in regulations and low law enforcement responses.

Moreover, different research methods and data analysis approaches are applied. Explanatory variables, such as cybersecurity, economic, technological, and political indicators, are analyzed and collected. Including GDP per capita (poverty rate), demographics, internet usage, and political corruption. Statistical techniques like GLMs (generalized linear models) are used to model relationships between a response variable and one or more predictor variables. Mapping is also used to illustrate the global status. This helps identify regions who present the highest concentration of cybercrime. Methods, such as statistical techniques like GLMs and geographic data analysis (mapping), provide a clearer understanding of the factors that increase cybercrime.

Based on the article, the topic of marginalized groups can be related to socioeconomic inequalities (poverty, unemployment, income inequality, etc.). Marginalized groups like the ones who belong to those categories lack the knowledge, help, and tools to protect themselves from the cyber world. Another reason why this topic relates to marginalized groups is the legal aspect, such as bad governance, that puts the safety of these individuals at risk.

An important aspect is the contribution the article has to society. It provides an in-depth explanation of cybercrime, helping cybersecurity specialists, organizations, societies, and governments. Identifying different factors that contribute to the propagation of cybercrime allows for the use of targeted interventions, and the comparative information provided on cybercrime across different countries gives a very broad view of the problem.

Lastly, the article is very complete since it provides helpful insights on cybercrime, makes comparisons between different countries and methods, and draws awareness to topics that not many people touch on.

Article used/Citations:

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023, February 23). Exploring the global geography of cybercrime and its driving forces. Nature News.
<https://www.nature.com/articles/s41599-023-01560-x#data-availability>