

Nicholas Morton

Date: November 11, 2024

Article Review #2: Cybercrime and Its Societal Impact

Introduction

The article “Establishing a Theory of Cyber Crimes” by K. Jaishankar explores the dynamics of cybercrime and the reaching effects it has on individual organizations and broader societal structures. The journal was posted in the International Journal of Cyber Criminology and focuses on human behavior and technological advancement to help understand and combat cybercrime.

Relevance to Social Sciences

The article relates to key social science principles. For example, cybercrime challenges society’s norms because they exploit stuff like vulnerabilities inside of digital infrastructures, which aligns with the concepts of deviance. Also, the costs and benefits of cybersecurity inventions are actually really important. This lens shows the societal consequences of data breaches. The spread of cybercrimes via tactics like phishing and social engineering is also prevalent in the eroding of trust in digital systems which reflect the challenges of maintaining societies. (Jaishankar, 2007)

Research Questions and Hypotheses

The article addresses two research questions, for example:

1. What motivates individuals to engage in cybercrime
2. How does societal and economic inequality contribute to the frequency of cybercrime

Jaishankar (2007) hypothesizes that economic disparities and limited access to real cybersecurity education creates cybercriminal activities to occur.

Research Methods

In the article, Jaishankar uses mixed-methods research, she used statistical data from the global cybercrime reports to analyze and identify patterns and trends which is a quantitative analysis. They also conducted interviews with cybersecurity experts and individuals who were affected by cybercrime to provide context to the numbers and consequences of cybercrime for a qualitative analysis. The combination of the two ensures the depth of understanding why people commit cybercrimes.

Data and Analysis

They used the Quantitative analysis for data on hacking, phishing, and ransomware to highlight global trends. They also used Qualitative themes such as economic desperation and the accessibility of technology are explored to understand why cybercrime happens (Jaishankar,2007). Because the data focuses on both the quantitative and qualitative analysis, the study’s final conclusion will have multiple perspectives and be closer to be accurate.

Connections to Class Concepts

The article also uses multiple theories that relate to the stuff we talked about in class. For example, phishing and identity theft are illustrated in the article and it shows how cyber criminals exploit

these vulnerabilities. It also talks about economic theories for cybercrime that relate to in class discussions. For example, the rational choice theory is present where people maximize their own personal gain despite facing their harm to society.

Conclusion

In conclusion, K. Jaishankar's "Establishing a Theory of Cyber Crimes" gives a good theory to the reason for cybercrime. It implements social science principles and it also adds stuff that we have learned in class. It also address how important of addressing cybercrime as a societal problem and not just a technical problem that everyone should be aware of.

References

Jaishankar, K. (2007). Cybercrime and its impact on society. *International Journal of Cyber Criminology*, 1(1), 1–15. Retrieved from <https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf>