Janay Dumas

13 November 2024

Article Review #2, Cyberattacks, cyber threats, and attitudes toward cybersecurity policies

Introduction: In this article review, I will be able to explain how the following article describes how it relates to the principles of the social sciences, the study's research questions or hypotheses, the types of research methods used, the types of data and analysis done, how the concepts from our PowerPoint slides relate, how it relates to the challenges and concerns of marginalized groups and the overall contributions of the study to society.

Cyber Threats and Public Attitudes: The article explores how cyberattacks influence public opinion on cybersecurity policies, connecting to some core ideas in social sciences—like how people respond to threats and the balance between government policy and individual rights. It shows that as people experience or learn about cyberattacks, they tend to become more supportive of specific cybersecurity measures. This topic is a great example of how social sciences aim to understand society's reactions to risks and government actions. Key concepts like security versus privacy and the psychological impact of feeling threatened tie into themes in political psychology and societal responses to perceived danger. The main research questions ask how exposure to different types of cyberattacks (lethal vs. nonlethal) effects public support for cybersecurity policies. Specifically, the study asks: Does seeing certain types of cyberattacks make people more likely to support certain policies? The researchers hypothesized that when people feel more threatened, they're more likely to support government measures to protect against those attacks. To investigate, the study used a randomized survey experiment with 1,022 participants in Israel. Participants watched simulated news videos depicting either lethal or nonlethal cyberattacks. This setup helped researchers see whether exposure to these different scenarios changed people's views on various cybersecurity policies, especially in terms of feeling threatened and supporting government intervention. Survey data was collected, where participants rated their support for different cybersecurity policies and their level of perceived threat. The researchers likely analyzed this data using statistical methods to find connections between the type of attack exposure and policy support. They probably also used mediation analysis to see if perceived threat was influencing the link between attack exposure and support for specific policies. This topic also brings in important issues for marginalized groups, who are often more at risk when it comes to data privacy and access to cybersecurity protections. Marginalized communities may also have different concerns about privacy and surveillance, given they often face more monitoring and discrimination. It's essential for cybersecurity policies to consider these unique perspectives to avoid unfair impacts and to ensure that everyone has equal access to security and privacy.

Conclusion: In conclusion, this research shows why understanding public opinion is so crucial for effective cybersecurity policy. By looking at how different types of cyber incidents effect public support for specific policies, the study gives policymakers a roadmap for creating strategies that address public concerns without compromising privacy. This kind of research is vital because it offers ways to balance security needs with civil liberties.

Sources Used:

Janay Dumas

13 November 2024

Article Review #2, Cyberattacks, cyber threats, and attitudes toward cybersecurity policies

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab019