# Article review 2

Audrey Gyane

Old Dominion University

Cybersecurity and Social Science 201s

Professor Matthew Umphlet

Mar 29, 2024

According to determinism, the way humans behave is shown by deeper reasons or variables, such as how people react to cyber attacks and create rules regarding cybersecurity. From this viewpoint, attitudes and behaviors towards cybersecurity can be expected or influenced by certain political, financial or technical variables. While on the flip side, relativism is recognized from different types of viewpoints, standards, and situations that influence how people and society react to cyberattacks and preferred courses of action. Looking at the views about cybersecurity, relativism shows how taking political, financial, and technical variables into account. This is because what is viewed as a danger or acceptable solution in a certain place could change and not be in others. Relativism and determinism together highlight how challenging it is to understand and address cybersecurity challenges since they need to not just have deeper reasons but also a range of subject to context views and responses.

In this article there are two hypotheses. The first one is cybersecurity policy adoption is greater probability to be backed by those who have experienced either deadly or less damaging cyberattacks than by those who have not. The second one is people that have experienced deadly cyberattacks are at greater risk to favor the start of cybersecurity measures than people who experienced less damaging cyberattacks.

The goal of the study was to see whether watching various news reporting items on cyberattacks can impact people in society's opinions regarding cybersecurity laws. The researchers achieved this by presenting videos of news reports on cyberattacks to those taking part of the experiment. A control group which are those who did not see any of the videos, while some discussed less damaging situations and lastly, others discussed deadly or lethal cyberattacks. After that, they inquired about those who were doing the experiment and their level of concern over cybersecurity. Because of different factors such as age, gender, and political orientation the scientists had to take it into account because it can affect the participants' views. The study analyzed videos to look at the potential effect of the kinds of cyber events individuals heard on their attitudes regarding cybersecurity.

Through an online poll, the researchers gathered data from Israeli citizens. Participants were divided into three groups. The control group that did not see any videos, those that watched less damaging videos, and those who watched the lethal videos. Following that, individuals had to respond to the questions about their views on cybersecurity and the level of concern they had for online dangers. In the article they showed a graph; the graph is called integrative path analysis model. By using this type of model they can determine the variables with both immediate and lasting impacts. After the analysis model follows two tables. The first table is the immediate effects but estimated and the second table is the mediation effects but also with estimated data.

The challenges, concerns and contributions of marginalized groups are closely related to cybersecurity and how the general public sees cyberattacks. By their lack of funds, there are flaws in their knowledge of technology, and a bigger likelihood of encountering online attacks, marginalized groups have more risk on cyberspaces. Policies for comprehensive cybersecurity have to deal with these particular issues and give marginalized groups safety and inclusion as a first priority.

This study has a considerable and broad social influence. To show the public encouragement to participate in cybersecurity policy making which helps the establishment of more open and successful rules by connecting public views and ways with cyberattacks concerns. By doing this it will increase the general understanding  of cybersecurity while promoting honesty and unity within the people, government and organization owners causing stronger cybersecurity policies.

# Citation

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021, October 7). *Cyberattacks, cyber threats, and attitudes toward cybersecurity policies*. OUP Academic. https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745?searchresult=1#406984008