Article Review #1 – Threat Perception & Intrusive Cybersecurity Policies

Alexander Berrios

CYSE 201S

Threat Perception & Intrusive Cybersecurity Policies

Public perception of cybersecurity policies is important for policymakers to consider before implementing new legislation. New regulations and laws developed to increase security on the cyber frontier may appear invasive and unattractive to those affected, limiting the success of their implementation. The article reviewed explores the relationship between public exposure to cyberattacks, support for intrusive cybersecurity policies, and the social phenomena of threat perception. This study directly investigates the relationship between sociology, human psychology, and political science within the context of cybersecurity.

Experiment

Researchers utilized theories associated with terrorism and political violence to ground their analysis, such as the Terror Management Theory, which argues that people experience emotional reactions when exposed to indirect violent acts that threaten their morality (Snider, p. 5). As a result, they hypothesized that there is a parallel relationship between exposure to cyberattacks and support of increased government cybersecurity measures, with threat perception being the mediator. Researchers also hypothesized that initial reports would increase this exposure effect.

To test this hypothesis, a controlled randomized survey experiment was conducted to gather data on how exposure to different cyber incidents affects public willingness to support cyber regulatory policies. Surveys and experiments are common methods for data collection among sociologists, as explained during this course's module 3 lecture; this is particularly important to note due to the relevance of sociology and psychology within this case.

Data Collection & Analysis

Exposure to lethal and non-lethal cyberattack reports was the predictor variable, while the dependent variable was support for cybersecurity policies. The dependent variable was examined with a questionnaire with answers that ranged from 1 (completely disagree) to 6 (completely disagree), which

employed two scales that placed the participants on a spectrum that measured their attitudes towards cybersecurity policies.

Results

The results of the experiment conducted aligned with the researcher's hypothesis; those exposed to lethal cyber incidents were significantly more likely to support oversight regulation cybersecurity policies than those exposed to non-lethal cyber incidents. In contrast, there was no direct effect found between this exposure and support of *presentative* cybersecurity policies (Snider, p. 7). This difference highlights public support for a *specific* type of security policy.

Societal Considerations

In conclusion, the results of this experiment spark additional discourse about forfeiting civil liberties in exchange for security, which groups of individuals are exposed to lethal manipulation and security demands. The information gained through this article will improve policy formulation procedures that align with the public's needs, whether perceived or actual.

References

Snider, L. G. Keren, Ryan Shandler, Shay Zandani, Daphna Canetti, Cyberattacks, cyber threats, and attitudes toward cybersecurity policies, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021