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

Student Name: Gavin Bacaoan

School of Cybersecurity, Old Dominion University

Instructor Name: Professor Diwakar Yalpi

Date: 16 April 2026

Introduction/Bluff

Cyberattacks are growing issue that affect governments, businesses, and ordinary citizens around the world. In the article, the authors explain that "cyberattacks have become increasingly common" and argue that cybersecurity is now "a central issue" in modern society (Snider et al., 2021). The article focuses on how exposure to cyberattacks shapes public opinion about cybersecurity policies. One of the main ideas in the study is that when people feel threatened by cyberattacks, they may become more supportive of stronger government action. The primary purpose of this article is to examine how lethal and nonlethal cyberattacks influence support for cybersecurity policies and whether threat perception helps explain that relationship.

Relation to Social Science Principles

The article strongly reflects the seven principles of social science:

- **Relativism:** The study shows that people's attitudes toward cybersecurity policies depend on the type of cyberattack they are exposed to. Public reactions are shaped by social context, especially whether the attack appears lethal or nonlethal.

- **Objectivity:** The authors maintain objectivity by testing their arguments through an experimental design rather than relying on personal opinions. They measure participants reactions with survey instruments and statistical analysis.
- **Parsimony:** Parsimony is reflected in the author's effort to explain support for cybersecurity policies through a clear and focused mechanism: exposure to cyberattacks increases threat perception, which then shapes policy attitudes.
- **Empiricism:** Empiricism is central to the study because the authors rely on observable and measurable evidence. They use survey responses from 1,022 participants and analyze the results quantitatively.
- **Ethical Neutrality:** The article demonstrates ethical neutrality by studying policy preferences scientifically rather than making moral judgments about whether stronger cybersecurity regulation is automatically good or bad.
- **Determinism:** Determinism appears in the argument that exposure to specific kinds of cyberattacks can predict changes in attitudes toward government cybersecurity policies.
- **Skepticism:** The authors demonstrate skepticism by questioning whether all cybersecurity policies should be treated as one broad category. Instead, they test whether different forms of cyberattacks lead to support for different policy Responses.

Research Question/Hypothesis/Independent & Dependent Variables

Research Question:

Does exposure to lethal and nonlethal cyberattacks influence public support for cybersecurity policies, and does threat perception mediate that relationship?

Hypothesis:

1. Exposure to cyberattacks will increase support for cybersecurity policies.

2. Lethal cyberattacks will produce stronger support for cybersecurity alert policies.

3. Nonlethal cyberattacks will produce stronger support for cybersecurity oversight policies.

4. Threat perception will mediate the relationship between exposure to cyberattacks and support for cybersecurity policies.

Independent Variable

Exposure to cyberattacks was divided into three experimental conditions. Lethal cyberattack exposure, nonlethal cyberattack exposure, and a control group.

Dependent Variable

Support for cybersecurity policies. This includes cybersecurity prevention policy, cybersecurity alert policy, and cybersecurity oversight policy.

Types of Research Methods Used

The study uses a controlled randomized survey experiment, which is a social science research

method. Participants were randomly assigned to different conditions and exposed to simulated television reports about cyberattacks. Afterward, they completed survey measures about threat perception and policy preferences. This quantitative design includes:

- Random assignment
- Experimental manipulation
- Survey measurement

Types of Data Analysis Used

The authors used:

- Principal Component Analysis
- Descriptive Statistics
- Pairwise comparisons with Bonferroni corrections
- Path Analysis
- Bootstrapped confidence intervals

The study also used reliability testing through Cronbach's alpha to evaluate the consistency of the policy and threat perception measures.

Connections to other Course Concepts

Module 2 (Principles of Science): Uses empiricism, objectivity, parsimony, skepticism, and

Determinism.

Module 3 (Research Methods): Uses experimental research survey research, quantitative analysis, and mediation modeling.

Module 4 (Cybersecurity and Human Factors): Uses human factors because studies show how people perceive cyber threats and how those perceptions influence decisions about Cybersecurity.

Module 5 (Psychological Principles of Cyber Offending, Victimization, and Professionals): Uses Behavior responses, cyber incidents, policy response, and perceived threats.

Connections to the Concerns or contributions of Marginalized Groups

- Cybersecurity policies can affect different groups in unequal ways, especially when stronger oversight and monitoring may increase surveillance.
- **Representation limits:** The study was conducted with Israeli participants and focused on Jewish Israeli respondents, excluding some populations such as ultra-Orthodox groups. This means the findings may not fully represent the experiences of all social groups.
- **Privacy and Surveillance Concerns:** The article discusses public support for policies that may limit civil liberties and privacy. These concerns are especially important for marginalized groups and communities that are often more heavily monitored.
- **Unequal Social Impact:** Different communities may experience cyber threats and government intervention differently depending on their social, political, and cultural Position.

Overall societal contributions of the study/Conclusion

The study highlights that cyberattacks are not only technical problems but also social and political issues. By showing that exposure to cyberattacks can increase support for government cybersecurity policies through threat perception, the article helps explain how public opinion forms in response to digital threats. The findings also show that people respond differently depending on whether the attack is lethal or nonlethal, which adds nuance to our understanding of cybersecurity policy preferences. Overall, the article contributes to both cybersecurity and social science by emphasizing the relationship between fear, public opinion, policy support, and civil liberties.

Reference

Snider, K. L. G., 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

Article Link: Journal of Cybersecurity | Oxford Academic