Article review: Cyberattacks, cyber threats, and attitudes toward cybersecurity policies

Alan Schneider

Department of Cybersecurity, Old Dominion University – Norfolk

CYSE201S: Cybersecurity and Social Science

Matthew Umphlet

10 February 2024

When considering the articles relation to social science principles, (Snider et al., 2021) the principle of relativism comes to mind. In researching threat perception and intrusive cybersecurity policies, a causal relationship can be seen. The greater the threat, the article posits, the more extreme the reaction. In this case that people will accept greater limits on their freedoms when faced with a perceived threat to their safety. The conclusion that these things are related and therefore changes to one's threat perception can lead to changes in policy directly relates to the social science principle of relativism. So, too does the article follow the principle of parsimony, while the methods of data gathering: controlled randomized surveys are empirical in nature, the relational nature of threat and actions taken to ensure safety as explained by the authors is simple to understand and relate to. So, aside from the social science principles this article follows, the next paragraph will discuss the research question the authors are looking to answer.

The articles research question in the abstract is framed as follows: "Does exposure to cyberattacks influence public support for intrusive cybersecurity policies? How do perceptions of cyber threats mediate this relationship? While past research has demonstrated how exposure to cyberattacks affects political attitudes, the mediating role played by threat perception has been overlooked." (Snider et al., 2021) This hypotheses suggest that individuals will adopt more extreme solutions to cyber threats dependent on individual perception of that threat to their person, rather than making decisions in line with evidence-based conclusions. With this in mind, what kind of research methods were used by the authors to answer this question? The authors choose to use controlled randomized survey experiment design using one thousand twenty-two research participants exposed to scripted television reports to test the effect of participant

exposure to lethal and nonlethal reports of cyberattacks on support for different types of cybersecurity policies. Next, we will discuss the types of data and analysis done on the data. The controlled survey used professionally produced video clips designed to simulate news reports and out of the one thousand twenty-two participants, three groups were assigned lethal= 387, non-lethal=374 and a control group=361 that was not exposed to any news reports. The experiment used three primary variables. A predictor variable: exposure to cyberattacks assigned randomly to one of the three conditions above: lethal, non-lethal and control. A dependent variable: support for cybersecurity policies collected with twelve questions taken from two scales (McCallister et al., 2010) and (Graves et al.,2014) and finally a mediator variable: threat perception gauged by a five-item factor analysis (Hefetz A, 2017). So, with the types of data and data analysis in mind are there concepts discussed in class that can be related to the article?

The first concept that comes to mind is the basic need of safety and security in Maslow's hierarchy of needs, the article captures in a digital context, the need for appropriate cybersecurity policies and legislation to fulfill societal and individual safety needs and how a perception of a lack of safety can push people to more extreme solutions to fill that need. The second concept that has relevance to this article is personality theory specifically elements of reinforcement sensitivity. When viewed through a lens that posits individuals have differing environmental responses based on stimuli of reward or punishment. You can perhaps see how when applied to individuals and their level of exposure to cyber-threats this could account for some of the articles resulting data-based conclusions.

This article does not have a direct relation to the challenges, concerns, and contributions of marginalized groups. Unlike the Equifax breach in 2017 that affected millions of lower income Americans, or online trends surrounding racism and hate speech. This article focused on

cyber-attacks and the threat perception they generate that influences cyber policy. It is important to note that during the time this article was submitted, Israel and Iran were embroiled in an escalatory cyber conflict that targeted shipping, petroleum, and water distribution as well as hospital infrastructure (Middle East Monitor, 2021). Finally, the article contributes to society by providing an important perspective of the driving forces behind societal acceptance of increasingly intrusive cyber policies. Providing a platform in which future research efforts could design mitigation strategies designed to ensure societal decisions on cyber policy are evidence-based vice being based on arbitrary perceptions of threat.

References

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

McCallister, E., McCallister, E., Grance, T., & Scarfone, K. A. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII)*. U.S. Dept. of Commerce, National Institute of Standards and Technology.

Graves J, Acquisti A,Anderson R. Experimental measurement of attitudes regarding cybercrime. In: *13th Annual Workshop on the Economics of Information Security* 2014; Pennsylvania State University.

Hefetz A, Liberman G. The factor analysis procedure for exploration: a short guide with examples. *Cult Educ* 2017; **29**:526–62.

Middle East Monitor. (2021, November 8). *The cyberwar between Israel and Iran is heating up*. https://www.middleeastmonitor.com/20211108-the-cyberwar-between-israel-and-iran-is-heating-up/