Article #1 Review: Public Cyberattack Response

Tay Lamell

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Prof. Diwakar Yalpi

October 2, 2024

Introduction and Relation to the Principles of the Social Sciences

The article that I chose to read is titled “Cyberattacks, cyber threats, and attitudes toward cybersecurity policies.” It focuses on a study conducted in 2021 to gauge how public support for an increase in government policies to hinder cyber crimes might change following various forms of attacks. The scientific principle that best matches what’s detailed in the article is that of objectivity. Objectivity is a principle through which questions about how society should handle different cyber-offenders are attempted to be answered. Questions such as what punishments should be dealt to the offender, or how technology could be implemented to keep track of criminals. Because the article revolves around a conducted study, the principle of ethical neutrality is also entailed as the nature of the question being posed by the researchers did not involve their own personal feelings towards the subject.

Hypothesis

The question posed by the researchers was how the public’s perception of various cyber crimes affected their support for increasingly intrusive cybersecurity measures by the government. Although acknowledging that there had been studies in the past that noted exposure to cyber crimes playing a role in how the public felt about government policies (Snider et al., 2021), the researchers for this study were interested in focusing on the mediating role that initial repotings on the attacks had on those feelings. They believed that the heightened, almost sensationalized first wave of coverage would bring about more public support for intrusive policies that fit the specific crime that was being reported on.

Research Methods

In order to put their hypothesis to the test, the researchers decided to conduct a controlled randomized survey on three different groups: a lethal treatment group, a nonlethal treatment group, and a control group, which altogether totaled 1022 people (Snider et al., 2021). For the experiment, the lethal treatment group was exposed to reports on various lethal cyber crimes, the nonlethal treatment group was exposed to reports on nonlethal attacks, and the control group wasn't exposed to any reports. They also broke the policies that the participants would be looking at into three categories: prevention policies, alert policies, and oversight policies. For the experiment, lethal cyber crimes were those that had deadly consequences, and nonlethal attacks were those that primarily carried a financial toll. The reports that the groups were exposed to were all video-based, as the researchers cited videos of major attacks tending to provoke strong emotions in the viewer.

Data Analysis

The researchers chose to break the cyber crimes down into the categories of lethal and nonlethal in an attempt to focus the research groups feelings regarding the crime and, in turn, the policy to combat it. Along with collecting data on each group's news and policy response, the researchers also collected sociodemographic data (i.e.: education and income level) on the participants, as well as having them fill out surveys before and after the experiment was conducted. These surveys helped capture each participant's feelings on cybersecurity and how it may have swayed.

Findings

After the experiment was completed, the researchers took note of what they found from each group. They noted that the lethal treatment group seemed to be more in favor of policies that wanted to alert the public of cyber attacks (Snider et al., 2021), whereas the nonlethal group seemed more in favor of policies that allowed for government-based cybersecurity oversight (Snider et al., 2021). Their reasoning for their findings was that cyberattacks that resembled terrorism took precedence over those where the attacker merely sought financial gain, and therefore the lethal treatment group wanted to be kept informed about looming threats. However, the commonness of nonlethal cyber attacks caused the nonlethal group to favor policies that improved their security in the digital space.

Conclusion

While the researchers made it a point to highlight that the results of the experiment were based on people's feelings immediately after being informed of the attacks, the findings make a lot of sense to me. Even outside of cybersecurity, people tend to want to be informed of the larger issues while letting the seemingly smaller things fade into the background with the knowledge that they’re being taken care of in some way. Nonlethal cyber crimes such as those committed for financial gain may not seem like a big deal in the first waves of their reporting, but their effects can come to be just as impactful as those of lethal attacks in the long run. Rarely are financially motivated cyber attackers only walking away with ill-gotten funds. They also often come away with the personal information of people (Snider et al., 2021) in the range of dozens to millions, putting everyone at risk for financial loss, and even lethal consequences depending on whose hands it lands in.

Citations

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