Isain Cortes, Jr.

3/24/2024

CYSE 201S

Article Review #2 and Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies

Introduction:

Cyberattacks pose a huge threat to infrastructure and the ability for organizations to function properly. Thousands of cyberattacks happen each day. Some lethal and others nonlethal. When the general public gets news on a cyberattack, it constantly reminds people how far behind we are in protecting our assets digitally. Many call for change, but do people really have an idea on what policies to make or whether they should be of concern? In Keren L. G. Snider's article, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," it dives into psychological and sociological factors of civilian perceptions of being able to mediate cyber threats.

How the topic relates to the principles of the social sciences:

In readings of the cybersecurity policy attitudes article, the topic relates to the principles of social sciences through relativism, empiricism, and ethical neutrality. All three are highlighted from the reactions of cyber threat exposure and how individuals perceived policies.

The study's research questions or hypotheses:

Does exposure to different types of cyberattacks lead to heightened support for different types of regulatory policies?

Does the public differentiate between interventionist and regulatory forms of cybersecurity policies?

Exposure to lethal or nonlethal cyberattacks will lead to greater support for adopting cybersecurity policies compared with people who were not exposed to any cyberattack. In other words, exposure to cyberattacks — lethal (LC) or nonlethal (NLC) — will increase support for adopting cybersecurity policies, as compared with a control group.

People who are exposed to lethal cyberattacks (LC) will exhibit to higher support for adopting cybersecurity policies than people who are exposed to nonlethal cyberattacks (NLC).

Cyber threat perception will mediate the relationship between individual exposure to cyberattacks and support for cybersecurity policies.

The types of research methods used:

The study employed a controlled survey experiment that argued public support for governmental cybersecurity measures rises as a result of exposure to different forms of cyberattacks, and that perceived threat plays a mediating role in the relationship. This takes both a survey and experimental approach, providing information to the interest of the researcher and characteristics of individuals with the increase likelihood of supporting cybersecurity policies regardless of the measures that have to be taken.

Types of data and analysis done:

According to Snider (2021), the experiment is structured as follows, "The lethal treatment group viewed a feature report discussing several lethal cyberattacks that had taken place against Israeli targets, while the nonlethal treatment group broadcast a collection of stories pertaining to nonlethal cyber incidence. The control group did not watch any new report." It incorporated three primary variables: the predictor variable (exposure to cyberattacks), the dependent variable (support for cybersecurity policies), and the mediator variable (threat perception).

How concepts from the PowerPoint presentations relate to the article:

Modules Two, Four, and Eight contain concepts from the PowerPoints that relate to Snider's Attitudes Toward Cybersecurity Policies article. Module Two relates as it explores the concepts of social research studies to grasp an understanding of social behavior, processes, and related phenomena. Later giving an understanding of recommendations for societal improvement. Module Four relates as it dives into the psychology of the individuals being observed who were exposed to coverage of cyberattacks in different severities. Factors of exposure led to support of cybersecurity policies compelling the government regulation or oversight policies for citizens. People who were exposed to lethal cyberattacks tended to support cybersecurity policies that compel the government and security forces to alert citizens. Exposure to nonlethal cyberattacks led to support for oversight policies (COP) at higher levels than respondents who were exposed to the lethal cyberattacks manipulation or the control group (Snider 2021). Module Eight relates as it looks into the social forces of media and politics. Coverage into the realm of cybersecurity may face adequate cost of personal privacy in the face of threat actors. The public willingness to accept government policies and regulations that limit personal civil liberties and privacy is part of a delicate tradeoff between security and privacy (Snider 2021).

How the topic relates to the challenges, concerns, and contributions of marginalized groups:

They study of people being shown different kinds of cyberattacks presents the advantages and disadvantages of groups through cybersecurity knowledge, general cognitive biases in calculating risk, and distortion of cyber risks by the media.

Overall contributions of the studies to society:

The study of people being shown different kinds of cyberattacks raises a political dilemma about whether cybersecurity is a public good deserving of government investment and regulation.

Conclusion:

Keren L. G. Snider's study on civilian perceptions of cybersecurity policies reveals how exposure to cyber threats influences support for regulatory measures. Through controlled survey experiments, the research shows that both lethal and nonlethal cyberattacks can increase public backing for governmental cybersecurity measures. These findings align with key social science principles and underscore the delicate balance between security measures and individual privacy rights. Contributing valuable insights to the ongoing discourse on cybersecurity as a public good, it emphasizes the need for informed policymaking and public awareness campaigns to address cyber threats effectively.

Works Cited

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