

Ramatu Hallie

2/11/14

The three ways that this article relates to the principle of social sciences is psychologists, they look into how individuals view cyberthreats, evaluate the efficacy of policies, and how feelings like trust or fear affect their attitudes and actions around cybersecurity. Sociologists research the effects of cybersecurity laws and cyberattacks on society. They might investigate the social dynamics of cyberthreats, such as how they impact various demographic groups, how social inequality influences exposure to cyberthreats, and how social institutions influence public opinion of cybersecurity regulations. Communication experts look at how different viewers receive, recognize, and understand information concerning cybersecurity policy and dangers. They might research how the media, social media platforms, and communication techniques influence how the public views cybersecurity.

They had hypothesized that “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).” Meaning that people may be more likely to support stricter security measures for protection against future cyberattacks if they observe or experience serious cyberthreats. The research method that was used for this article was looking into different types of researcher papers and using it for their own different test, and studies. Doing this made their research more effective. They had different types of analysis, analysis of variance (ANOVA), CAP ANOVA, and mediation analysis. Where they are using different data and methods as testing. Some of the content in this article relates to some of the content that was discussed in class because they discuss cybercrime, policies, and terrorism.

Everyone, even people of color, should be aware of cybersecurity issues and attitudes toward cybersecurity policies. Marginalized populations frequently have to deal with issues like restricted access to technology and increased vulnerability to cyberattacks. They might be more concerned about unfair internet targeting or invasions of privacy. These organizations can,

however, also make significant contributions. They can support laws that uphold their rights and assist in educating others about internet safety. Together, we can tackle these problems and ensure that cybersecurity regulations are fair and available to all.

The article explains the public's understanding of cybersecurity dangers and regulations, assisting decision-makers in developing winning plans. It encourages inclusive cybersecurity practices by taking marginalized populations into account. In general, it improves social responses to cyberthreats and influences policy decisions.

<https://academic.oup.com/cybersecurity/article/7/1/tyab019/6382745?searchresult=1>