New Knowledge, Better Decisions: Promoting Effective Policymaking Through Cybercrime Analysis Review

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Dr. Leigh Armistead

November 4, 2023

How does the topic relate to social science principles? (3 or more)

The article's study of cybercrimes and their impact can be related to the principle of relativism in social science. Cybercrimes and the perceptions of these crimes can vary across different cultures and societies. What is considered a cybercrime in one culture may not be viewed the same way in another. The principle of relativism recognizes the importance of considering cultural and contextual differences when analyzing social phenomena, which applies to understanding cybercrimes and their interpretations in different societies.

The principle of skepticism in social science encourages a critical and questioning approach to research findings and claims. When examining the article's content, skepticism can be applied to assess the validity and accuracy of media reporting on cyberterrorism. Media coverage is subject to biases, inaccuracies, and sensationalism, and skepticism plays a role in scrutinizing these reports to determine their accuracy and potential impact on public perceptions of cyber threats.

The principle of ethical neutrality suggests that social scientists should strive to maintain an unbiased and impartial stance in their research, avoiding the imposition of their personal values or judgments. In the context of the article, ethical neutrality is relevant when examining the research on cyberbullying and its impacts. Researchers should maintain an objective and nonjudgmental approach when investigating the prevalence and trends of depression among cyberbullied adolescents, as this can help ensure the integrity of the study's findings and recommendations while avoiding bias or moral judgment.

What are the research questions and hypotheses?

The first study in the article aimed to investigate the evolution of research in the fields of cybercrime and cybersecurity, focusing on the period from 1995 to 2021. The primary research

question is, “How has research in the areas of cybercrime and cybersecurity evolved during this time frame, and what are the key themes and trends that have emerged?” The first study also hypothesized that the research landscape in cybercrime and cybersecurity has undergone substantial changes over the specified period. The study anticipated identifying discernible patterns and themes within the research literature signifying the evolution of these fields.

The second study’s investigation sought to assess the influence of the media on public perceptions of malicious cyber activity, with a particular emphasis on cyberterrorism. The central research question is framed as follows: To what extent does media coverage shape public perceptions of cyberterrorism, and is there evidence of overuse or imprecise utilization of the term "cyberterrorism" in media reporting? It hypothesized that media coverage exerts a significant impact on public perceptions of cyberterrorism, contributing to heightened levels of fear among the general population. Furthermore, the study posits that the term "cyberterrorism" is frequently employed imprecisely in media coverage, thereby exacerbating irrational and unnecessary fears.

The third study’s research aimed to explore the prevalence and temporal trends of depression among adolescents who have experienced cyberbullying. Additionally, the study seeks to ascertain whether gender and racial/ethnic disparities exist in the observed impact. The central research question is formulated as follows: What is the prevalence and temporal trajectory of depression among adolescents who have been subjected to cyberbullying, and are there variations in the experience of depression based on gender and racial/ethnic backgrounds? The hypothesis for the study posits that a correlation exists between instances of cyberbullying and the manifestation of depressive symptoms among adolescents. It is further hypothesized that

such a correlation may exhibit variances across gender and racial/ethnic lines, underscoring the complex interplay of these factors.

Lastly, the fourth study focused on the examination of potential relationships between the age, gender, and nationality of hackers and the specific types of electronic attacks in which they engage. The primary research question is articulated as follows: Are there discernible connections between the age, gender, and nationality of hackers and the nature of electronic attacks they perpetrate? The study hypothesized that publicly available data sources can yield valuable insights into patterns of hacker behavior, including the deployment of distinct attack methods. These patterns may offer predictive value in determining the demographics and behavioral tendencies of hackers. The analysis anticipated identifying specific correlations between the age, gender, and nationality of hackers and the types of electronic attacks they employ.

What type of research methods are used?

The first study used archival research. They conducted a review based on the Web of Science core collection database, which involves examining and analyzing existing published research.

The second study used surveys and quantitative analysis. This study utilizes both survey data and quantitative analysis to assess the influence of media on public perceptions of cyberterrorism.

The third study, like the first, also used archival research. The study utilizes data from the Youth Risk Behavior Survey conducted by the U.S. Centers for Disease Control and Prevention (CDC), which involves analyzing existing survey data.

The last study in the article also used archival research. The research in this study involves examining publicly available information on hacking from the U.S. Department of Justice (DOJ) to discern and analyze patterns of behavior from hackers. This method can be categorized as archival research.

The methods used in the studies primarily fall under archival research, where existing data and information are analyzed to address specific research questions. The second study also involves survey data and quantitative analysis to assess media influence.

What types of data and analysis are done?

For the first study, the researchers analyzed data from the Web of Science core collection database, which includes publications related to cybercrime and cybersecurity from 1995-2021. The analysis involved data visualization and examination of thousands of publications to identify key themes and trends among researchers in the field.

In the second study, they used quantitative and qualitative analyses of survey data to assess the influence of the media on public perceptions of cyberterrorism. Their analysis included quantitative techniques to assess the impact of media coverage on public fear and qualitative analysis to examine the imprecision in the use of the term "cyberterrorism" in media reporting.

The data for the third study was obtained from the U.S. Centers for Disease Control and Prevention (CDC) Youth Risk Behavior Survey, which provides information on the prevalence and trends of depression among cyberbullied adolescents. The analysis involved examining and interpreting the data to understand the scope and trends of depression among cyberbullied adolescents.

Lastly, for the last study, the data used in this study came from publicly available information on hacker behavior and electronic attacks from the U.S. Department of Justice. The analysis focused on discerning and analyzing patterns of behavior from hackers, with the aim of determining if specific targets or methods used to hack could be leveraged to predict a hacker's age, gender, and location.

How does this article relate to concepts from class? (4 or more)

One concept from class this article mentions is victimization. Victimization refers to the state or process of becoming a victim of cybercrimes or cyberattacks. This includes individuals, organizations, or entities that experience harm, loss, or damage as a result of various malicious activities conducted in the digital realm. Cyber victimization can encompass a wide range of incidents, such as hacking and data breaches, phishing social engineering, and also cyberbullying. Victimization in cybersecurity is a serious concern, and it often has legal, financial, and emotional consequences for the affected parties. Cybersecurity measures and awareness are crucial to minimize the risk of victimization and mitigate its impact when it does occur.

Another concept we've covered in class is cyberbullying. Cyberbullying refers to the malicious and harmful activities conducted in a digital environment with the intention of targeting and harassing individuals or organizations. It involves the use of technology and online platforms to intimidate, threaten, or harm the reputation, privacy, or digital well-being of a victim. Cyberbullying can take various forms, such as harassment and threats, doxing, and impersonation. It has severe consequences not only on an individual's psychological well-being but also on their digital security. It can lead to identity theft, cyberattacks, and breaches of personal or sensitive data.

A third concept both the article and our lectures have mentioned is cybercrime. Cybercrime refers to the criminal activities that are carried out in the digital realm using computer systems, networks, and technology. Cybercrime examples are hacking and unauthorized access, malware attacks, and DDoS attacks. In cybersecurity, the prevention, detection, and mitigation of cybercrime are crucial to safeguarding digital assets and maintaining the security and privacy of individuals, organizations, and governments. Cybersecurity professionals work to develop and implement security measures and technologies to counteract cybercriminal activities and protect against the evolving threats in the digital landscape.

The fourth concept from class that is related to the article is cybersecurity. Cybersecurity refers to the practice of protecting computer systems, networks, and digital data from various forms of threats and vulnerabilities. It encompasses a broad range of strategies, technologies, and measures aimed at safeguarding information and technology assets from unauthorized access, data breaches, cyberattacks, and other risks. Cybersecurity involves activities such as implementing robust security protocols, deploying firewalls and intrusion detection systems, encrypting data, conducting regular security audits, and training personnel to identify and mitigate potential security threats. The overarching goal of cybersecurity is to maintain the confidentiality, integrity, and availability of digital assets, ensuring that they are secure and resilient against the evolving landscape of cyber threats.

What are the overall societal contributions of the study? (2 or more)

The studies contribute to the enhancement of cybersecurity knowledge by providing insights into various aspects of cybercrimes, cyberterrorism, and cyberbullying. Understanding the patterns, trends, and impacts of these phenomena allows policymakers, law enforcement agencies, and cybersecurity experts to make more informed decisions and develop effective

strategies for addressing these threats. This, in turn, can lead to improved cybersecurity measures and the protection of individuals and organizations from online threats.

The study on media influence on perceptions of cyberterrorism sheds light on the potential effects of media reporting on public fear and perceptions. By highlighting the overuse and imprecise use of the term "cyberterrorism" in media coverage, the research contributes to media awareness and responsible reporting practices. Media outlets can use these findings to improve their reporting on cyber-related issues, leading to more accurate and less sensationalized reporting. This, in turn, can help reduce unnecessary fear and panic among the general public regarding cyber threats.

The study on the prevalence and trends of depression among cyberbullied adolescents has significant societal implications. It brings attention to the mental health impacts of cyberbullying on adolescents. By identifying the correlation between cyberbullying and depression and recognizing gender and racial/ethnic disparities, this research raises awareness about the need for targeted interventions and support systems for affected individuals. This can lead to improved mental health care for young people and better-informed anti-cyberbullying efforts in schools and communities.

These societal contributions demonstrate the practical and valuable outcomes of the research conducted in the articles, ranging from improved cybersecurity strategies and responsible media reporting to better mental health support for individuals affected by cyberbullying.

References

Givens, A. (2018). New Knowledge, Better Decisions: Promoting Effective Policymaking Through Cybercrime Analysis. *International Journal of Cybersecurity Intelligence & Cybercrime*, *6*(1). https://doi.org/10.52306/oyxb3896