

Article Review #2

Student Name: Michael Everett

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Yalpi, Diwakar

Introduction/BLUF

An article titled “Navigating the Digital Frontier: New Perspectives on Cybercrime and Governance” and written by Kayser, Dearden, Parti, and Choi (2022), continues to elaborate the implications of the changes that are being observed within cybercrime because of the advancements that are taking place through technology. In the article it is mentioned how highly recommended that governments, organizations, and researchers must come and work together in figuring out ways to deal with cyber threats. The overall topic of the article is that cyber governance and international collaboration are required to safeguard individuals and businesses online.

Relation/Connection to Social Science Principles

The relevance of the article to the field of social science is that the article investigates the ways and the means through which people interact online and the resultant effect of the online behavior towards cybercrime. The article encompasses various principles that are key to the field of social science and include aspects such as empiricism, objectivity, and determinism. The article touches on the issue of culture and the way people’s values are impacted to influence online behavior.

Research Question / Hypothesis / Independent Variable / Dependent Variable

The article focuses on the question of the importance of enhanced cyber governance, international collaborations, and the extent to which these issues affect the issue of cybercrime. The authors of the paper propose a hypothesis relating to the importance of having enhanced structures of governance and international collaborations that are vital for fighting cybercrime

and improving practices of cyber security. The independent variable within the research paper is the implementation of policies and international collaborations concerning cyber governance that are currently applied and proposed. The other variable constitutes the reduced level of cybercrime and the level of online safety of individuals.

Kinds of Research Methods Employed

The authors applied a qualitative research method, mostly through a literature review. The researchers reviewed various papers that contain research related to cybercrime and the field of governance. The authors did not carry out any research to obtain data but reviewed various papers that contained information used to construct a new understanding of collaboration and governance for cybersecurity.

Different Kinds of Data Analysis Techniques

The paper applied thematic analysis, which involves the search for common notions and themes among various studies. The authors sought out to compare various findings that emerged from different studies to demonstrate the weaknesses within international co-operation and the best practices of cyber governance. The analysis strived to interpret trends and the notions that govern cybercrime.

Connections to Other Course Concepts

This article proves several important points that are brought up within the framework of our course. This includes the role of human factors within cybersecurity, the issue of social engineering, and the role of societal behavior within online risk. This article confirms that cybercrime cannot be addressed through the use of technology alone and that the motives of human behavior play a key role within the issue of online security.

Links to the Concerns of Marginalized Groups

The article also highlights that vulnerable groups are even more at risk online because of a lack of cyber security capability and resources. These groups of people are considered vulnerable and might be taken advantage of online through online scams and online fraud. The authors state that the cyber security gap needs to be bridged if the vulnerability issue is to be fixed.

Conclusion:

Furthermore, the article's importance to society and relevance to society cannot be emphasized since it shows that the responsibility to be cybersecure rests not only on individuals but also on the community. Moreover, the article shows that the future of cyberspace security depends not only on the knowledge and advancements of technology but also on the understanding of the community.

Reference

Kayser, C. S. , Dearden, T. , Parti, K. & Choi, S. (2025). Navigating the Digital Frontier: New Perspectives on Cybercrime and Governance. *International Journal of Cybersecurity Intelligence & Cybercrime*, 8(2), - . DOI: <https://doi.org/10.52306/2578-3289.1222> Available at: <https://vc.bridgew.edu/ijcic/vol8/iss2/1>