Article Review #1: Navigating the Digital Frontier: New Perspect Cybercrime and Governance

Leyah Knox

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 2/25/2026

Introduction/BLUF

The article I chose explains how cybercrime is growing in the digital age and it states the governance and policy frameworks that are aware of the changes. The bottom line up front is cybercrimes can no longer be accurately understood or governed while using technical or legal paradigms. Interdisciplinary approaches taken in social sciences, and collaborative governance are kind of necessary to the complexities of the modern cyber threats.

Relation/Connection to Social Science Principles

This article is deeply connected to the social science principles. Empiricism is applied because it is grounding the discussions of the cybercrimes in observed trends and documented cases instead of them being speculated. The second principle is determinism. It appears the authors are

exploring how societal structures such as the legal institutions influence the current and management of these cyber threats. The next one the article reflects on is objectivity which does emphasize evidence based analysis vs the normative judgements. Skepticism is also in this because it is obvious questioning traditional governance mechanisms as sparse for emerging cybercrime forms. The fifth one is parsimony which is applied by the authors synthesizing complex socio technical interactions into the governance recommendations. I also see a bit of humanism in this article because it states consideration of how these cyber threats affect people, communities, and even some organizations. The last one is ethical neutrality which is addressing that cybercrimes impact a lot of things across contexts. These principles help show cybercrime not just as a technical problem, but it also shows it as a societal challenge that is influenced by human behavior and policy structures.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

Research Question: How should policies and governance systems frameworks evolve to effectively address the changing nature of cybercrime in the digital age?

Hypothesis: Traditional governance models are poor for managing contemporary cybercrime

Independent Variable: Changes in the digital technology and cybercrime patterns

Dependent Variable: effectiveness of governance systems

Types of Research Methods used

The research methods the authors used in this article are qualitative. Instead of showing quantitative research, the article does synthesize literature, and policy documents. They also make sure to give credit to other authors who they found this information from. The techniques they used include literature review, and conceptual.

Types of Data Analysis used

Due to the article being conceptual the analysis doesn't rely on statistical or experimental data analysis. It uses qualitative thematic analysis, which means it identifies key themes and patterns in the research that is already there. The authors compare theoretical perspectives to highlight the opportunities for improvement.

Connections to other Course Concepts

The articles connect to the modules in this course because it emphasizes human and social behavior of cyber threats. It shows us that cybercrime isn't just only a technical problem but it is also a social problem. Which does require them to understand the human behavior of cyber crimes and cyber threats. The article also shows human decisions and social structures are framed how cyber threats emerge and how defenses are being used. It shows people cybersecurity can be solved with societal thinking vs technical tools.

Connections to the Concerns or contributions of Marginalized Groups

The article addresses digital inequality and disparities. One of the key implications that was explained in the article was the digital divide where people and organizations had limited access to technology.

Overall societal contributions of the study/Conclusion

To sum everything I talked about up, the study contributes to the understanding of cybersecurity by seeing cybercrime as a complex social phenomenon. This article shows how its implicants extend technical defense and then call for a collaborative approach across institutions, and social science perspectives to shape the effectiveness of cybersecurity strategies. By showing us this, the article works to get our understanding of cyber threats as a societal viewpoint which requires both societal and technological responses. This highlights the need for more adaptive frameworks, and evidence based policies for all digital users. This supports the efforts of digital societies.