

Article Review #2: The Role of Intentional Law in Combating Illicit Drug Trafficking Via the
Dark Web

Shelton Jones

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity & Social Sciences

Professor Yalpi

April 16th, 2026

BLUF:

The article examines cybercrime through a social science lens, showing that human behavior, social structures, and inequality significantly influence both cyber offending and victimization. The article itself also highlights how technological threats are rooted in social dynamics rather than just technical vulnerabilities.

Connection to Social Science Principles

The article aligns with key principles of sociology, criminology, and psychology by showing how behavior in cyberspace can mirror offline social patterns. Concepts such as social learning, rational choice, and routine activity theory help explain why individuals engage in cybercrime. The study suggests that cybercriminals are influenced by perceived rewards, low risk, and social environments that normalize deviant behavior (Cybercrime Journal, n.d).

Research Question, Hypothesis, and Variables

The primary research question explores what social and behavioral factors contribute to cybercrime participation and victimization. The hypothesis proposes that individuals exposed to certain online environments and lacking awareness or protective measures are more likely to become victims or offenders. The independent variables include user behavior, cybersecurity awareness, and online exposure, while the dependent variable is the likelihood of experiencing or engaging in cybercrime.

Research Methods

The article employs a quantitative research approach, using surveys or structured data collection to analyze behavioral patterns. This method allows for measurable comparisons and statistical testing of relationships between variables. The structured design ensures reliability and supports generalizable findings across populations.

Data & Analysis

The data consists primarily of numerical responses related to user habits, risk perception, and cyber experiences. Statistical analysis, such as correlation or regression, is used to determine the relationship between variables. This approach helps identify trends, such as increased risk associated with poor cybersecurity practices of high online activity.

Connection to Course Concepts

The article reflects PowerPoint concepts such as risk assessment, human factors in cybersecurity, and behavioral vulnerabilities. It reinforces the idea that technology alone cannot prevent cyber threats; human decision-making plays a critical role. Concepts like threat modeling and social engineering directly connect to the study's findings.

Marginalized Groups & Social Impact

The article highlights disparities in cybersecurity awareness and access, particularly among marginalized groups. Limited resources, digital literacy gaps, and systemic inequalities increase vulnerabilities to cybercrime. This raises concern about digital equality and the need for inclusive cybersecurity education and policy interventions.

Contributions to Society

This research contributes by emphasizing prevention through education and behavior change. It informs policymakers and cybersecurity professionals about the importance of addressing human factors. The study promotes more effective and equitable cybersecurity strategies.

Conclusion

The article demonstrates that cybercrime is not just a technical issue but a social one. Understanding behavioral patterns, social inequalities, and human decision-making is essential for reducing cyber threats and building a safer digital environment.

Reference

<https://cybercrimejournal.com/manuscript/index.php/cybercrimejournal/article/view/487/146>