Article Review: Cyber Deviance Among Adolescents

Student Name: Patrick Bays

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/14/2026

Introduction/BLUF

This study examines illegal downloading and hacking among adolescents across 30 countries using data from the second International Self-Report Delinquency Study (ISRD-2). The primary objective is to investigate how individual and societal factors (such as family, school, and neighborhood environments) predict cyber deviance. BLUF: Family attachment, school bonding, and individual self-control are good predictors of cyber deviance, but traditional theories in criminology explain less variance in online behaviors compared to offline delinquency.

Relation/Connection to Social Science Principles

The study incorporates several principles of social sciences. First, it incorporates Determinism by positing that adolescent behavior is determined by social structures such as parental monitoring and disorganized schooling rather than just technical ability. Secondly, Objectivity is demonstrated in the study through the use of standardized self-report surveys across 30 different nations to minimize researcher/locality bias. Thirdly, the study applies Relativism by comparing deviance rates across diverse cultural environments such as the Mediterranean and Post-Socialist regions to see if behavioral norms are universal of context-specific. Finally, it demonstrates Empiricism by relying on quantitative data and statistical regression to validate theoretical claims about delinquency.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Questions: Do adolescents differ in their engagement in cyber deviance around the world? Are traditional theories in criminology applicable to cyber deviance in comparison to predicting offline delinquency?
- Hypothesis: Stronger parental attachment and school bonding will decrease deviance, while low self-control and positive attitudes toward violence will increase it.
- Independent Variable: Parental Control, attachment to family, self-control, attitudes towards violence, school attachment/disorganization, and neighborhood integration.
- Dependent Variable: Self-reported perpetration of illegal downloading and hacking within the last 12 months.

Types of Research Methods used

The study uses quantitative research methods. Data was collected through a large-scale international survey, the IRSD-2, involving 68,507 students in the 7^{th}, 8^{th}, and 9^{th} grades. This method allows the researchers to gather a massive, cross-national dataset that provides a broader perspective than the small single-nation college samples used in earlier studies.

Types of Data Analysis used

The author used logistic regression analysis to examine the dependent variables of hacking and downloading. Analysis was conducted using the 'glm' function of R, where variables were tested for multicollinearity and significance levels were set at $p < 0.05$. Adjusted McFadden R^2 scores were also used to compare the power of the models across different types of delinquent acts to explain delinquency rates.

Connections to other Course Concepts

The study reinforces concepts from the most recent course module. Carley (2020) defines the field of Social Cybersecurity as the use of computational social science to understand cyber-mediated human behavior, which mirrors Udris's approach to identifying predictors of digital deviance. The study also links to the concept of risk surfaces by identifying computer availability at home as the strongest predictor of cybercrime. It also aligns with expected social behaviors of cybersecurity professionals, such as systemic thinking, by showing that cyber risk is interconnected with a given individual's offline social environment.

Connections to the Concerns or contributions of Marginalized Groups

The research highlights significant implications for marginalized groups, specifically regarding the gender gap and socioeconomic status. Udris finds that hacking is overwhelmingly male-dominated, (8.29% vs 2.58%), which points to a hacking culture that may discourage or exclude women. Additionally, the study identifies a kind of digital divide, where computer availability at home significantly influences the likelihood of engaging in or learning about hacking. Computer availability, in this instance, is used as a proxy for the variance of socioeconomic resources among individuals that reported to the dataset. This suggests that individuals from lower-income backgrounds may face different barriers to entering spaces or careers in tech, or may be less represented in these behavioral models.

Overall societal contributions of the study/Conclusion

In conclusion, the study advances the understanding of cybersecurity by proving that domestic social bonds (i.e. family, school, and neighborhood) are more critical predictors of cyber deviance than country of origin. Its primary societal contribution is the empirical evidence that, while traditional theories are indeed relevant, they explain less variance in *digital* crime than in offline crime, demonstrating a need for new cyber-specific sociological theories. This research helps society shift from viewing cybercrime as a purely technical problem to a social one that required better parenting, monitoring, and educational bonding.

Reference

Udris, R. (2016, October 26). *Cyber Deviance among Adolescents and the Role of Family, School, and Neighborhood: A Cross-National Study*. International Journal of Cyber Criminology. https://www.cybercrimejournal.com/pdf/Udrisvol10issue2IJCC2016.pdf