

**Article Review #2: Cyber offending predictors and pathways in middle adolescence:
Evidence from the UK Millennium Cohort Study**

Student Name: Thomas Gable

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/7/2025

Introduction/BLUF

The purpose of this article is to determine which personal, social, family, and environmental factors increase adolescents' likelihood of committing cybercrime.

Relation/Connection to Social Science Principles

The article properly represented the principle of objectivity by using a quantitative, statistical analysis to analyze data collected on individuals over time. Furthermore, they presented findings that refuted some of their predictions, showing that they didn't hold obvious confirmation bias. Moreover, the piece reflected the principle of empiricism by evaluating real-life data relating to individuals' experiences and characteristics, such as gender, family conditions, and mental health. Lastly, the principle of Determinism is present in the text, as the study was based on investigating how different aspects of an individual's life increased the chance of them participating in cybercrime.

Research Question/Hypothesis/Independent Variable/Dependent Variable

The authors of this article were attempting to figure out which personal, social, family, and environmental factors could predict cybercrime offending in adolescence and if they differed from traditional crimes. Their hypothesis was "We predicted that being male, having higher cognitive scores (i.e., for the required skillset), lower parental monitoring, lower school connectedness, a diagnosis of autism, spending more time online and online gaming, spending less time in offline leisure activities, and engaging in cyber offending at age 14 would predict cyber offending at age 17, over and above that of predictors of more traditional (offline) offending (such as substance use and socioeconomic status)" (Maras, et al., 2023, p. 3). The independent variables were the different personal, social, familial, and environmental attributes they examined. More specifically, these included things such as gender, parental monitoring, gaming participation time, well-being, and family relationships. The Dependent variable was whether the individual participated in cybercrime by 17 years old.

Types of Research Methods Used

The researchers used a dataset that originated from the UK Millennium Cohort Study, which asked children and their families a set of questions regarding their lives from 9 months of age to seventeen years old. They asked things like their age, gender, if domestic violence is present, how long they play video games, if they have ever participated in traditional crime, and if they express mental health concerns. Then, at ages 14 and 17, the participants were asked if they had committed cybercrime. They used a quantitative data analysis.

Types of Data Analysis used

The researchers then looked for patterns of characteristics among the kids using statistical analysis, examining which factors were consistently present in cyber offenders. For example, they looked to see what percentage of the kids who endured low parental monitoring committed cybercrime. They then used a logistical regression to see if different groups of these possible predictors had any relationship to one another and an influence on the possibility of cybercrime offending by seventeen years old.

Findings

First off, out of 13,277 adolescents they examined, they found that only 5.6% committed any cybercrime by age fourteen, dropping to 3.8% by age seventeen, so it was relatively rare overall. The analysis also revealed that a significantly higher percentage of boys cyberoffended than girls. Overall, the traits that were consistently present in the offenders were male, high video game playing, the presence of familial domestic abuse, low parental oversight, poor mental health, rejection from school, and prior traditional crime offending. Furthermore, they found that those who participated in real-life recreational activities were more likely to commit cybercrime, although the relationship was minute. The factors that were not predictors of cybercrime were an autism diagnosis, parents' financial status, deviant peer association, and high cognitive ability. Finally, the study concluded that the characteristics of cyber offenders were not very different from those who committed traditional crime. However, cybercrime offenders tended to grow out of that behavior, which was the opposite of traditional crime.

Connections to other Course Concepts

One concept from the course that this study tested was the influence of online peer networks and behavioral theories on participants. They examined whether peer association and participation in online communities were predictors, but found no relationship, although they called for further research due to their limitations. One theory that we learned, which was heavily involved, was the Psychodynamic theory, which says that early childhood experiences influence behavior. Rejection from school and the presence of parental domestic abuse were linked to cyberoffending, which could negatively influence emotions, supporting this theory. Two of the “Big Five Personality Traits” were present in participants who cyber-offended, one being Neuroticism, as represented by the low mental health predictor. The other was Extraversion, which can be represented by participation in real-life activities, which increases the likelihood of cybercrime. Lastly, the study examined families' financial and class status, which could be linked to our most recent module on economics. They attempted to see if adolescents who were able to obtain more money, and therefore have access to more advanced tools and knowledge, led to cybercrime, but found no relationship.

Connections to the Concerns or Contributions of Marginalized Groups

It was found that those with poor mental health and participation in self-harm were more likely cyber offend. This shows how emotional distress, inaccess to therapy, and exclusion from social environments can cause marginalized youth to act uncharacteristically, harming others and potentially their future. These behaviors can result from frequent feelings of loneliness and incompetence, emphasizing the need for more supportive resources. Furthermore, it was discovered that autistic adolescents were not likely to commit cybercrime, contrary to the researchers' predictions. Disabled individuals are often stereotyped as being chronically online or antisocial, which might lead the masses to unfairly assume they will be more likely to engage in cybercrime. However, this study showed no strong relationship between the two, disproving these baseless beliefs, highlighting the need for more truthful and compassionate views.

Overall societal contributions of the study/Conclusion

Overall, this study concluded that theories such as the social learning and differential association were not predictors of cybercrime in adolescents, even though they are widely believed to be associated. However, the authors did note that there were limitations in their peer influence data, which may have skewed this result. Furthermore, they concluded that some of their findings, such as low parental oversight and high online gaming activity, partially affirm the routine activity theory. The main theory they found to explain cybercrime was the ecological systems theory, which states that multiple environmental, personal, and social factors work together to influence an individual's behavior, not just one. The researchers assert that to prevent cyber offending in adolescence, parents should ensure their children are in a positive environment with strong oversight.

Reference

1. Maras, K., Sweiry, A., Villadsen, A., & Fitzsimons, E. (2024). *Cyber offending predictors and pathways in middle adolescence: Evidence from the UK Millennium Cohort Study*. Computers in Human Behavior, 151, 108011. <https://doi.org/10.1016/j.chb.2023.108011>