International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 1 Article 1

3-2022

Understanding Cybercrime Offending and Victimization Patterns from a Global Perspective

cybercrime awareness; cybercrime offending; cybercrime victimization; global perspective

Lee. (2022). *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(1), 1-3.

Understanding Cybercrime Offending and Victimization Patterns from a Global Perspective

Jin R. Lee*, Ph.D., George Mason University

Keywords: cybercrime awareness; cybercrime offending; cybercrime victimization; global perspective

Abstract:
Cybercrime research within criminology and criminal justice sciences has increased over the past few decades, improving the knowledge and evidence-base around cybercrime offending and victimization generally. While earlier cybercrime studies were based primarily in the United States, there has been a recent surge in studies using international samples and multidisciplinary approaches to understand cybercrime patterns. The current issue of the *International Journal of Cybersecurity Intelligence and Cybercrime* consists of four articles that seek to advance our understanding of cybercrime behaviors from a global perspective. To that end, the objective of this paper is to provide a brief overview of the articles included in this issue. The overview will comprise a summary report of each study's objectives, main findings, and implications. Exploring cybercrime from an international perspective underscores both the global nature of the phenomena and the need to form deeper insights into its unique properties.

Introduction

Cybercrime research within criminology and criminal justice sciences has increased over the past few decades, improving the knowledge and evidence-base around cybercrime offending and victimization generally. These contributions often focus on exploring the causes and correlates of computer-dependent (i.e., actions that did not exist before the advancement of the computer and digital technology) and computer-assisted (i.e., actions that pre-dated the Internet and digital technology, but were enhanced as a result of it) behaviors using a variety of different methodologies and theoretical frameworks. While earlier cybercrime studies were based primarily in the United States (U.S.), there has been a recent surge in studies using international samples and perspectives to understand cybercrime patterns. This current issue of the *International Journal of Cybersecurity Intelligence and Cybercrime* consists of three studies that seek to advance our understanding of cybercrime behaviors from a global perspective. Specifically, the articles included in this issue explore: (1) the mediating role of moral beliefs in the relationship between parenting practices and cyberbullying offending among South Korean adolescents; (2) the social construction of Internet fraud as an innovative means to combat economic depravity in Nigeria; and (3) an analysis of U.S. government alerts and advisories to understand different cybercrime actor types and the tactics used during cyber operations. A brief overview of the research featured in this issue is provided below.

*Corresponding author
Jin R. Lee, Ph.D., Department of Criminology, Law and Society, George Mason University; 4400 University Drive, MS 4F4; Fairfax, VA 22030, U.S.A.
Email: jlee331@gmu.edu

Jaeyong Choi, Seungmug Lee, and Layne Dittman (2022, this issue) explored the mediating effects of moral beliefs on parenting practices and cyberbullying offending in their article, "The relationship between parenting practices and cyberbullying perpetration: The mediating role of moral beliefs." While extant literature has found that parenting styles and practices differentially influence the development of morality in children (i.e., value statements and beliefs that are in favor of certain behaviors and emotions), limited research has explored the interaction effect of adolescents' moral beliefs on parenting practices and cyberbullying perpetration (see Choi, Lee, & Dittman, 2022). Using a cross-sectional sample of South Korean adolescents ($n = 779$), the study explored the mediation effects of youths' moral beliefs on the relationship between parenting practices and cyberbullying offending. Results revealed that parental supervision and excessive parenting behaviors were significant predictors of cyberbullying offending (Choi, Lee, & Dittman, 2022). Relatedly, the analysis revealed that parenting practices was partially mediated through adolescents' moral beliefs (Choi, Lee, & Dittman, 2022). This study provides support to suggest that parenting practices are critical in the development of moral beliefs and cyberbullying offending. Given the importance of parenting, the authors suggest further research be conducted on parents' role in instilling moral beliefs among children.

In the article, "Social construction of Internet fraud as innovation among youths in Nigeria," Austin Ayodele, Jonathan Kehinde Oyedeji, and Huthman Olamide Badmos (2022, this issue) conducted in-depth qualitative interviews of 15 Nigerian residents to examine their perceptions of Internet fraud. Using Merton's (1968) Anomie/Strain Theory as the guiding theoretical framework, the study found that individuals viewed Internet fraud as an innovative means to economic survival. Specifically, the study found that individuals engaged in Internet fraud as a means to support themselves financially during times of difficult economic conditions, emphasizing necessity over nefarious intent. This finding represents a stark contrast from the normative perspective that views Internet fraud as an act solely inspired by deviant motivations. In terms of its behavioral traits and characteristics, the study revealed that Internet fraud in Nigeria is socially organized and based heavily on specializations, with social hierarchies grounded on the accumulation of clients and wealth. Further, the study found that skilled offenders were more likely to exploit loopholes within existing legislation to avoid arrest and apprehension. The authors conclude by suggesting the imperative need to create a better economy with more legitimate employment opportunities in Nigeria.

In the last article, "Cybersecurity risk in U.S. critical infrastructure: An analysis of publicly available U.S. government alerts and advisories," Zachary A. Lanz (2022, this issue) employed the text analysis program, Profiler Plus, to extract information from 1,574 U.S. government alerts and advisories to generate insights into different cyber threat actor types, tactics that can be used for cyber operations, and sectors of critical infrastructure at risk of an attack. The study revealed that cyber-threat reporting has increased exponentially throughout the past decade, with more comprehensive reporting of cybercrime demonstrating a greater understanding of the cyber-risks present across the different sectors of government. Overall, this study enhances cyber-threat intelligence by providing a deeper understanding of the trends in public information sharing, as well as identifying limitations in open-source cyber-threat reporting.

Concluding Remarks

Though obtaining deeper understanding of social phenomena is vital to social science research, the ability to translate these findings into tangible policies and implications is crucial. The four articles featured in this issue of the *International Journal of Cybersecurity Intelligence and Cybercrime* demonstrate the unique properties of cybercrime behavior and the need to consider creative solutions to both cybercrime offending and victimization. Specifically, these articles demonstrate the importance of considering global perspectives in the fight against cybercrime. Future studies should continue to explore cybercrime from an international perspective and seek solutions that cover the wide breadth and scope of cybercrime.

References

Ayodele, A., Oyedeji, J. K., & Badmos, H. O. (2022). Social construction of Internet fraud as innovation among youths in Nigeria. *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(1), 23-42.

Choi, J., Lee, S., & Dittmann, L. (2022). The relationship between parenting practices and cyberbullying perpetration: The mediating role of moral beliefs. *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(1), 4-22.

Lanz, Z.A. (2022). Cybersecurity risk in U.S. critical infrastructure: An analysis of publicly available U.S. government alerts and advisories. *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(1), 43-70.