International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 2 Article 1

8-2021

Editorial introduction to the special issue: Supporting future scholarship on cybercrime

Choi et al. (2021). *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 1-3.

Editorial Introduction to the Special Issue: Supporting Future Scholarship on Cybercrime

Jaeyong Choi*, West Chester University, U.S.A.
Brandon Dulisse, University of Tampa, U.S.A.
Richard L. Wentling, Pennsylvania State University, U.S.A.
Nathan Kruis, Pennsylvania State University, U.S.A.

Keywords: North Korean cyberterrorism; COVID-19; fear of online victimization

Abstract:
This editorial introduction will present an overview of the three papers published in this special issue of the International Journal of Cybersecurity Intelligence and Cybercrime. The winners of the student paper competition during the 2021 Whitehat Conference have prepared their papers for this special issue. Their research directs our attention to key issues regarding cybercrime that have often been overlooked in the literature ranging from North Korean cyberterrorism to the relationship between COVID-19 and cybercrime and to fear of online victimization.

Introduction

As rapid technological advances have fundamentally changed how a majority of individuals interact, so too have recent inquiries into how some individuals use these new technologies to commit crime. Commonly referred to as cybercrime, these deviant and illegal interactions through digital and other technological means have created a fertile area of study for social scientists, even though historically the focus of criminologists has been limited mainly to traditional street crimes (Payne & Hadzhidimova, 2020). Fortunately, the number of publications and original research inquiries on topics related to cybercrime has continued to increase in recent years. Nevertheless, it is fair to say that cybercrime has not been treated as a fundamental area that criminologists should prioritize when studying criminological topics. For example, the proportion of publications related to cybercrime is incredibly low compared to traditional criminological topics, especially in top-tier refereed journals within the field. The obstacles to understanding cybercrime are not just in the scholarly domain but also within the educational setting. Students in criminal justice programs often have a hard time finding courses or concentrations focused on cybercrime, whether they prioritize causality or prevention/intervention of cybercrimes (Nodeland, Belshaw, & Saber, 2019). Similarly, comprehensive introductory textbooks regarding cybercrime are very limited, with some exceptions (e.g., Holt, Bossler, & Seigfried-Spellar, 2015; Yar & Steinmetz, 2019); unlike the near-endless resources available for traditional criminological topics.

*Corresponding author
Jaeyong Choi, Ph.D., Department of Criminal Justice, West Chester University, Suite 518, 50 Sharpless St., West Chester, PA 19383, U.S.A.
Email: jchoi@wcupa.edu

Data show that the number of cybercrimes committed globally has continued to increase over the last several decades even though accessibility and quality of technology has improved and become more efficient. The harmful consequences of various cybercrimes on individuals, organizations, and society—most of whom are not equipped or even aware of their own vulnerability—have also been documented. Another challenge exists in how the patterns and methods of cybercrime change rapidly over time, making it harder to track, understand, and disseminate knowledge in order to reduce potential victimization. Ironically, this difficulty highlights the importance of investing and supporting future scholarship on cybercrime so that more criminologists are familiar with this cybercrime and willing to embark on the task of researching this area.

The recent creation of the Division of Cybercrime under the American Society of Criminology signals the recognition by criminologists of the importance and necessity of more organized and systematic efforts to understanding cybercrime. Additionally, these efforts lend to encouraging and supporting students to be more involved in this area. The committee members of the 2021 Whitehat Conference held these goals in mind when creating an opportunity for students to participate in the student paper competition. Students were given the opportunity to learn more about cybercrime while developing original research ideas under the tutelage of their respective advisors. Submitted works were awarded with recognition for the paper competition winners during the conference, reinforcing students' passion for this area of inquiry while recognizing and disseminating important findings. With this in mind, this special issue was compiled based on the three winning participant's papers.

Overview

Three articles appear in this issue and they direct our attention to key issues regarding cybercrime that have often been overlooked in the literature. The first article is by Hwang and Choi (2021) exploring the perceptions of cyberterrorism from the Democratic Peoples Republic of Korea through the lens of differential opportunity theory and the network theory of world politics. Based on interviews with several experts, their research highlights the point that North Korea is a very conducive environment for cyber terrorists to develop their skills and execute terrorist attacks online. They also offered several policy suggestions that could effectively deter North Korea's cyber-terror activities. Given that there has not been much research devoted to North Korean cyberterrorism—especially from a criminological perspective—this study is a great addition to the existing literature.

Next, Gero, Back, LaPrade, and Kim (2021) shed light on a very timely issue regarding the relationship between COVID-19 and cybercrime. Specifically, they examined the relationship between the number of malware infections, COVID-19 positive cases, closed non-essential businesses, and closed K-12 public schools in the United States, drawing on routine activities theory. The authors used various data sources to address this research question including the Kaspersky Cyberthreat Real-Time Map and the Centers for Disease Control and Prevention. Their results indicated that the increasing likelihood of malware infection victimization was positively associated with closed non-essential businesses and COVID-19 positive case numbers. The unprecedented pandemic posed a new threat to human society, but its impact on cybercrime is largely unknown and remains an important gap in research. Gero et al.'s study contributes to developing the knowledge base in this regard.

Finally, Yeonjae and Vieraitis (2021) tackled the fear of online victimization committed through social networking services (SNS) using the data from a sample of 1,000 individuals aged 14 to 59 living in South Korea. The results from their mediation analysis showed that more exposure to SNS increases online victimization, which leads to greater fear of victimization on SNS. Public sentiment is a critical topic because it is often a driver of key criminal justice policies. Their research helps to address this issue by identifying some factors related to the emotion of cybercrime.

Concluding Remarks

Not surprisingly, these studies are not without limitations but help illustrate potential directions for more robust research. We strongly believe that students' involvement and efforts to initiate and complete their research ideas for this paper competition make this special issue even more special. The desire and perseverance that these young researchers have shown during this student paper competition gives us hope for a brighter future for scholarship on cybercrime in the coming age. We hope that this special issue sparks further interest in cybercrime among students and prompts other organizations related to cybercrime to create more opportunities for students to engage in the research endeavor.

References

Gero, S. L., Back, S., LaPrade, J., & Kim, J. (2021). An empirical study on cybercrime and COVID-19. *International Journal of Cybersecurity Intelligence and Cybercrime*, *4*(2), 25-37.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. New York, NY: Routledge.

Hwang, J., & Choi, K.-S. (2021). North Korean cyber attacks and policy responses: An interdisciplinary the oretical framework. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 4-24.

Nodeland, B., Belshaw, S., & Saber, M. (2019). Teaching cybersecurity to criminal justice majors. *Journal of Criminal Justice Education, 30*(1), 71-90.

Park, Y., & Vieraitis, L. M. (2021). Level of engagement with social networking services and fear of on line victimization: The role of online victimization experiences. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 38-52.

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology, 14*(1), 81-105.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). Thousand Oaks, CA: Sage.