International Journal of Cybersecurity Intelligence & Cybercrime

Volume 2 | Issue 1 Article 1

2-2019

Awareness and Perception of Cybercrimes and Cybercriminals

awareness, perception, cybercrime, cybercriminal, cyber victimization, policy

Recommended Citation

Lee, Hannarae and Lim, Hyeyoung (2019) Awareness and Perception of Cybercrimes and Cybercriminals, International Journal of Cybersecurity Intelligence & Cybercrime: 2(1), 1-3. https://www.doi.org/10.52306/02010119UYIB64

Lee, H., & Lim H. (2019). *International Journal of Cybersecurity Intelligence and Cybercrime, 2* (1), 1-3.

Awareness and Perception of Cybercrimes and Cybercriminals

Hannarae Lee*, Marywood University, U.S.A

Hyeyoung Lim, University of Alabama at Birmingham, U.S.A

Key Words; awareness, perception, cybercrime, cybercriminal, cyber victimization, policy

Abstract:

Awareness is a starting point to recognize, understand, or know a situation or fact, and the perception makes a difference in how to deal with it. Although the term cybercrime may not be new to the most public and the police, not all of them are well aware of the nature and extent of cybercrimes, cybercriminals, and cyber-victims, which in turn affects their perceptions of matters. The four papers in this issue of the International Journal of Cybersecurity Intelligence and Cybercrime empirically examine these important topics and discuss policy implications.

There is no golden methodology in scientific research. Researchers either replicate or utilize different methodologies on similar topics and phenomena to examine whether they can reach similar findings of the previous literature. This process of triangulation is necessary to enhance the validity of the study in a given field. Studying cybercrime and cybersecurity is not easy to conduct due to data unavailability and hardship of data collection. Hence, we are happy to present the three empirical studies that not only enhanced the validity of the proposed topics but also add new insights in the field of cybercrime and cybersecurity, as well as a policy paper discussing cybercrime issues in Nigeria.

The majority of studies on people's cybercrime awareness and victimizations are based on self-report surveys and provide mixed-results. Since the use of self-report data is widespread across diverse fields of empirical research, the method has its own merit. At the same time, a self-report survey also carries several limitations, which include but are not limited to telescoping, deception, and social desirability biases. To overcome the limitations of the self-report survey and to triangulate the study, Roderic Broadhurst, Katie Skinner, Sifniotis Nicholas, Brayn Matamoros-Macias, and Yuguang Ipsen (2019, this issue) present one of the few quasi-experimental observational studies to examine the impact of people's awareness of cybercrime risks on their actions when handling phishing scams. It is unpractical to set up a physically controlled environment to perform an experiment on cybercrime, especially to trace the action of the victims in cyberspace. To overcome this huddle, Broadhurst et al. (2019) duplicated the login screens of a number of hosting web services to trace the record of

*Corresponding author

Hannarae Lee, Ph. D., Assistant Professor of Criminal Justice, Department of Social Sciences, Marywood University, USA. Email: hnrlee@marywood.edu

---

respondents' reactions of phishing scams. The findings indicate that people's awareness of phishing is not enough to deter or prevent a person from victimization. They found that relevant and salient content, which also instills the urgency of the phishing email, may influence cybercrime susceptibility. Their findings warrant the constant effort and specific rather than general prompts or warnings about cybercrime. For the record, we are not arguing that Broadhurst et al. (2019) study provided the best approach. Instead, this exploratory study opens the door for future studies to replicate and enhance the methods to examine people's actions in cyberspace.

Myriads of literature on police legitimacy support that procedural police legitimacy encourages compliance with the law and police (Tyler, 2004; Tyler & Fagan, 2008; Wolfe, Nix, Kaminski, & Rojek, 2015). While it is important to know how public perception shapes their willingness to cooperate with police (Lim, 2015, 2017), it is also imperative to know how police perceive their job, especially handling crimes that are relatively new compared to other common crimes such as cybercrime cases. From this standpoint, Thomas J. Holt, Jin R Lee, Roberta Liggett, Karen M. Holt, and Adam M. Bossler (2019, this issue) demonstrated how U.K. constables view the threat of bullying and harassment, and victims of these crimes based on the data collected from 34 local agencies across England and Wales. Holt et al. (2019) found that constables are less interested in these offenses and feel that specialized units should be responsible for handling such calls. The findings of this study warrant a need for resource development and training to improve the awareness of individual officers as well as the entire constabulary of England and Wales regarding how serious online harassment and bullying incidents are and how to handle those cases and the victims.

Other than the internet crime complaint data collected by the Internet Crime Complaint Center (IC3) under the Federal Bureau of Investigation (FBI), there is a paucity of reliable and valid nationwide data of cybercrimes that are collected, published, and archived for consecutive years in the United States. Such data deficiencies limit scholars and practitioners to study the characteristics of cybercrime and cyber offenders. Besides, due to the no restriction of time and place in the cyberspace, locating cyber offenders places an extra burden to investigators. By collecting the case examples from the Department of Justice press release between 2009 and 2017, however, Lora Hadzhidimova and Brain Payne (2019, this issue) built a dataset that includes various aspects of cybercriminal characteristics, especially international cyber offenders who were prosecuted in the U.S., even under the complicated jurisdictional issues. By analyzing the dataset, Hadzhidimova and Payne (2019) found support for the previous literature, as well as shed some new insights into the field. They also addressed the importance of similar data collection in other countries focusing on international cybercriminals to identify their collaboration with domestic criminals as well as for the comparative purpose.

The last paper by Kabiru Hamza Mohammed, Yusuf Danlami Mohammed, and Abiodun Abdullahi Solanke (2019, this issue) presents knowledge and a skill gap of law enforcement officers as well as the relevant actors in the judiciary system in Nigeria. In this policy paper, Mohammed et al. (2019) pointed that there has not been any empirical evidence that the Cybercrime Act 2015 prevents misuses of computer or electronic devices due to the lack of expertise in and support from both law enforcement and judicial system in Nigeria. In this paper, Mohammed et al. (2019) provide recommendations to bridge the gap that exists among legislators, investigations, and prosecutors in Nigeria including developing mechanisms against cybercrimes by increasing public and government awareness and establishing global cooperation to combat cybercrime.

Our discussion in this editorial page only begins to scratch the surface of the scholarship directed toward and public awareness on phishing scams and victimization, police perceptions on interpersonal cybercrime, and international cyber offender characteristics, as well as how governments and public

awareness matters to fight against cybercrimes and cybercriminals and how to protect the victims of cybercrimes. The articles included in this volume present an infinite possibility of studying different dimensions of cybercrime and cybersecurity. We always welcome and sincerely appreciate the scholars who concern and empirically examine these important topics and provide valuable insights in the field of cybercrime and cybersecurity.

References

Broadhurst, R., Skinner, K., Nicholas, S., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence and Cybercrime,* 2(1), xx-xx.

Hadzhidimova, L., & Payne, B. (2019). The profile of the international cyber offender in the U.S. *International Journal of Cybersecurity Intelligence and Cybercrime,* 2(1), xx-xx.

Holt, T. J., Lee, J. R., Liggett, R., Holt, K. M., & Bossler, A. M. (2019). Examining perceptions of online harassment among constables in England and Wales. *International Journal of Cybersecurity Intelligence and Cybercrime,* 2(1), xx-xx.

Lim, H. (2015). Social modeling effects on perception of the police: Focus on indirect police contact experience among college students. Policing: *An International Journal of Police Strategies & Management,* 38(4), 675 – 689.

Lim, H. (2017). Police bias, use of deadly force, public outcry: Vicious cycle? *Criminology & Public Policy,* 16(1), 305 – 308.

Mohammed, K. H., & Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and digital forensics: Bridging the gap in legislation, investigation, and prosecution of cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence and Cybercrime,* 2(1), xx-xx.

Tyler, T. R. (2004). Enhancing police legitimacy. *The Annals of the American Academy of Political and Social Science,* 593(1), 84-99.

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities? *Ohio State Journal of Criminal Law, 6,* 231-275.

Wolfe, S. E., Nix, J., Kaminski, R., & Rojek, J. (2016). Is the effect of procedural justice on police legitimacy invariant? Testing the generality of procedural justice and competing antecedents of legitimacy. *Journal of Quantitative Criminology,* 32(2), 253-282.