International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 1 Article 1

2-28-2020

Review of Fundamental to Know about the Future

fundamental elements, cybercrime, digital forensics, cybersecurity

Recommended Citation

Lee, H. (2020). Review of fundamental to know about the future. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 1-2. https://www.doi.org/10.52306/03010120TJKQ7353

Lee, H. (2020). *International Journal of Cybersecurity Intelligence and Cybercrime, 3* (1), 1-2.

Review of Fundamental to Know about the Future

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

Keywords; fundamental elements, cybercrime, digital forensics, cybersecurity

Abstract:

What we consider fundamental elements can be easily overlooked or perceived as facts without the process of empirical testing. Especially in the field of cybercrime and cybersecurity, there are more speculations regarding the prevalence and the scope of harm carried out by wrongdoers than empirically tested studies. To fill the void, three articles included in the current issue addresses empirical findings of fundamental concerns and knowledge in the field of cybercrime and cybersecurity.

Introduction

Critical thinking is the art of analyzing and evaluating thoughts and concepts to improve ideas. Without critical thinking, much of our reasoning can easily be biased, distorted, or partial. Through the process of raising vital questions and problems, gathering and assessing relevant information, we formulate clear and precise ideas. We, however, do not naturally recognize the limitations of our point of view. Thus, through the rigorous application of intellectual standards such as clarity, accuracy, precision, relevance, depth, breadth, logic, and fairness to the elements of reasoning (i.e., purposes, questions, assumptions, points of view, evidence, theories, inferences, and implications), we develop scientific study for given topic of our interest. This approach is typically easier said than done. Fortunately, however, three articles included in the current issue are well-formulated to address not only fundamental concerns and knowledge in the field of cybercrime and cybersecurity but also provide the empirical application on the given topic.

For example, the Darknet and Bitcoins have been hot button issues due to the notorious anecdotal stories surrounding those subjects. Most of the literature, however, is based on hearsays rather than empirical evidence. To accommodate our craving for scientific studies in these areas, Sinyong Choi, Kyung-Shick Choi, Yesim Sungu-Eryilmaz, and Hee-Kyung Park (2020, this issue) examine online gambling sites on both the Dark Web and Surface Web. All gambling sites selected for their study allow Bitcoin as their primary or secondary payments. By comparing the characteristics of online gambling sites among different browsers: the Dark Web and Surface Web, the authors identify distinct features and operational tactics. While applying the routine activity theory, the authors also validated the borderless nature of the Internet that attract gambling operators.

*Corresponding author

Hannarae Lee, Ph. D., Department of Social Sciences, Marywood Univesrity, 2300 Adams Ave., Scraonton PA 18509 USA
Email: hnrlee@marywood.edu

Even though the fundamentals of any given field are valued, sometimes they are easily overlooked. To address such an issue in digital forensics, Kumarshankar Raychaudhuri and M. George Christopher (2020, this issue) examined the importance of using a write-blocker in the file-system of a NTFS by testing changes in the file-system of a NTFS formatted USB storage device. While working in the digital forensic fields, officers can neglect to use a write-blocker either intentionally or unintentionally. By demonstrating changes made by improper treatment of data in the file-system of a NTFS, Raychaudhuri and Christopher (2020, this issue) presents clear evidence to alert wrongful practice in the area of digital investigation.

The last paper by Scott Debb, Daniel Schaffer, and Darlene Colson (2020, this issue) presents another empirical study that targets anecdotal stories regarding cybersecurity practices and concerns among different age groups. By addressing findings from the Online Security Behaviors and Beliefs Questionnaire (OSBBQ), the authors present different attitudes toward cybersecurity between Generation Y and Generation Z. The results regarding the knowledge and performance gap between two age groups offer a potential roadmap for policy implications and future security features of technological developments.

The discussion on this editorial page only begins to scratch the surface of the scholarship provided in the current issue. Three articles included in this issue present the importance of critical thinking process to develop a study to test various hearsays in the field of cybercrime and cybersecurity while reiterating the infinite possibility of studying different dimensions of cybercrime and cybersecurity. I hope you will enjoy this issue of IJCIC and find it thought-provoking. We always welcome and sincerely appreciate the scholars who are concerned with and empirically examine these crucial topics and provide valuable insights in the field of cybercrime and cybersecurity.

References

Choi, S., Choi, K. Sungu-Eryilmaz, Y., & Park H. (2020). Illegal gambling and its operation via the Darknet and Bitcoin: An application of routine activity theory. *International Journal of Cybersecurity Intelligence and Cybercrime, 3*(1), 3-23.

Debb, S., Schaffer, D., & Colson, D. (2020). A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults.*International Journal of Cybersecurity Intelligence and Cybercrime, 3*(1), 42-55.

Raychaudhuri, K., & Christopher, M. G. (2020). An empirical study to determine the role of file-system in modification of hash value. *International Journal of Cybersecurity Intelligence and Cybercrime, 3*(1), 24-41.