Understanding and Moving Forward Research on Online Crime: Introduction to Cybercrime Minitrack

J. Tuomas Harviainen
Tampere University
tuomas.harviainen@tuni.fi

Piotr Siuda
Kazimierz Wielki University
piotr@ukw.edu.pl

Juho Hamari
Tampere University
juho.hamari@tuni.fi

Robert W. Gehl
York University
rwg@yorku.ca

Abstract

Research on cybercrime is on the rise in many areas of internet studies, often with a strong emphasis on interdisciplinarity. Hence, for HICSS-56 research is not confined to a single area, and the minitrack includes multiple disciplines and different methodologies. In response to the call for papers, seven manuscripts from a wide variety of disciplines were submitted which were then subjected to peer and editorial review. Three submissions were accepted for presentation and publication. Here, preliminary issues and accepted articles are being discussed.

Keywords: cybercrime, darkweb, disnormative behavior, interdisciplinary, multidisciplinary

1. Introduction

Advances in digital technologies create various opportunities for crime (Holt et al., 2017). Criminals–usually with high technical skills–can commit cybertrespass (e.g., unauthorized system access, see MacLeod, 2021), cyberdeception and cybertheft (e.g., online fraud, identity theft, see van de Weijer et al., 2019), obscenity (e.g., child sexual exploitation materials, see Henry et al., 2018), cyberviolence (e.g., cyberstalking, cyberbullying, see Costello et al., 2022) or even cyberterrorism (e.g., different intrusions, building extremist networks, see Lee et al., 2021).

At the same time, cybercrime is difficult to define and should be rather understood as a broad term that ranges 1) computer-assisted crimes, in which digital technologies play an auxiliary role, e.g. one uses a device to send harassing messages, and 2) computer-focused crimes that would not exist without the technologies discussed (Bossler & Berenblum, 2019).

Cybercrime could also be understood in a more general, 'cultural' sense: as any online behavior that differs from the normative behavior of a significant number of people in society, or behavior evaluated negatively by the society as a whole (Haasio, 2019). Here one could focus on different social structures and highlight contextual differences, including the role of textualities, language and culture (Haasio et al., 2020).

Moreover, it is very difficult to estimate the amount of cybercrime occurring worldwide, mainly due to the lack of unambiguous legal definitions and official and reliable statistics (Holt et al., 2017). However, it can be suspected that cybercrime rates are increasing year by year; hence the research has grown exponentially over the last few decades. Our cybercrime minitrack is part of this growth with all submitted and accepted manuscripts tackling various faces of cybercrime.

2. Cybercrime Minitrack

This minitrack aims to give insights and develop a theoretical and practical understanding of issues related to cybercrime without excluding any methodological approaches. When introducing the call for papers we welcomed conceptual, theoretical, empirical and methodological papers that would enrich understandings of illegal online practices. Topics of interest included, but were not limited to: trading in illicit goods and services online; the use of dark web as a marketplace or information sharing environment; ransomware; phishing and scamming; cryptomarkets and cryptocurrencies; information manipulation for commercial gain; violence, deception, risk, security, and privacy; regional differences in cybercrime; and investigative techniques and methods for cybercrimes.

URI: https://hdl.handle.net/10125/103073
978-0-9981331-6-4

Submissions explored both theoretical perspectives and distinct theories, whether traditional criminological theories, or novel ideas that help us understand various aspects of online crime. We also welcomed inquiries into methods and data and empirical research on issues related to cybercrime.

3. Review of Accepted Research

For HICSS-56, three manuscripts were accepted for presentation and publication. The first paper (Giddens, Petter, Bichler, Rivas, Fullilove, Cerny), *Navigating an Interdisciplinary Approach to Cybercrime Research*, tackles human trafficking online and presents a project conducted by the authors. However, the paper's focus is broader than just trafficking; it also discusses how to study cybercrimes in an interdisciplinary manner and how to develop efficient interventions. Thus, the paper is a valuable contribution showing what is needed to understand the complexity, occurrence, and impact of online crime on victims and society.

The second paper (Liu, Frank, Warkentin), *Drugs for Sale! An Analysis and Estimation of Drug Products on the Cryptomarket Ecosystem*, examines product information from eight large dark web markets which are being analyzed during one-year time period. Apart from analyzing the drugs being available, research identifies factors that encourage or discourage vendors from shipping globally. This leads the authors to the conclusion that in the future cryptomarkets will be even more important and popular.

Finally, the third paper (Fitzgerald, Mason, Mulhair, Glisson), *Exploiting a Contact Tracing App to Attack Neighboring Devices*, presents a case of Louisiana Department of Health's COVID Defense contact tracing application, which helped people avoid infection during the COVID-19 lockdowns. The presented research highlights a symptom sharing feature of this app as a potential attack vector. The paper explores effectiveness of various kinds of attack (through email, WiFi direct, and nearby share) thus provides initial assessment of safety of similar solutions.

4. Conclusion

Research on the internet has focused mostly on legal ('ordinary', 'everyday') practices. Recent years have nevertheless seen a significant increase in cybercrime. Rarely a day goes by without online crime being reported in the media. Examples include online trading in narcotics and other illicit goods and services, the hijacking of individual accounts and organizational systems, extortion, exit scams, fake investments in cryptocurrencies and even blatant information manipulation for financial gain.

Research on cybercrime should therefore be the main information source for policymakers, the public, and security professionals on how to decrease various forms of online crime. With the field of cybercrime research growing, this could very well be the case, and the presented HICSS-56 minitrack could be another step in making a larger impact.

5. Funding

This research is supported by the Polish National Science Center (Narodowe Centrum Nauki) grant 2021/43/B/HS6/00710.

6. References

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495–499. https://doi.org/10.1080/0735648X.2019.1692426

Costello, M., Reichelmann, A. V., & Hawdon, J. (2022). Utilizing criminological theories to predict involvement in cyberviolence among the iGeneration. *Sociological Spectrum*, *0*(0), 1–18. https://doi.org/10.1080/02732173.2022.2105767

Haasio, A. (2019). What is Disnormative Information? *Information and Communication Sciences Research*, *23*(1), 9–16.

Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark Web marketplace. *Information Processing & Management*, *57*(2), 102080. https://doi.org/10.1016/j.ipm.2019.102080

Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, *19*(6), 565–581. https://doi.org/10.1080/15614263.2018.1507892

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction* (2nd edition). Routledge.

Lee, C. S., Choi, K.-S., Shandler, R., & Kayser, C. (2021). Mapping Global Cyberterror Networks. *Journal of Contemporary Criminal Justice*, *37*(3), 333–355. https://doi.org/10.1177/10439862211001606

MacLeod, A. J. (2021). Cyber Trespass and Property Concepts. *IP Theory*, *10*, 1.

van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610