

9-30-2016


Special Issue on Cyberharassment Investigation: Advances and Trends

Joanne Bryce
University of Central Lancashire, UK

Virginia N. L. Franqueira
University of Derby, UK

Andrew Marrington
Zayed University, UAE

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Bryce, Joanne; Franqueira, Virginia N. L.; and Marrington, Andrew (2016) "Special Issue on Cyberharassment Investigation: Advances and Trends," *Journal of Digital Forensics, Security and Law*. Vol. 11 : No. 3 , Article 4.

DOI: <https://doi.org/10.15394/jdfsl.2016.1416>

Available at: <https://commons.erau.edu/jdfsl/vol11/iss3/4>

This Editorial is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



FROM THE SPECIAL ISSUE EDITORS

SPECIAL ISSUE ON CYBERHARASSMENT INVESTIGATION: ADVANCES AND TRENDS

Empirical and anecdotal evidence indicates that cyberharassment is more prevalent as the use of social media becomes increasingly widespread, making geography and physical proximity irrelevant. Cyberharassment can take different forms (e.g., cyberbullying, cyberstalking, cybertrolling), and be motivated by the objectives of inflicting distress, exercising control, impersonation, and defamation. Little is currently known about the *modus operandi* of offenders and their psychological characteristics. Investigation of these behaviours is particularly challenging because it involves digital evidence distributed across the devices of both alleged offenders and victims, as well as online service providers, sometimes over an extended period of time. This special issue aims to improve understanding of cyberharassment from a multidisciplinary perspective in order to further develop theoretical knowledge and investigative practice.

The article “Differentiating Cyberbullies and Internet Trolls by Personality Characteristics and Self-Esteem”, by Zezulka and Seigfried-Spellar, examines the differences and similarities of two types of cyberharassment (cyberbullying and cybertrolling). Their research identified differential patterns of personality traits between individuals who engaged in the two examined behaviours. This indicates the importance of further research identifying individuals at risk for engaging in electronic harassment, and the need to develop appropriate interventions which address underlying psychosocial problems.

The second paper, “The Impact of Low Self-control on Online Harassment: Interaction with Opportunity” by Baek et al., also addresses cyberharassment from a psychological perspective. It found that low self-control, opportunity, and gender have a significant influence on online harassment. The authors argue that identifying the characteristics of offenders can assist investigators to more effectively triage targets and enable more efficient use of associated resources, particularly when combined with computationally enabled forensic tools.

Automation is the focus of the third paper, “Toward Online Linguistic Surveillance of Threatening Messages” by Spitzberg and Gawron. This paper provides an examination of text analysis approaches useful to automate threat identification, assessment and possible interventions based on written communication. Such developments are beneficial for detection, prevention and investigation of cyberharassment and the associated risk of violent and criminal actions. It highlights the importance of automation in assisting law enforcement and intelligence agencies to cope with the increasingly overwhelming volume of written communication posted online.

The final article, “A Legal Examination of Revenge Pornography and Cyber-harassment” by Lonardo et al., explores legal and evidential perspectives on revenge pornography, a popular instrument of cyberharassment usually adopted by formerly intimate ex-partners. Using a case study, the authors discuss the identification, collection and preservation of digital evidence which

is typically relevant to building a legal case to prosecute offenders or defend victims of online revenge pornography.

These papers indicate the different areas of empirical and theoretical research currently being undertaken in the area of cyberharassment. They demonstrate the utility of combining research methods and disciplinary perspectives in order to further develop understanding of offending and victimisation, as well as the associated challenges in obtaining and interpreting associated digital evidence. Although a relatively under-developed research area, the papers included in this special edition highlight the importance of evidence-based approaches to preventing and responding to this category of cybercrime.

Sincerely,

Joanne Bryce
School of Psychology
University of Central Lancashire, UK

Virginia N. L. Franqueira
College of Engineering and Technology
University of Derby, UK

Andrew Marrington
College of Technological Innovation
Zayed University, UAE