CYBERSEXUAL HARASSMENT AS ICTS DEVELOPMENT CONSEQUENCES: A REVIEW

Jūratė Kuklytė[1]

[1] *Vytautas Magnus University, Kaunas, Lithuania*

EUROPEAN JOURNAL OF BUSINESS SCIENCE AND TECHNOLOGY

Volume 4 Issue 2
ISSN 2336-6494
www.ejobsat.com

ABSTRACT

Rapid progress of information and communication technologies (ICTs) affected the evolution of sexual harassment. Cybersexual harassment can be exposed via social media but as well might be a tool for harassers to attack or stalk individuals after anonysmously. This evolution of phenomenon enter to virtual reality require changes in differenr levels: individual, enterprise and state to counter the hybrid threats. The proposed conceptual framework reflects the main vulnerable groups, consequences. These main aspects trigger for the development of ICTs in order to change organizational policies, political and security regulations.

KEY WORDS

cybersexual harassment, cyberbullying, cybercrime, hybrid threats

JEL CODES

M1, D8, D74

1 INTRODUCTION

A rise of social media and networking has made faster access to information and engage to communicate through tweet, post, Instagram, sharing various content on Facebook, making Tumblr blogs or Youtube videos. Individuals have the voice to tell their story in a massive scale via different mobile applications by making digital messages more personal and intimate. Also and broadcast specific moments live.

However, the viral spread of information leads to power imbalance of specific individuals who are targeted against social norms and express revolutionary ideas, attitudes and insights. The scholars highlighted that there is a need of cybersexual harassment prevention among adolescence (Pereira et al., 2016) and university students (Moafa et al., 2018). Mainiero and Jones (2013) develop new communication ethics in order to prevent work-

KUKLYTĖ, Jūratė. 2018. Cybersexual Harassment as ICTs Development Consequences: A Review. *European Journal of Business Science and Technology,* 4 (2): 187–195. ISSN 2336-6494, DOI http://dx.doi.org/10.11118/ejobsat.v4i2.137.

place romances that may subsequently turn into workplace sexual harassment through the use of social networks and other forms of digital communication between employees. The interest among academicians is growing. Kuem et al. (2017) tested what different aspects which may have significant effect and may lead to prosocial behaviour in social networking services. Misbehaviour in social networks has gained public attention and encourage to report of cybersexual harassment to legal instutitions.

Furthermore, cybersexual harassment, including cyber-porn, obscenity, sharing sexually expressive illegal content or activities, are identified as a cybercrime (Holt, 2018). These actions play a key role to digital diplomacy. According to Surma (2016) international conflicts may be started by using "Factories of Trolls" in order to use provocation strategy to manipulate public opinion of specific country. Hybrid threats are complex like cyberattacks, alienation, extortion of confidential information, cyberbullying, cybersexual harassment and others.

This research aims to broaden the understanding what are the major threats and consequences of cyber sexual harassment in different levels. Following the aim of this research the main attention was gained, how cybersexual harassment perception evolved and changed in different level. By intending to investigate a research gap, following questions were formulated:

RQ_1: How cybersexual sexual harassment evolve?

RQ_2: What are the main vulnerable groups and consequences in different levels?

2 BACKGROUND OF CYBERSEXUAL HARASSMENT

Sexual harassment became an important issue and throroughly analysed as face-to-face actions. Interpretive way reveal multiple realities, which are socially constructed by different workplace environments – academia (Carstensen, 2004), military (Matheson and Lyle, 2017), private sector organizations (Sarpotdar, 2013).

Moreover, hermenautical delectical analysis could be employed based by the concept of Gramsci hegemony that social practice construct the actions and desires excluding personal interests and values by analyzing the nature of sexual harassment and cybersexual harassment (see e.g. Hatch and Cunliffe, 2006). Dialectical perspective reveal that deviant behaviors can be seen as mimicry. According to Bhabha (1997), "mimicry emerges as the representation of a difference that itself a process of disavowal." Also mimicry is defined as "the sign of a double articulation, a complex strategy of reform, regulation and discipline, which "appropriates" the Other as it visualizes power". Such complex nature is shown in some researches. Lindberg et al. (2012) revealed that the Finnish adolescents who "expressed their massacre threats online as cybersexual harassment could be considered a riskier group than the group who expressed the threats offline".

Cybersexual harassment involves destructive electronic means mediated communication such as e-mail spoofing, stalking, cyber sexual defamation, cyber flirting, hacking, cyber pornography, and cyberbullying. Moreover, similarities, differences and interrelationship of cyberbullyinh and cyber sexual harassment were exposed. Akbulut and Eristi (2011) highlight that cyberbullying can be expressed through flaming, sexual harassment and stalking. Also it includes verbal and visual social and relational aggression like harassment, denigration, sexting, posting embarrassing photos or memes (Ballard and Welch, 2015). Vveinhardt and Kuklytė (2017) online misbehaviors in three types: violent and pornographic content, threats and vulgar language, and grooming. Thus, both phenomena are tend to refer as cybercrime by having tripple nature – could be expressed in a direct, indirect and mixed ways. Thus, extensive literature review and synthesis required in order to identify the targeted groups, possible threats, and consequences in different levels.

3 CONCEPTUAL FRAMEWORK

The use of various social networks and online technology is increase and transform the phenomena of sexual harassment in various perspectives. The provided model of cybersexual harassment aims to contribute conceptual understanding what are vulnerable groups, what could be consequences in different level (Fig. 1).

State level showed the incidents of cybersexual harassment operating at digital diplomacy level as a hybrid conflict – massive cyber attacks against minorities (children, adolescents, women) to cause socio-demographic problems and influence political issues without use of army force (Maurer and Janz, 2014).

Interpersonal level defines cyber sexual abuse among non-related individuals. Innapropriate dissemination and gender discrimination may appear among children, adolescents, students and virtual agents in different electronic environment – social networks and video games. The main intention is to initiate and engage a video connection or face-to-face meeting with the victim. Furthermore, the high level anonymity and power imbalance enable long lasting destructive communication which may cause psychological damage.

Enterprise level represents analysis of employees' misbehaviour in social networks. These offensive actions targeted against gender issues are analysed as deviant behaviors in computer-mediated communication (Ritter, 2014). Cyber incivility and online sexual harassment among employees has been analysed by Giumetti et al. (2016), Park et al. (2018) and others. Such an extent of spread of cybersexual harassment may cause financial and non-financial damage, also harm the well-being of employees.

According to Lewis et al. (2017), cybersexual harassment is an extention of offline sexual violence against women. Cyber-aggression among adolescents tend to have a sexual nature regarding the gender such as getting an unwanted sexual message from somebody or receiving sexual request by an adult may cause social-emotional consequences (Shapka and Maghsoudi, 2017). Several researchers argued that cybersexual harassment can adversely affect the organization (Ritter, 2008) and has a negative professional and economic outcomes for victims. Gamergate's misogynist scandal have revealed that social networking may play a key role of online abuse in conflicts that enable to gain a public and technological power (Salter, 2018). Moreover, massive attacks of cybersexual harassment messages targeted against minorities can be used as political tool to start hybrid or information warfare. Thus, cybersexual harassment is analysed in different contexts by using various keywords.

The scientific literature review enable to divide victims: women, adolescents, students, virtual agents, employees.

Tab. 1 represents cybersexual harassment among individuals who are not subordinated by specific job agreements. On the other hand, one group of victims – university students – has an intimate relationships with a perpetrator. These online actions affect interpersonal level.

Cybersexual harassment activities conducted in social networks during leisure time or on a daily basis may evolve to on-duty activities in different organizations (Maneiro and Jones, 2013). Although, outcomes of individual online misbehaviour may have negative impact on socio-demographic factors.

The most vulnerable victims group is adolescents (Tab. 1). Malicious online activities may defined as "online sexual solicitation", "Internet-initiated offense", and "online sexual grooming". Sklenarova et al. (2018) analysed 2238 adolescents (14–17 years) in Germany and found that some participants (24.7%) reported about online sexual experiences with peers and/or adults, 43.3% reported of exchanging pictures and 6.2% had engaged in cybersex.

Another group of victims are women. A considerable evidence shown that women experience cybersexual harassment and interpersonal misbehaviour is more often observed in individual level (Vitis and Gilmour, 2017; Ritter, 2014; Ritter, 2008). Women tend to experience online misbehaviour in various environment like blogs (Eckert, 2018), video games (Ballard and Welch, 2017) and other.

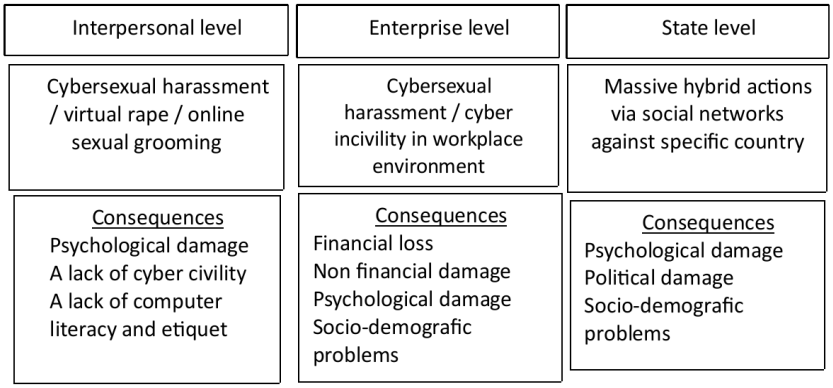

Fig. 1: The model of cybersexual harassment in different level

Less common online misbehaviour is virtual rape in a two or three dimentional environment. The first virtual rape case LambdaMOO was discussed in 1992. Spence (2012, p. 125) argued that "an avatar as virtual representation of an individual in reality can and must be perceived as a virtual purposive agent that have moral rights and obligations similar to those of their real counterparts. With regard to agency those rights are merely prima facie but with regard to personhood framed around the notion of self-respect those rights are absolute." According to Wolfendale (2007) virtual world is based to performative utterances and have illocutionary force (intentional virtual agents actions) and perlocutionary force (virtual agents have significant social effect). Warren and Palmer (2010) mentioned in Australian Institute of Criminology report that a female user of "Second Life" (3D game) informed Belgian police that her avatar had been raped in May, 2007. It is affirmed that "the rape of an avatar may produce some real-world physical discomfort or shock among unsuspecting or novice users" (Boellstorff, 2008). On the contrary, Fox et al. (2015) assert that virtual rape is understudied phenomena and claim that women's self-objectification lead to increases of rape myth acceptance.

Enterprise level represents organizational context. Online communication such as cyberbullying among adults (Lowry et al., 2016), cyber sexual harassment (Choi and Lee, 2017) among employees during working hours can be identified as on-duty deviance and off-duty deviance (Lyons et al., 2016). Moreover, cyber incivility through e-mail messages tend to have a double-edge sword effect (Lim and Teo, 2009). It can be illustrated by the case of women bloggers when they response with a humour creating memes and posts after online abuse (Eckert, 2018). This coping strategy is giving the same online abuse response to the perpetrator. Thus, a victim switches the roles and becomes a harasser.

Also online sexual aggression as an expression of misogynistic culture after GamerGate hate speech campaigns when female game developer Zoe Quinn was receiving death threats, threats of rape, and many harassing comments after an accusation of her ex-boyfriend that she had been given sexual favors for positive game reviews (Kaplan, 2014). Misogyny and homophobia may have impact on online aggression among massively multiplayer online game players (Ballard and Welch, 2017).

Cyber incivility and job subordination expressed in "not safe for work" (NSFW) blogs like tumblr.com may jeopardise the status of employees. Tiidenberg (2014) presented a case study of male sexual dominance by using the image of suit – tie combination and focusing on crotch area adding a caption: *"I think it's time you took some dictation. Clearly, I need a secretary to assist me."*

Louderback and Antonaccio (2017) extended typology of online misbehaviour by adding human and computer interaction issue –

Tab. 1: Conceptual analysis of cybersexual harassment in interpersonal level

Keywords	Definition	Victims	Source
Online obsessive relational intrusion	"The use of social networking sites, blogs, and other technologies to gain greater information, awareness, and knowledge of their partner's online and offline activities."	University students	Marganski and Melander, 2018
Online sexual aggression	An online actions when males use various coercive strategies to engage the women in consensual sexual activities.	Women	Strikwerda, 2015
Online sexual harassment	"Number of manifestation like revenge pornography, non-consensual sexting, cyberstalking, sending unsolicited nude images and sexually violent threats and harassment over online platforms such as gender-based hate speech."	Women	Vitis and Gilmour, 2017
Online aggression	A systematic abuse of power using electronic technology. It includes verbal and visual social and relational aggression like name-calling, sexting, posting embarrassing photos or memes, stalking and impersonation.	Gamers	Ballard and Welch, 2017
Online sexual solicitation	"Online risk behaviors like sexting, relating to strangers through the Internet, time using internet, using chat rooms, and adding strangers to social network friend lists."	Adolescents	Gámez-Guadix et al., 2018
Internet-initiated offense	Offensive actions that consist of enticing child into a sexual relationship or sexual gratification by using Internet communication platforms and fantasy-enhancing items like web camera and others.	Adolescents	Kloess et al., 2017
Cyber-interpersonal violance	Online harassment that consists of spreading of rumors, unwanted sexual photos without consent, and/or threatening individuals, and cyber impersonation.	College students	Choi and Lee, 2017
Technology-facilitated abuse (cyber violence)	Online actions enable abusers to overcome geographic and spatial boundaries that would have otherwise prevented them from contacting victims. Forms of domestic violence in electronic environment like cyber-stalking, non-consensual sexting and cyberbullying.	Adults	Al-Alosi, 2017
Virtual rape	"Virtual act of forcing sex upon an unwilling person in virtual environment."	Virtual agent	Strikwerda, 2015
Virtual rape	An unwanted sexual intercourse in order to harm the avatar in virtual environment.	Virtual agent	Young and Whitty, 2010
Online sexual grooming	An online manipulation process when offender creates circumstances to sexually abuse or exploit a child by earning the trust and initiating intimate physical contact with the victim.	Adolescents	Shannon, 2008

computer-focused digital deviance that is a consequence of a lack of technological mindfulness (Maier et al., 2017).

Another important aspect is that initiated massive cybersexual harassment attacks through social networks may work as a tool of digital diplomacy to seek control and power in state level. According to the European Parliamentary Research Service Blog, hybrid threat can be defined as "a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat". It is very complex in terms of nature of challenges, multiplicity of actors involved and diversity of (un)conventional means used (i.e. military, diplomatic, technological). Thus, hybrid threats involve the cyber incidents and actions. The European Centre of Excellence for Countering Hybrid Threats categorize hybrid threats based by three aspects. Firstly, hybrid threats are "coordinated and synchronised action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a

Tab. 2: Conceptual analysis of cybersexual harassment in enterprise level

Keywords	Definition	Victims	Source
Online abuse	"A crime that include intertwined online-offline communication and gendered, raced constructions of who is privileged to speak publicly in which way."	Women bloggers	Eckert, 2018
Cyber incivility	Widespread and discourteous treatment among employees that occurs via information and communication technologies. E-mail and text messages refer as uncivil behaviors.	Employess	Giumetti et al., 2016
Cyber incivility	"A day-level incivility via work e-mail."	Employess	Park et al., 2018
Cyber incivility	"A communicative behaviour exhibited in computer mediated interactions that violate workplace norms of mutual respect."	Employess	Lim and Teo, 2009
Cyber sexism	A phenomenon when women are putting off careers.	Women	Foster, 2015
Computer-focused digital deviance	It includes cybercrimes such as cyber offending, damaging sensitive data and online malware.	Employees	Louderback and Antonaccio, 2017

wide range of means". Secondly, it is related to the activities that exploit the thresholds of detection and attribution. Thirdly, different forms that may effect decision making at the state, or institutional level to realize the agent's strategic goals in order to undermine the target.

The increasing interests of hybrid conflict when interested parties may use technological means to exploit social, economic or political vulnerabilities leads to the main question how to counter the hybrid threat (Maurer and Janz, 2014). What if cybersexual harassment could be seen as a social vulnerability. The cyber perpetrators may use bots, specific algorithms or "factory of trolls" to spread massive panic and increase level of suicide in specific country.

In addition, cybersexual harassment is interpretated differently in various levels and may have different antecedents, outcomes to pursue specific objectives of perpetrator.

4 DISCUSSION AND CONCLUSIONS

The analysis and synthesis of scientific literature review provides a specific discource of cybersexual harassment in different levels by specifying victims and targeted groups. This paper contributes to the conceptual development of cybersexual harassment and expresses a deeper research interest, motivation and practical implications in public and private sectors.

The developed model broaden the conceptual understanding if we defining it to the multilevel framework of interpersonal mistreatment (Cunningham et al., 2007). This methodological approach is extended in different contexts – daily cyber aggression among non-related individuals, job relationship subordinated individuals and specific country level in terms of hybrid threat to harm the marginalized or the weakest group of individuals. According to Arcos (2018), target audience segmentation and preliminary research and analysis play a key role in order to identify targeted publics, that is important to overt and covert disinformation and propaganda campaigns. The constructed model showed three unique perspectives of cybersexual harassment: interpersonal level, enterprise level and state level. The presented conceptual framework is important for further investigations in order to prevent negative outcomes in terms of countering the hybrid threats (Bachmann, 2011).

ICTs, Internet of Things, Big Data and cyber-physical systems are influenced major changes in the context of Industry 4.0 by considering technical aspects, human interactions and development of new business models (Navickas et

al., 2017). Cyber-physical systems are used by hackers in order to reach sensitive data or raw information of individuals or fully automatated enterprises. Moreover, it could be used as a tool to start a hybrid warfare. The provided conceptual framework of cybersexual harassment could be useful to maintain organizational policies, security strategies, technological solutions for development of counter-measures and building resistance.

5 REFERENCES

Akbulut, Y. and Eristi, B. 2011. Cyberbullying and Victimisation among Turkish University Students. *Australasian Journal of Educational Technology*, 27 (7), 1155–1170.

Al-Alosi, H. 2017. Technology-Facilitated Abuse: The New Breed of Domestic Violence. *The Conversation* [online]. Available at: `https://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683`.

Arcos, R. 2018. Post-Event Analysis of the Hybrid Threat Security Environment: Assessment of Influence Communication Operations. *Strategic Analysis* [online]. Available at: `https://www.hybridcoe.fi/wp-content/uploads/2018/11/Strategic-Analysis-2018-10-Arcos.pdf`. [Accessed 2018, November 25].

Bachmann, S.-D. 2011. Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats – Mapping the New Frontier of Global Risk and Security Management. *Amicus Curiae*, 88, 14–17.

Ballard, M. E. and Welch, K. M. 2017. Virtual Warfare: Cyberbullying and Cyber-Victimization in MMOG Play. *Games and Culture*, 12 (5), 466–491.

Boellstorff, T. 2011. Placing the Virtual Body: Avatar, Chora, Cypherg. In Mascia-Lees, F. E. (ed.). *A Companion to the Anthropology of the Body and Embodiment*, pp. 504–520.

Bhabha, H. 1997. Of Mimicry and Man: The Ambivalence of Colonial Discourse. In Cooper, F. and Stoler, A. L. (eds.). *Tensions of Empire: Colonial Cultures in a Bourgeois World*, Part I (Framings), Chapter 3, pp. 152–160.

Carstensen, G. 2004. *Sexuella trakasserier finns nog i en annan värld: Konstruktioner av ett (o)giltigt problem*. PhD Thesis. Förlags AB Gondolin.

Choi, K.-S. and Lee, J. R. 2017. Theoretical Analysis of Cyber-interpersonal Violence Victimization and Offending using Cyber-routine Activities Theory. *Computers in Human Behavior*, 73, 394–402.

Cunningham, W. A., Zelazo, P. D., Packer, D. J. and Van Bavel, J. J. 2007. The Iterative Reprocessing Model: A Multilevel Framework for Attitudes and Evaluation. *Social Cognition*, 25 (5), 736–760.

Eckert, S. 2018. Fighting for Recognition: Online Abuse of Women Bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New Media & Society*, 20 (4), 1282–1302.

Foster, D. 2015. Five Proposals on Homophobia. In *Expanding the Circle: Creating an Inclusive Environment in Higher Education for LGBTQ Students and Studies*, pp. 225–235.

Fox, J., Ralston, R. A., Cooper, C. K. and Jones, K. A. 2015. Sexualized Avatars Lead to Women's Self-Objectification and Acceptance of Rape Myths. *Psychology of Women Quarterly*, 39 (3), 349–362.

Gámez-Guadix, M. De Santisteban, P. and Alcazar, M. Á. 2018. The Construction and Psychometric Properties of the Questionnaire for Online Sexual Solicitation and Interaction of Minors with Adults. *Sexual Abuse*, 30 (8), 975–991.

Giumetti, G. W., Saunders, L. A., Brunette, J. P., DiFrancesco, F. M. and Graham, P. G. 2016. Linking Cyber Incivility With Job Performance Through Job Satisfaction: The Buffering Role of Positive Affect. *Psi Chi Journal of Psychological Research*, 21 (4), 230–240.

Hatch, M. J. and Cunliffe, A. L. 2006. *Organization Theory: Modern, Symbolic, and Postmodern Perspectives*. 2nd ed. New York: Oxford University Press.

Holt, T. J. 2018. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *The ANNALS of the American Academy of Political and Social Science*, 679 (1), 140–157.

Kaplan, S. 2014. With #GamerGate, the Videogame Industry's Growing Pains go Viral. *The Washington Post* [online]. Available at: `https://www.washingtonpost.com/news/morning-mix/wp/2014/09/12/with-gamergate-the-video-game-industrys-growing-pains-go-viral/?noredirect=on&utm_term=.957ef0c3defd`. [Accessed 2018, September 29].

Kloess, J. A., Seymour-Smith, S., Hamilton-Giachritsis, C. E., Long, M. L., Shipley, D. and Beech, A. R. 2017. A Qualitative Analysis of Offenders' Modus Operandi in Sexually Exploitative Interactions with Children Online. *Sexual Abuse*, 29 (6), 563–591.

Kuem, J., Ray, S., Siponen M. and Kim, S. S. 2017. What Leads to Prosocial Behaviors on Social Networking Services: A Tripartite Model. *Journal of Management Information Systems*, 34 (1), 40–70.

Lewis, R., Rowe, M. and Wiper, C. 2017. Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls. *The British Journal of Criminology*, 57 (6), 1462–1481.

Lim, V. K. G. and Teo, T. S. H. 2009. Mind Your E-manners: Impact of Cyber Incivility on Employees' Work Attitude and Behavior. *Information & Management*, 46 (8), 419–425.

Lindberg, N., Sailas, E. and Kaltiala-Heino, R. 2012. The Copycat Phenomenon after Two Finnish School Shootings: An Adolescent Psychiatric Perspective. *BMC Psychiatry*, 12, 91–106.

Louderback, E. R. and Antonaccio, O. P. 2017. Exploring Cognitive Decision-Making Processes, Computer-focused Cyber Deviance Involvement and Victimization: The Role of Thoughtfully Reflective Decision-Making. *Journal of Research in Crime and Delinquency*, 54 (5), 639–679.

Lowry, P. B., Zhang, J., Wang, C. and Siponen, M. 2016. Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. *Information Systems Research*, 27 (4), 962–986.

Lyons, B. D., Hoffman, B. J., Bommer, W. H., Kennedy, C. L. and Hetrick, A. L. 2016. Off-duty Deviance: Organizational Policies and Evidence for Two Prevention Strategies. *Journal of Applied Psychology*, 101 (4), 463–483.

Maier, C., Wirth, J., Laumer, S. and Weitzel, T. 2017. Personality and Technostress: Theorizing the Influence of IT Mindfulness. In *ICIS 2017 Proceedings* [online]. Available at: `https://aisel.aisnet.org/icis2017/Security/Presentations/10/`. [Accessed 2018, September 15].

Mainiero, L. A. and Jones, K. J. 2013. Workplace Romance 2.0: Developing a Communication Ethics Model to Address Potential Sexual Harassment from Inappropriate Social Media Contacts Between Coworkers. *Journal of Business Ethics*, 114 (2), 367–379.

Marganski, A. and Melander, L. 2018. Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association with In-person Dating Violence. *Journal of Interpersonal Violence*, 33 (7), 1071–1095.

Matheson, L. C. I. and Lyle, E. 2017. Gender Bias in Canadian Military Leadership Training. *Journal of Ethnographic & Qualitative Research*, 12 (1), 18–28.

Maurer, T. and Janz, S. 2014. The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context. *The International Relations and Security Network*, 17, 277–293.

Moafa, F. A., Ahmad, K., Al-Rahmi, W. M., Yahaya, N., Kamin, Y. B. and Alamri, M. M. 2018. Cyber Harassment Prevention Through User Behavior Analysis Online in Kingdom of Saudi Arabia (KSA). *Journal of Theoretical and Applied Information Technology*, 96 (6), 1732–1746.

Navickas, V., Kuznetsova, S. A. and Gruzauskas, V. 2017. Cyber–Physical Systems Expression in Industry 4.0 Context. *Financial and Credit Activity: Problems of Theory and Practice*, 2 (23), 188–197.

Park, Y. A., Fritz, C. and Jex, S. M. 2018. Daily Cyber Incivility and Distress: The Moderating Roles of Resources at Work and Home. *Journal of Management*, 44 (7), 2535–2557.

Pereira, F., Spitzberg, B. H. and Matos, M. 2016. Cyber-harassment Victimization in Portugal: Prevalence, Fear and Help-seeking among Adolescents. *Computers in Human Behavior*, 62, 136–146.

Ritter, B. A. 2008. Cybersexual Harassment: Development and Validation of a Measure of the Online Environment and Online Sexual Harassment. *Academy of Management Annual Meeting Proceedings*, 1, 1–6.

Ritter, B. A. 2014. Deviant Behavior in Computer-Mediated Communication: Development and Validation of a Measure of Cybersexual Harassment. *Journal of Computer-Mediated Communication*, 19 (2), 197–214.

Salter, M. 2018. Publicising Privacy, Weaponising Publicity: The Dialectic of Online Abuse on Social Media. In Dobson, A. S., Robards, B. and Carah, N. (eds.). *Digital Intimate Publics and Social Media*, pp. 29–43.

Sarpotdar, A. 2013. Sexual Harassment of Women: Reflections on the Private Sector. *Economic & Political Weekly*, 48 (40).

Shannon, D. 2008. Online Sexual Grooming in Sweden – Online and Offline Sex Offences against Children as Described in Swedish Police Ddata. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 9 (2), 160–180.

Shapka, J. D. and Maghsoudi, R. 2017. Examining the Validity and Reliability of the Cyber-Aggression and Cyber-Victimization Scale. *Computers in Human Behavior*, 69, 10–17.

Sklenarova, H., Schulz, A., Schuhmann, P., Osterheider, M. and Neutze, J. 2018. Online Sexual Solicitation by Adults and Peers – Results from a Population Based German Sample. *Child Abuse & Neglect*, 76, 225–236.

Spence, E. H. 2012. Virtual Rape, Real Dignity: Meta-Ethics for Virtual Worlds. In Sageng, J. R., Fossheim, H. J. and Larsen, T. M. (eds.). *Philosophy of Computer Games*, Chapter 9, pp. 125–142.

Strikwerda, L. 2015. Present and Future Instances of Virtual Rape in Light of Three Categories of Legal Philosophical Theories on Rape. *Philosophy & Technology*, 28 (4), 491–510.

Surma, I. 2016. Pushing the Boundaries of Digital Diplomacy: The International Experience and the Russian Practice. In Zlateva, T. and Greiman, V. A. (eds.). *International Conference on Cyber Warfare and Security*, pp. 304–311.

Tiidenberg, K. 2014. Bringing Sexy Back: Reclaiming the Body Aesthetic via Self-Shooting. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8 (1).

Vitis, L. and Gilmour, F. 2017. Dick Pics on Blast: A Woman's Resistance to Online Sexual Harassment Using Humour, Art and Instagram. *Crime, Media, Culture: An International Journal*, 13 (3), 335–355.

Vveinhardt, J. and Kuklytė, J. 2017. The Side Effect of Cyberbullying. In Kuzmin, S. V. (ed.). *XLIX Международная научно-практическая конференция «Теория и практика мирового научного знания в XX веке»*, pp. 8–10. ISBN 978-5-9500243-0-6.

Warren, I. and Palmer, D. 2010. Crime Risks of Three-Dimensional Virtual Environments. *Trends & Issues in Crime and Criminal Justice*, 388, 1–6.

Wolfendale, J. 2007. My Avatar My Self: Virtual Harm and Attachment. *Ethics and Information Technology*, 9 (2), 111–119.

Young, G. and Whitty, M. T. 2010. Games Without Frontiers: On the Moral and Psychological Implications of Violating Taboos within Multi-Player Virtual Spaces. *Computers in Human Behavior*, 26 (6), 1228–1236.

AUTHOR'S ADDRESS

Jūratė Kuklytė, Faculty of Economics and Management, Vytautas Magnus University, S. Daukanto str. 28, Kaunas, 44246 Lithuania, e-mail: jurate.kuklyte@vdu.lt