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 anonymously. 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 mas- sive 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-
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:

RQ1: How cybersexual sexual harassment evolve?
RQ2: What are the main vulnerable groups and consequences in different levels?

2 BACKGROUND OF CYBERSEXUAL HARASSMENT

Sexual harassment became an important issue and thoroughly 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 cyberbullying 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. Inappropriate 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 2388 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.
Less common online misbehaviour is virtual rape in a two or three dimensional 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 cyber-bullying 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 –
<table>
<thead>
<tr>
<th>Keywords</th>
<th>Definition</th>
<th>Victims</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online obsessive relational intrusion</td>
<td>“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.”</td>
<td>University students</td>
<td>Marganski and Melander, 2018</td>
</tr>
<tr>
<td>Online sexual aggression</td>
<td>An online actions when males use various coercive strategies to engage the women in consensual sexual activities.</td>
<td>Women</td>
<td>Strikwerda, 2015</td>
</tr>
<tr>
<td>Online sexual harassment</td>
<td>“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.”</td>
<td>Women</td>
<td>Vitis and Gilmour, 2017</td>
</tr>
<tr>
<td>Online aggression</td>
<td>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.</td>
<td>Gamers</td>
<td>Ballard and Welch, 2017</td>
</tr>
<tr>
<td>Online sexual solicitation</td>
<td>“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.”</td>
<td>Adolescents</td>
<td>Gámez-Guadix et al., 2018</td>
</tr>
<tr>
<td>Internet-initiated offense</td>
<td>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.</td>
<td>Adolescents</td>
<td>Kloess et al., 2017</td>
</tr>
<tr>
<td>Cyber-interpersonal violence</td>
<td>Online harassment that consists of spreading of rumors, unwanted sexual photos without consent, and/or threatening individuals, and cyber impersonation.</td>
<td>College students</td>
<td>Choi and Lee, 2017</td>
</tr>
<tr>
<td>Technology-facilitated abuse</td>
<td>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.</td>
<td>Adults</td>
<td>Al-Alosi, 2017</td>
</tr>
<tr>
<td>Virtual rape</td>
<td>“Virtual act of forcing sex upon an unwilling person in virtual environment.”</td>
<td>Virtual agent</td>
<td>Strikwerda, 2015</td>
</tr>
<tr>
<td>Virtual rape</td>
<td>An unwanted sexual intercourse in order to harm the avatar in virtual environment.</td>
<td>Virtual agent</td>
<td>Young and Whitty, 2010</td>
</tr>
<tr>
<td>Online sexual grooming</td>
<td>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.</td>
<td>Adolescents</td>
<td>Shannon, 2008</td>
</tr>
</tbody>
</table>

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

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

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 interpreted 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 multi-level 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
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


**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