CYBER SAFE

Cyber Violence against Women & Girls REPORT

University *of Ljubljana*
Faculty *of Social Sciences*

With financial support from the
Rights, Equality and Citizenship
Programme of the European Union

CYBER SAFE

Changing Attitudes among teenagers
on Cyber Violence against Women and Girls

CYBERSAFE
810264 — CYBERSAFE — REC-AG-2017/REC-RDAP-GBV-AG-2017
WP2 – Report on Cyber VAWG and CYBERSAFE Frameworkn – Final report on WP2
UL FDV

This report was funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020). "The content of this report represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains."

University of Ljubljana
Faculty of Social Sciences

Nexus NI
rape & sexual abuse support

SERIOUS GAMES INTERACTIVE

AZIENDA SPECIALE
RETESALUTE

WAVE

Women's Support and Information Center
There is a way out of violence!

International Child Development Initiatives

UNIVERSITY OF TARTU
Johan Skytte Institute of Political Studies

With financial support from the
Rights, Equality and Citizenship
Programme of the European Union

Cyber Violence against Women & Girls REPORT

Table of Contents

Preface 5
Introduction 6
Terminology 7
Different forms of cyberviolence related to the sexual aspect of violence against girls and women 10
Contextualization: Factors underpinning the emergence of online sexual harassment 11
Dating and cyberviolence 12
Cyberviolence – Children and teens 13
- Gender of victims 13
- Vulnerable groups 14

Impacts of cyberviolence 15
Existing research 17
Existing interventions 23
Childnet international Step Up, Speak Up! 24
Teaching Toolkit 24
Serious games 24
- Conectado 24
- Friendly ATTAC (Adaptive Technological Tools Against Cyberbullying) 25
- FearNot 25
- Online Pestkoppenstoppen (Stop Bullies Online/Stop Online Bullies) 25

Support and Prevention 26
Existing interventions to prevent/raise awareness about cyberviolence in partner countries 29
- Estonia 29
- Greece 30
- Northern Ireland 30
- Italy 31
- Slovenia 31

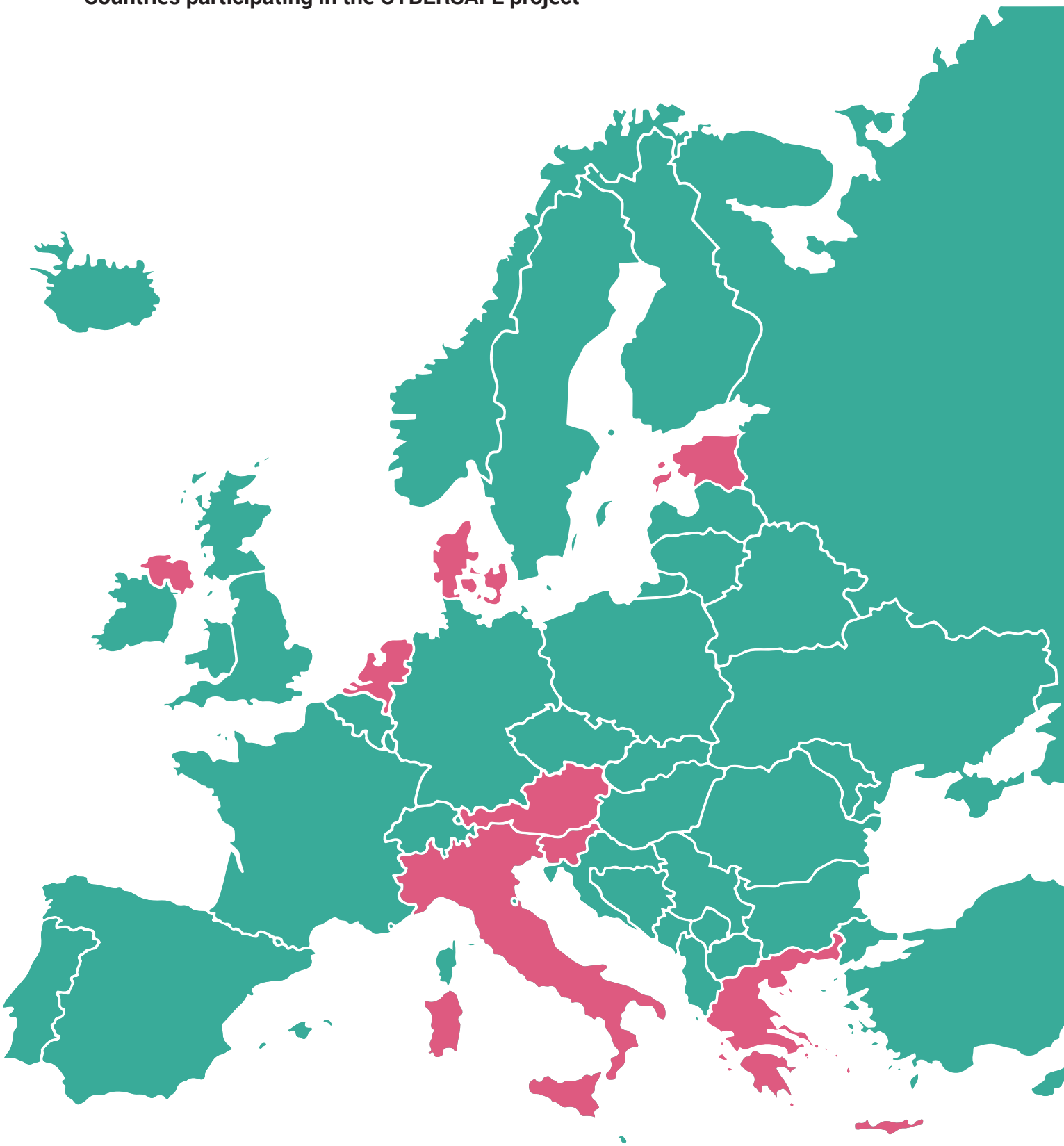
Legislation 32
- Legislation in partner countries 32
- Legislation in other EU countries 33
- Best practice in VAWG legislation 34

Focus groups among teenagers 36
- Summary of results of the focus groups 37
- Key findings of the focus groups 38

Identification of target behaviours & objectives – project framework 38
- The purpose of the framework 38
- Cyberviolence definition 39
- Characteristics of abusive behaviours 40
- Behavioural elements and behaviour change 41
- Why cyberviolence happens? 42
- The needs identified 42
- Behaviours to tackle in the project – Targets 43

Glossary 44
Sources 45

Countries participating in the CYBERSAFE project



Preface

This document is a public output of the CYBERSAFE project – Changing Attitudes among teenagers on Cyber Violence against Women and Girls.

With the CYBERSAFE project we address cyberviolence against women and girls that is gender-based, meaning the act of violence happens because of the gender of the victim.

CYBERSAFE Objectives

- Create an evidence based, attitude-changing prevention educational intervention, for teenagers on Cyber Gender Violence Against Women and Girls (cyber VAWG), applicable to all EU countries;
- Address cyber VAWG as a form of violence against women and girls and develop a systematic gender sensitive approach to prevent it and promote healthy relationships and gender equality online;
- Develop and promote innovative experiential as well as playful educational ICT tools that facilitate behavioural change among teenagers (12–18) on cyber VAWG;
- Facilitate professionals working with teenagers (12–18) to run and implement educational prevention programmes on cyber VAWG;
- Build on and scale up the results of the "CYBERVAW" project;
- Disseminate the developed intervention throughout Europe.

CYBERSAFE target group

The **primary** target group of the project are boys and girls, aged 12–18, as they constitute a population group that heavily builds relationships and communication online. Thus, awareness and education on issues of gender on the cyberspace are of great importance. Moreover, women aged 18–24 constitute the group most at risk of experiencing cyber VAWG and, hence, prevention programmes for teenagers are deemed necessary. In CYBERSAFE, teenagers will be involved in key activities of the project.

Secondary target groups are professionals working with children in formal and informal learning settings (schools, youth centres, sports clubs, activity groups, etc.) are the second target group of the project. They have been selected as we consider it essential to improve their capacity in engaging with prevention and response to cyber VAWG. A third group are professionals working against gender-based violence as they can provide valuable input, especially in terms of being able to present messages that illustrate the harmful effects that can arise from unhealthy (intimate) relationships and gender based violence. Last but not least, stakeholders across Europe (victim support organisations, children organisations, professional networks, policy makers, researchers, etc.) will be targeted via dissemination efforts to help diffuse the best practices developed to the wider European community.

In this document the existing findings on the topic will be presented (literature review), followed by the presentation of the situation in the partner countries and results of focus groups conducted in four participating countries (Italy, Greece, Northern Ireland, Estonia). In the last part the framework of the CYBERSAFE project is presented.

Introduction

In the last decade, the rise of technological advancement as a popular means of socialisation has extended gender violence to a new dimension. As a result, young women experience the digital world both as a site of empowerment and a source of sexual repression.

Violence and discrimination against women are global social issues, where abuse is afflicted systematically, relentlessly and are often times tolerated, if not explicitly condoned. The United Nations Declaration on the Elimination of Violence against Women (GA Resolution 48/104, 20 December 1993) defines violence against women (VAW) as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."[1]

Millions of women and girls around the world are subjected to deliberate violence because of their gender. Violence against women and girls (VAWG) knows no boundaries, cutting across borders, race, culture and income groups, profoundly harming victims, the people around them, and society as a whole.

The growing reach of the Internet, the rapid spread of mobile information and communications technologies (ICTs) and the widespread use of social media have presented new opportunities and enabled various ways to address VAWG.

Online violence against women and girls is gender-based violence through electronic communication and the Internet. Although online violence can affect both women and men, women and girls experience different and more traumatic forms of cyberbullying. There are various forms of cyberbullying against women and girls, such as online stalking, pornography without the consent of the person in the pictures (so-called revenge porn), blaming and harassment for sex, slut-shaming, unwanted pornography, sexual harassment (sextortion), rape and death threats, the collection of information about a victim and the disclosure of her private information on the Internet (doxing) (EIGE, 2017).

The FRA study (2012) found that there are between 5% and 18% of women in the EU over 15 years of age who have already experienced cyberbullying. EIGE - The European Institute for Gender Equality (2017) notes that one in ten women older than 15 years, experience online violence. This proportion is even higher among adolescents. A Slovenian survey found that over 50 % of girls older than 13, has already experienced some form of cyberviolence. Cyberviolence victimisation is reported to be associated with depression and anti-social behaviour (Sargent et al. 2016), diminished self-esteem, as well as fear and anxiety. Some assert that cyberviolence actually might be more damaging than in-person abuse because it has a wide audience, can be anonymous, and is insufficiently regulated.

Cyberviolence can leave a permanent trauma for a woman (or girl). Public memory of shaming and blaming can lead to the internalisation of trauma and mental health challenges, ranging from self- harm as an option to cope with trauma, to suicide as the only remedy to end such trauma. Current reports further point to other psychological trauma and distress such as anxiety, depression due to the fears of shaming, humiliation, harassment, and stigma associated with cyber (sexual) violence (Pashang et al 2018).

Research by the World Health Organization shows that one in three women will experience some form of violence during her lifetime, and despite the relatively new and growing phenomenon of Internet connectivity, it is estimated that one in ten women have already experienced a form of cyberviolence since the age of 15 (EIGE).

The World Health Organization (WHO) defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or mental harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life" (2013:2). The WHO elaborates by saying that "sexual violence is any sexual act, attempt to obtain a sexual act, or other act directed against a person's sexuality using coercion, by any person regardless of their relationship to the victim, in any setting" (2013:2). Sexual violence thus exists on a continuum from obscene name-calling to rape and/or homicide, and includes online forms of sexual violence (e.g., Internet threats and harassment) and sexual exploitation (usually associated with minors but can include adults with particular vulnerabilities – e.g., social, physical, or cognitive disabilities).

There is a vast array of terms used to debate this issue in policy, research, and intervention contexts. These include, but are not limited to: "domestic violence/abuse," "intimate partner violence/abuse," "sexualised violence,"

1 https://www.apc.org/sites/default/files/VAW_ICT_EN_0.pdf

"violence against women," "wife abuse," "dating violence," "gender-based violence," and "gendered violence" (Klein, 2013; Ruiz-Perez, Plazaola-Castaño, & Vives-Cases, 2007). What these various terms have in common is the implicit recognition that violence is gendered. The term "gender-based violence," for instance, has wide distribution and highlights how patterns of violence are shaped by gender roles, behaviours, and norms that contribute to patterns wherein men are significantly more likely to be physically violent toward women than the reverse.

Terminology

When addressing cyberviolence, we are faced with the challenge, as the literature review indicates, of a lack of consistent, standard definitions or methodologies used to conceptualise and measure cyberviolence. As also highlighted by the Council of Europe (2018),there is not yet a stable lexicon or typology of offences considered to be cyberviolence, and many of the examples of types of cyberviolence are interconnected or overlapping or consist of a combination of acts.

The definition used by CoE (2018) is: *Cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.*

As Backe et al (2018) point out, most of the literature focuses on cyberbullying among heterosexual adolescents in high-income countries. Demographic data on perpetrators is limited, prevalence estimates are inconsistent, and almost no primary research has been conducted in low- and middle-income countries (LMIC). Cyberviolence is not only associated with negative psychological, social, and reproductive health outcomes but it is also linked with offline violence, disproportionately affecting women, girls, and sexual and gender minorities.

In this chapter we provide the reader with the most common types of cyberviolence and the terminology used. **There are many overlaps and several terms for one form of violence.** Also, not all forms or instances of cyberviolence are equally severe and not all of them necessarily require a criminal law solution but may be addressed by a graded approach and a combination of preventive, educational, protective and other measures (Council of Europe 2018).

CYBERVIOLENCE CONCEPTS AND RELATED TERMINOLOGY

Cyberviolence	online violence, digital violence, digital abuse, cyber VAWG, cyber abuse, cyber agression, technology-related violence
Online Harassment	Electronic harassment, Internet harassment, cyber gender harassment, cyber/online sexual harassment, technology related cyber VAWG
Cyberbullying	electronic bullying, Internet bullying, cyber aggression, online bullying
CDA	Cyberdating violence, electronic teen dating violence, online dating abuse, Internet partner cyber aggression, cyber teasing, Digital dating abuse (DDA), electronic leashing

Source: Backe et al. 2018

CYBERVIOLENCE

Source: Council of Europe, 2018

Cyberviolence

Cyberviolence is defined by Attrill et al (2015; 136-137) as accessing and distributing of injurious, hurtful or dangerous materials online to cause emotional, psychological or physical harm. The most common form is bullying and harassment. We understand cyberviolence as an umbrella term for many other forms of violence which happen with the use of ICT.

Cyberharassment

Cyberharassment is harassment by means of email, text (or online) messages or the Internet. Cyberharassment is perhaps the broadest form of cyberviolence and involves a persistent and repeated course of conduct targeted at a specific person that is designed to cause severe emotional distress and often the fear of physical harm. Cyberharassment is often targeted at women and girls and termed "cyberviolence against women and girls" (cyber VAWG or Cyber VAWG).

It can take many forms, including but not limited to:

- Unwanted sexually explicit emails, text (or online) messages;
- Inappropriate or offensive advances on social networking websites or Internet chat rooms;
- Threats of physical and/or sexual violence by email, text (or online) messages;
- Hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (such as sexual orientation or disability).

(Source: European Institute for Gender Equality (2017)

FRA (2015) defines cyberharassment as receiving unwanted, offensive, sexually explicit emails or SMS messages; inappropriate, offensive advances on social networking websites or in Internet chat rooms.

Cyberharassment thus involves a range of conduct, including for example "cyberbullying" and "revenge porn".

Online harassment

Duggan et al. (2014) defined five different types of online harassment: being called offensive names, being physically threatened, being harassed for a sustained period of time, being stalked, being purposefully embarrassed, and being sexually harassed

Cyber aggression

Cyber aggression refers to any behaviour enacted through the use of information and communication technologies that is intended to harm another person(s) that the target person(s) wants to avoid. Intent to cause harm should be judged on the basis of how a reasonable person would assess intent. Corcoran, McGuckin& Prentice (2015: 253)

Cyberbullying

According to the general perception, cyberbullying is strongly associated with young people (http://cyberbullyingandstalkingguide.com) and per Attrill et al (2015; 99), includes aspects such as cyberharassment and cyberstalking.

Nocentini et al categorize four main types of cyberbullying behaviour:

- written-verbal behaviours (phone calls, text messages, e-mails, instant messaging, chats, blogs, social networking communities, websites),
- visual behaviours (posting, sending or sharing compromising pictures and videos through mobile phone or internet),
- exclusion (purposefully excluding someone from an online group) and
- impersonation (stealing and revealing personal information, using another person's name and account) (Nocentini, Calmaestra, Schultze-Krumbholz, Scheithauer, Ortega &Menesini, 2010: 130).

Cyberviolence against women and girls is a type of gender-based violence that is perpetrated through electronic communication and the Internet. Although cyberviolence can affect both women and men, women and girls experience different and more traumatic forms of cyberviolence.

There are various forms of cyberviolence against women and girls, including, but not limited to, cyber stalking,

non-consensual pornography (or 'revenge porn'), gender-based slurs, hate speech and harassment, 'slut-shaming', unsolicited pornography, 'sextortion', rape threats and death threats, and electronically facilitated trafficking.

Cyberviolence is not a separate phenomenon to 'real world' violence, as it often follows the same patterns as offline violence. (Source: European Institute for Gender Equality (2017).

Cyberdeviance
Cyberdeviance is defined by Attrill et al (2015; 268) as online behaviours that may not be illegal, but are considered to exist outside of socially accepted norms and beliefs of behaviour.

Cyberstalking
Cyberstalking is stalking by means of email, text (or online) messages or the Internet. Stalking involves repeated incidents, which may or may not individually be innocuous acts, but combined, undermine the victim's sense of safety and cause distress, fear or alarm.

Acts can include:

- Sending emails, text messages (SMS) or instant messages that are offensive or threatening;
- Posting offensive comments about the respondent on the Internet;
- Sharing intimate photos or videos of the respondent, on the Internet or by mobile phone.

To be considered as cyber stalking, these acts must take place repeatedly and be perpetrated by the same person (Source: European Institute for Gender Equality (2017)).

Cyber-porn
Cyber-porn and obscenity based on Wall's typology, is according to Attrill (2015: 136) unique since some forms of sexuality online are legal but porn and obscenity may be deviant or criminal based on local law.

Gender violence
Gender violence is harassment that happens to a person for the sole reason of their gender. Although physical assault is a common form of gender violence, it is not limited to just that. The European Council defines gender-based violence as acts that lead to "physical, sexual, psychological or economic harm or suffering to women." The reasons for gender-based violence are typically not limited to the reasoning by the perpetrator, which can include aggression, revenge, jealousy and entitlement. However, gendered violence against women has become institutionalised in cultures like those of the United States where women are expected to look and act in a specific way. (https://nobullying.com/gender-violence/)

Internet harassment
Internet harassment is "an overt, intentional act of aggression towards another person online" (according to Ybarra, Diener-West & Leaf (2007)).

Non-consensual pornography
Non-consensual pornography (the most common form of which is known as 'revenge porn') involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge.

Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's 'real-world' life (for example, intending to cause a person to be fired from their job, or in some cases causing suicide). (Source: European Institute for Gender Equality (2017))

Different forms of cyberviolence related to the sexual aspect of violence against girls and women

Non-Consensual Distribution of Images

A person's sexual images and videos being shared without their consent or taken without their consent.

- Posting or distributing sexually graphic images or videos online without a person´s permission;
- Revenge porn (is the term used to describe when people (generally men) post naked pictures of their ex-partners (generally women) on designated revenge porn websites with their exes' contact information, including phone number, email address, Facebook profile and home address, for the purpose of humiliating and getting revenge on their ex-partner, resulting in women being bombarded with harassing, degrading, and threatening messages from strangers);
- Sexual images/videos taken without consent ('creep shots' or 'upskirting');
- Sexual images/videos taken consensually (=sexting) but shared without consent ('revenge porn');
- Non-consensual sexual acts (e.g., rape) recorded digitally (and potentially shared).

Exploitation, coercion and threats (= sextortion, could include "grooming")

A person receiving sexual threats, being coerced to participate in sexual behaviour online, or blackmailed with sexual content.

This includes a range of behaviours, such as:

- Harassing or pressuring someone online to share sexual images of themselves or engage in sexual behaviour online (or offline);
- Using the threat of publishing sexual content (images, videos, rumours) to threaten, coerce or blackmail someone ('sextortion');
- Online threats of a sexual nature (e.g., rape threats);
- Inciting others online to commit sexual violence;
- Inciting someone to participate in sexual behaviour and then sharing evidence of it.

Unwanted sexualisation

A person receiving unwelcome sexual requests, comments and content.

This includes a range of behaviours, such as:

- Sexualised comments (e.g., on photos);
- Sexualised viral campaigns that pressurise people to participate;
- Sending someone sexual content (images, emojis, messages) without their consent;
- Unwelcome sexual advances or requests for sexual favours;
- 'Jokes' of a sexual nature;
- Rating peers on attractiveness/sexual activity;
- Altering images of a person to make them sexual.

Unsolicited pornography

Unsolicited exposure to sexual materials. E.g. random and unsolicited sending of sexual images or videos from men to young women, notoriously referred to as "dick pics". (In the UK, 41% of women aged 18 to 36 have reportedly received non-consensual sexual images.)

Cyberstalking

Cyberstalking is stalking by means of email, text (or online) messages or the Internet. Stalking involves repeated

incidents, which may or may not individually be innocuous acts, but combined undermine the victim's sense of safety and cause distress, fear or alarm.

Acts can include:

- Sending emails, text messages (SMS) or instant messages that are offensive or threatening;
- Posting offensive comments about the respondent on the Internet;
- Sharing intimate photos or videos of the respondent on the Internet or by mobile phone.

To be considered as cyberstalking, these acts must take place repeatedly and be perpetrated by the same person.

Harassment and stalking online – 'cyberstalking' – is a particular problem for young women because of their greater use of and exposure to the Internet and social media. Where cyberstalking exists, operators of social media platforms should ensure that victims have quick and effective recourse to assistance if they are targeted by repetitive abusive behaviour. This is particularly important for young people, who may not be in a position to easily stand up to a deluge of abuse that can occur in the form of sexual threats and 'hate' in the form of misogyny.

Slut-shaming

Slut-shaming is the practice of criticizing people, especially women and girls, who are perceived to violate expectations of behaviour and appearance regarding issues related to sexuality.

Cyber dating abuse (CDA)

using technology to monitor and control the behaviours of a partner; using a partner's password without permission to access his or her mail or social media accounts; installing tracking devices or apps to monitor a partner's location; or perpetrating emotional aggression and verbal threats through digital means during or after a relationship has ended[2].

Contextualization: Factors underpinning the emergence of online sexual harassment

As pointed out in deSHAME (2017), online sexual harassment emerges from a complex combination of societal, peer, relationship and developmental factors, which are mediated and facilitated by digital technology. deSHAME (2017) report outlines the following factors:

- **Societal factors:** Online sexual harassment takes place in societal context, where a pervasive culture of sexualisation, misogyny and homophobia is often left unchallenged (Henry & Powell, 2016; Womens Aid, 2014). The issues of 'slut shaming' and 'victim blaming' are not unique to teens (Pew Research Centre, 2014) or to online sexual harassment (e.g., Hackman et al., 2017), but like with all forms of sexual violence, they play a central role in determining how it is experienced. Other intersecting factors, including race, ethnicity, disability, sexuality or sexual identity often create further marginalisation of young people experiencing online sexual harassment.

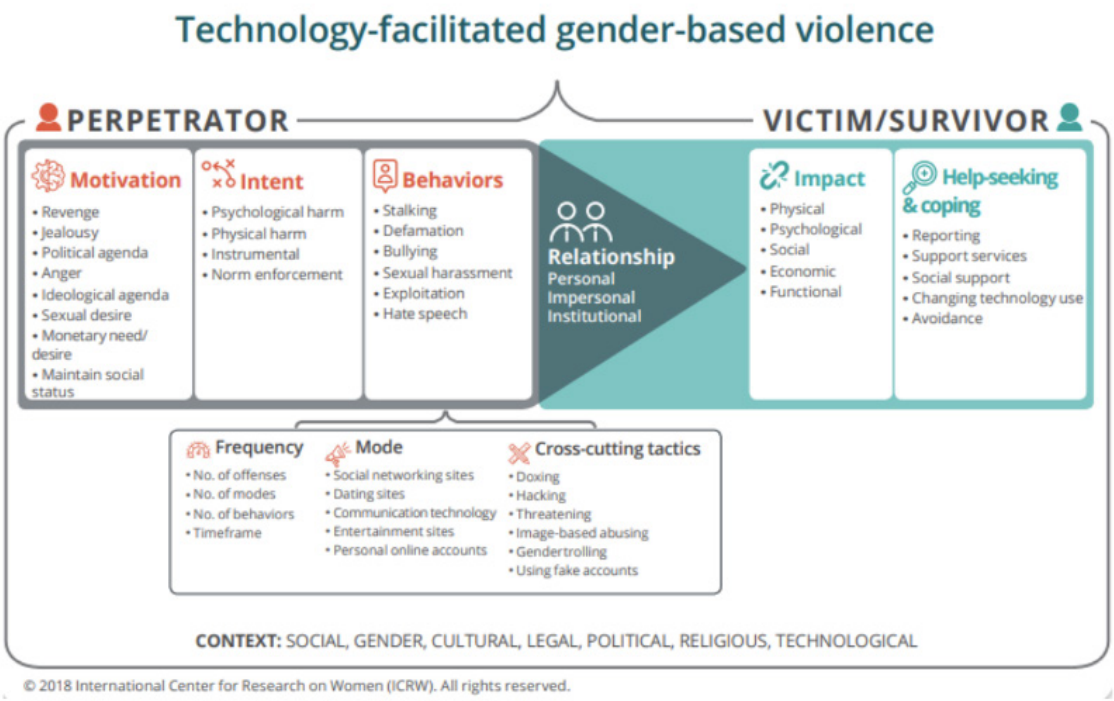
- **Peer group factors:** Whilst wider societal norms and attitudes underpin much of young people's behaviours, it is clear that their intimate relationships and incidents of online sexual harassment are also being played out in a more localised manner in the context of their peer groups, with peer norms and attitudes driving their behaviour. As young people negotiate peer approval and acceptance, there can be intense peer pressure to engage in sexual activities, and peer groups can normalise the expectation to engage with certain activities with a group attitude of 'everyone is doing it' – even if this isn't the case. Any perceived violation of expected norms can result in 'shaming' and this often plays out online. The values of the peer group can also shape young people's attitudes and expectations of relationships, including normalising potentially harmful behaviours.

2 https://www.liebertpub.com/doi/full/10.1089/vio.2017.0056

- **Relationship factors:** As young people explore their early sexual interactions and intimate relationships, they learn about consent, respect and trust. They may cross the line between flirting and harassment, encouragement and coercion. Sometimes these behaviours are abusive or exploitative or reinforce damaging perceptions of gender and sexuality.

- **Developmental factors:** As young people transition from childhood to adulthood, developmental factors underpin their tendency to seek new sensations, take risks and explore their budding sexuality, while their vulnerability towards peer pressure and lack of understanding about sex and relationships can place them at a greater risk.

The International Centre for Research on Women has developed a conceptual framework for understanding technology-facilitated gender-based violence, including what motivates perpetrators to commit acts of cyber VAWG and the potential impact such acts have on victims (Hinson et al, 2018) (see diagram below).



Source: International Centre for Research on Woman, 2018

This conceptual framework helps us to better understand the relationship between online and offline violence against women and girls. Though acts of violence may be committed online, the motivation for these acts is rooted in the offline world, in the emotional, psychological, cultural and ideological drivers behind the perpetrator's behaviour. Likewise, even though acts of violence may be committed online, the impact of these acts is felt by victims/survivors offline, in the real world, where they experience physical, psychological, social and economic harm.

Dating and cyberviolence

A relatively new and important topic in cyberviolence research concerns how cyberviolence and dating coincide. While this topic gets a lot of attention in the field of adult Internet users, only a handful of studies that delve into this subject with young respondents exist.

Baker and Carreño (2016) conducted a study with focus groups consisting of 39 high school aged adolescents who had been in a problematic relationship in the past year. The adolescents used technology to initiate and end their relationships, often using text messages or posts on social networking sites. The adolescents also used technology to incite jealousy, and to monitor and isolate partners from others. Furthermore, they often used a mixture of technology

during their relationships; cell phone calls, texts, posting comments/pictures to personal pages on social networking sites. One of the findings of this study was that technology use made feelings of jealousy worse, resulting in quarrels and violence between couples. Participants mentioned using technology to monitor their partner and being monitored themselves. Using technology had a different meaning for girls, who saw it as an opportunity to get to know a boy before in-person contact occurred, whilst boys viewed it as a means of preventing them from being rejected and consequently embarrassed. Korchmaros, Ybarra and Mitchell (2015) concluded that a minority of adolescents use the Internet to initiate romantic relationships; and that the Internet benefits adolescents who have difficulty forming relationships as well as those who do not (Korchmaros, Ybarra and Mitchell, 2015: 62). Consistent with this explanation, authors cite Peter et al. (2005) found that introverted adolescents were »motivated to communicate online to counter their lack of social skills, which increased the likelihood of forming friendships online. Conversely, they found that extroverted adolescents formed friendships online as a consequence of their frequent online communication and self-disclosure« (Korchmaros, Ybarra and Mitchell, 2015, 60-61). They conclude that even though youngsters are using the Internet to form romantic relationships, they also seem to continue to rely on conventional methods to meet romantic partners.

Cyberviolence – Children and teens

Cyberviolence victimisation is connected to traditional bullying, whilst also being a unique phenomenon. Pšunder (2012: 46) pinpoints that with traditional violence, the power of the perpetrator lies in his/hers physical and social characteristics (like popularity), whilst with cyberbullying, the power lies in ICT knowledge. Randa, Nobles & Reyns (2015: 182) noticed: »Among cyberbullying victims, only 16,73 % reported not experiencing traditional bullying, and only 1% of all respondents reported experiencing cyberbullying without having experiencing any form of traditional bullying victimisation. Conversely, and perhaps equally important, we find that a large majority (83%) of cyberbullying victims report experiencing both cyber and traditional bullying victimisation. Furthermore, nearly 1 in 5 victims of traditional bullying are also being victimized 'online'.

NCGM survey, conducted in 7 EU states, found that only slight differences by socioeconomic status are noted, with children from middle socio-economic status homes reporting more frequent levels of bullying (O'Neill in Dinh, 2015: 387).

Gender of victims

Older and newer studies are still inconclusive on the effect of gender on being a victim or a perpetrator. Slonje and Smith (2008) in their study in Sweden concluded that gender didn't have an effect on being a victim of cyberviolence.

Rivers and Noret (2010) reported an increase in girls in cyberviolence. The exploratory analyses of the content of the text and email messages received indicated that boys received more hate-related messages than girls, and that girls were subject to more name-calling than boys. Although they did not find any significant links between sex and reasons for being bullied, they did find that students who had received nasty or threatening text messages and emails were victims of other forms of bullying as a result of their appearance, clothing, weight, size, or body shape, or because they were called 'gay' (boys in this case) (Rivers and Noret, 2010: 663).

Smith, Mahdavi, Carvalho, Fisher, Russell & Tippett (2008: 383) did find girls to be more often victims of cyberbullying in Study One, which was not confirmed in Study Two, where no gender differences were found for being a cybervictim or cyberbully; but the lack of a gender difference for bullying others does suggest a greater involvement of girls in traditional bullying, where the boys always predominated.

Considering the results of newer studies, the NCGM survey shows that the incidence of bullying in seven EU states was higher among girls overall and for those in their mid-teens, aged 13–14 years (26 %). Girls were more likely to experience bullying (26 %) than boys (19 %) and were more likely to be upset by it (20 %), compared to only 13% of boys (O'Neill, Dinh, 2015).

In an Irish sample of the same NCGM survey, more girls reported being bullied at all, with gender being a factor defining the form of cyberbullying. More boys than girls reported being bullied face-to-face, especially in the younger cohort. When we consider teenagers, more than twice as many girls reported being bullied online than boys (20 % compared to 8 %). Three times as many girls than boys reported being bullied via SMS (6 % vs. 2 %), and girls reported more than twice the amount of bullying on social networking sites (14 % vs. 5 %) (O'Neill, Dinh, 2013).

Lindfors, Kaltiala-Heino and Rimpelä (2012) reported that girls in their Finnish sample more often confessed to experiencing at least one dimension of cyberviolence during the previous year and that this discrepancy between sexes was highest among 14-year-olds and lowest among 18-year-olds of both sexes. Girls commonly witnessed the cyberviolence of friends (16 %); and were a victim slightly more frequently than they were a bully (11% vs. 9%). An equal proportion of boys – one tenth - had been a victim, a bully, or had witnessed cyberviolence. It was least common for both sexes and in all age groups to be a bully-victim. Girls reported serious and disturbing bullying more often than boys (Lindfors, Kaltiala-Heino and Rimpelä, 2012).

Navarro, Yubero, Larrañaga & Martínez (2012) found that sex differences did not emerge among the Spanish schoolchildren in the victim group.

Mena-Rodriguez & Velasco-Martínez (2017) have touched upon the topic of gender violence and social networks in adolescents in Malaga. Their research topic was gender violence among adolescent students, 15–17-years of age, from the province of Malaga. Additionally, they wanted to identify the predictive factors of occasional and frequent violence on social networks. The study was conducted in electronic form with 283 participants. The results show that there are significant differences in regard to which social networks young people use; girls preferred Facebook, Twitter and Instagram while boys used Skype more. Both sexes perceived the risks of the Internet similarly and girls considered opening a social network profile as more risky than boys (Mena-Rodriguez & Velasco-Martínez, 2017: 48). Young girls deemed more actions as violent, or more violent than their male counterparts (Mena-Rodriguez & Velasco-Martínez, 2017: 49).

Vulnerable groups

One of the crucial questions in the research on the topic of cyberviolence is “which group of young people is most at risk for cyberviolence?”

Unsurprisingly, Smith et al. (2008: 383) have pinpointed the risk factor of using the Internet; those students who use the Internet more regularly appear to be at greater risk of experiencing at least some cyberviolence.

More recently, O'Neill and Dinh (2015) concluded on the Irish sample of the NCGM study that smartphone users (17 %) and tablet users (15 %) were more likely to experience any form of cyberviolence in comparison to the children who do not use mobile devices at all (8 %). The authors showed also that smartphone users are more likely to engage in the various forms of cyberviolence (O'Neill and Dinh, 2015: 392).

Similarly, the results of all seven EU countries that participated in NCGM show that both boys and girls across all age groups, who have at least one SNS profile, were at least twice as likely to be cyberbullied than children who had no SNS profile. Almost one quarter (23 %) of 13–16-year-old girls who had at least one SNS profile were more likely to be cyberbullied, compared to 4 % of girls from the same age group. For boys, the percentages were 9 % compared to 1% of boys from the same age group. This was true for the Irish population as well (O'Neill, Dinh, 2015).

The findings of Tsitsika et al. mirror this almost perfectly; they also found that »high frequency of Internet use in general, as well as SNS use in particular (i.e., more than two hours per day), was significantly associated with victimisation online among the study participants« (Tsitsika et al., 2015: 6).

If we touch upon psychological characteristics of the victims: Navarro, Yubero, Larrañaga & Martínez (2012) named social anxiety, interpersonal difficulties and lack of social skills as predictors of victimisation in cyberspace in a large Spanish sample. Primary school students, who were ten to twelve years old (n=1127), took part in a study that used a self-report questionnaire which measured cyberviolence victimisation, social anxiety and social competence. The researchers found that specific symptoms of social anxiety, that is fear of negative evaluation, combined with interpersonal difficulties to communicate with peers and close friends and lack of appropriate social skills, all increased the likelihood of the child being cyberbullied. Researchers conclude that increased worry about others' judgement is what makes children vulnerable to cyberviolence. Furthermore, children with poor social skills, those who find it difficult to talk in front of a large group of people or to interact with friends, are also at risk of being cyber-victimized.

Similarly, Ybarra, Alexander & Mitchell (2005) suggested that young people with depressive symptoms use the Internet more intensely, perhaps avoiding in-person interaction at school where the possibility of peer-to-peer interface is greatest. Rivers and Noret (2010) have found that among girls, unpopularity among peers was associated with receiving nasty or threatening text messages and emails. The unpopularity was measured with the help of four ques-

tions – *do you feel lonely at school, do you feel you are less well liked than other pupils, how many good friends do you have in your class and how often does it happen that other pupils don't want to spend break times alone with you* (Rivers and Noret, 2010: 653).

We can't, however, distinguish completely between what was before the victimisation and what was after. However, we will touch upon this subject in the chapter of consequences, where authors like Dempsey et al (2009) agree that the symptoms – depression and social anxiety – are the results of peer victimisation, including in cyber settings.

Navarro, Serna, Martínez and Ruiz-Oliva (2012) have shed some light on the correlation between how much parents monitor their children when they use Internet, and the cyber victimisation of the children. Their sample of youngsters (10–12 years) from rural public schools was large (1068 pupils). The results of the self-report questionnaire show that parent's monitoring of computer software, the creation of rules about time spent online, as well as the degree to which young people discuss personal information with their parents, lessen the likelihood of online victimisation.

Impacts of cyberviolence

West (Cyberviolence against women, 3) points out the uniqueness of cyberviolence against women:

1) the anonymity so easily maintained online translates into impunity for perpetrators of online violence,

2) it is easy to commit an act of cyberviolence against women due to:

   a. the automation of technology, requiring little or no technical knowledge to do things like monitor a woman's movements or make slanderous comments about her,

   b. the affordability of the technology, which makes it inexpensive to distribute a woman's photograph or create and propagate misogynistic images and writing, and

   c. the ability to contact anyone in the world from anywhere in the world broadens the pool of potential victims and reduces the probability of getting caught. The third aspect that makes cyber-violence against women unique is digital permanence. As the saying goes, "the Internet records everything and forgets nothing". Whatever content is posted about a person on the Internet becomes a part of their permanent online identity. (Source: http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf)

One thing we should consider above all when thinking about cyberviolence victimisation as Slonje and Smith (2008) point out, is how it affects children's psychosocial functioning and its negative impact might be even stronger than traditional bullying since the aggressors can follow their victims to their homes. Studies show that victims show an elevated level of distress (Smith, Mahdavi, Carvalho, Fisher, Russell & Tippett, 2008), symptoms of depression (Ybarra, Alexander & Mitchell, 2005), low self-esteem (Frisen, Berne, Lunde, 2014), higher levels of social anxiety (Dempsey et al. 2009, Navarro, Yubero, Larrañaga & Martínez, 2012), more interpersonal difficulties and less appropriate social skills than the children forming the non-victim group. The aftermath of cyberbullying sometimes even went as far as (Navarro, Yubero, Larrañaga & Martínez, 2012) suicidal thoughts (Hinduja & Patchin, 2010) and internalizing and externalizing problems (Tsitsika et al., 2015).

Moreover, and perhaps more importantly, we should realise, as the study by Dempsey et al. (2009) demonstrates, that cyber victimisation is a form of victimisation that is separate when comparing to overt or relational victimisation, and that "cyber victimisation is a unique phenomenon that youth may encounter regardless of whether they are exposed to overt or relational aggression in other settings" (Dempsey et al., 2009: 969).

Smith, Mahdavi, Carvalho, Fisher, Russell & Tippett (2008) concluded after the results of Study One data that respondents reported that picture/video clip bullying, distributing abusive images of the victim widely in the peer group could have a strong negative impact on the victim, much more than traditional bullying, while they did not perceive other media of cyberbullying as having such a high impact.

The proportion of adolescents in the Finnish study, who perceived cyberviolence as very serious and disturbing was extremely small (1%). The percentage remained small even when those who reported they found bullying only slightly serious and disturbing were included (Lindfors, Kaltiala-Heino and Rimpelä, 2012).

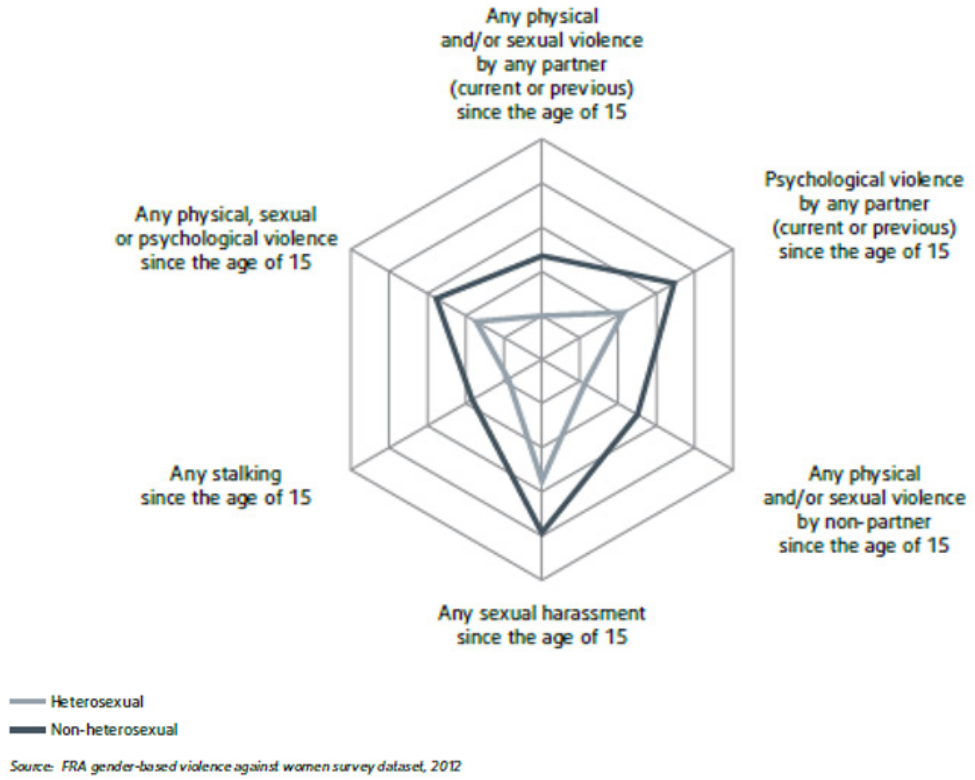
Frisen, Berne and Lunde (2014) investigated the relationship between cyber victimisation and body esteem among Swedish pupils (1076 respondents, ages 10–15). They were interested in young people's opinion about how often the cyberviolence was directed at the victims' appearance, and if this view was more common when girls were cybervictims compared to when the victims were boys. The results showed that the victims of cyberviolence reported poorer body image than non-victims. The results also showed that pupils believed that cyberviolence was directed at the victims' appearance, especially in the case of a girl being the victim.

Dredge, Gleeson & and de la Piedad Garcia (2014:16) interviewed twenty-five adolescents (15–24 years old). All participants reported experiencing an emotional impact as the result of an incident on a social networking site. The overwhelming majority, or 84 % of adolescents, reported a behavioural impact, 80% a social impact, 56 % a cognitive impact, 12 % a physical impact and 24 % reported experiencing no impact at all.

West's report for BWSS concluded that the impacts of cyberviolence against women are psychological, social, physical and economic. The most prevalent are psychological impacts, which are felt by most women who experience cyberviolence. 65 % of women from the survey reported experiencing some sort of psychological impact, ranging from anxiety and damaged self-image at one end of the spectrum (with roughly half and 43% of respondents respectively), to the extreme end, which incorporated thoughts of suicide and engaging in self-harming behaviour (10% of respondents). The economic impacts, particularly non-consensual distribution of images and revenge porn, result in a drop in credit rating. Cyberviolence can also coincide, exacerbate or lead to physical violence, particularly if online violence did not give the perpetrator the expected results. Social impacts include isolation from friends and family, as the threat of exposing information that could potentially cause women's friends and family to turn against them is taken very seriously. (Source: http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf)

The EU survey on Violence against women, undertaken in 2014, shows the impact of various forms of violence against women across the EU; violence against women undermines women's core fundamental rights such as dignity, access to justice and gender equality. For example, one in three women (33 %) have experienced physical and/or sexual violence since the age of 15, every second woman (55 %) has been confronted with one or more forms of sexual harassment. (Source: Violence against women: an EU-wide survey, European Union Agency for Fundamental Rights, 2014)

Figure A3.1: Prevalence of various forms of violence by women's self-declared sexual orientation



Source: FRA gender-based violence against women survey dataset, 2012

Existing research

While the issue of cyberbullying involving children is well researched, statistical studies focusing on cyberviolence against women in different regions of the world is less prevalent.

In the exploratory study, published by Branch et al – Revenge Porn Victimisation of College Students in the United States: An Exploratory Analysis in IJCC in June 2017, 470 college freshmen were surveyed about their practices and perceptions around revenge porn. Findings revealed that approximately 10% of the current sample had had a private photo shared beyond the intended recipient, and that male students and female students had different experiences. More specifically, victims of revenge porn were predominantly female, freshmen, and 18 years of age and the majority of private pictures that were forwarded to others beyond the intended recipient were sent by a current or former boyfriend.

Anecdotal reports suggest that having a picture shared that was intended to be private has a significant negative impact on the victim and that women are more likely to be victims of this behaviour. As a result, individuals have begun to raise awareness about this issue. Recent efforts have focused on creating and/or changing legislation to allow for criminal penalties for engaging in "revenge porn". While research on sexting has proliferated, a dearth of empirical literature exists concerning college students' experience with former boyfriends or girlfriends sharing pictures that were intended to be private and instead used for revenge purposes.

Findings also indicate that students who also forwarded private pictures to someone beyond their intended recipient were more likely to have their own private pictured shared as well. It is interesting to see that victims of this behaviour are offenders too. (Source: http://www.cybercrimejournal.com/Branchetalvol11issue1IJCC2017.pdf)

UK's Women's Aid survey in 2014

on online domestic abuse made the following findings:

- For 85 % of respondents the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline.
- Nearly a third of respondents (29 %) experienced the use of spyware or GPS locators on their phone or computers by a partner or ex-partner.
- For half (50 %) of respondents the online abuse they experienced also involved direct threats to them or someone they knew.
- Nearly a third of those respondents who had received threats stated that where threats had been made online by a partner or ex-partner they were carried out. Source:

https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

Amnesty International and IPSOS MORY

conducted a survey on online abuse in 2017 or harassment on women in the UK, US, New Zealand, Spain, Italy, Poland, Sweden and Denmark aged 18-55 years.

Table 1: Have you ever personally experienced abuse or harassment online?

	Total	UK	US	New Zealand	Spain	Italy	Poland	Sweden	Denmark
Yes, on more than one occasion	451 11%	50 10%	95 19%	66 13%	42 8%	38 8%	30 6%	93 19%	36 7%
Yes, on one occasion	463 12%	56 11%	72 14%	77 15%	52 10%	43 9%	56 11%	55 11%	51 10%
No, this has never happened to me	2960 74%	393 78%	323 65%	337 67%	395 79%	408 81%	376 75%	326 65%	403 80%
Don't know	109 3%	5 1%	8 2%	14 3%	10 2%	7 1%	32 6%	22 4%	11 2%
Prefer not to say	27 1%	1 *	2 *	6 1%	1 *	5 1%	7 1%	3 1%	2 *

Source: Amnesty International 2017

As the table shows, a total of 23 % of women have already experienced abuse or harassment online at least once. In the UK there are 22 %; in Italy 17 % and in Denmark there are 17 % who have already experienced abuse or harassment online at least once.

Platforms where the harassment happens differ among countries, as the popularity of platforms differs among countries. Nevertheless, the most often mentioned platform is Facebook, in addition to Facebook messenger, Instagram and Snapchat.

Table 2: On which, if any, of the following websites or social media platforms have you experienced abuse or harassment online?

	Total	UK	US	New Zealand	Spain	Italy	Poland	Sweden	Denmark
Facebook	525 57%	64 60%	114 68%	91 63%	42 45%	44 54%	46 53%	78 52%	46 53%
Facebook Messenger	211 23%	24 23%	49 29%	46 32%	17 18%	19 24%	12 14%	28 19%	15 18%
Twitter	68 7%	17 16%	16 10%	5 3%	19 20%	- -	1 1%	9 6%	1 1%
Instagram	95 10%	5 5%	28 17%	12 8%	15 16%	8 10%	2 2%	17 11%	7 8%
Snapchat	51 6%	8 8%	11 7%	8 6%	2 2%	1 1%	1 1%	9 6%	10 12%
WhatsApp	77 8%	13 12%	8 5%	5 3%	21 22%	17 21%	4 5%	5 3%	4 5%
Pinterest	2 *	- -	1 1%	1 1%	- -	- -	- -	- -	- -
LinkedIn	9 1%	- -	4 2%	- -	3 3%	- -	- -	1 1%	1 1%
Reddit	8 1%	1 1%	5 3%	- -	2 2%	- -	- -	- -	- -
4Chan	3 *	- -	1 1%	- -	1 1%	- -	- -	1 1%	- -
Twitch	7 1%	- -	4 2%	1 1%	1 1%	- -	- -	1 1%	- -
YouTube	54 6%	7 7%	12 7%	4 3%	11 12%	3 4%	3 4%	12 8%	1 1%
Another web forum or chatroom	224 25%	22 21%	32 19%	25 17%	26 28%	20 25%	14 16%	61 41%	24 28%
The comments section under a news article online	60 7%	5 5%	16 10%	7 5%	7 7%	2 2%	7 8%	14 9%	2 3%
The comments section under a personal blog	42 5%	4 4%	9 5%	3 2%	4 4%	2 2%	4 5%	14 10%	2 2%

In messages sent to my private or work email address	117 13%	15 14%	19 11%	19 13%	10 11%	12 15%	19 22%	19 13%	3 4%
Somewhere else	113 12%	10 9%	23 14%	14 10%	8 9%	7 9%	25 29%	17 12%	8 10%
Don't know	9 1%	- -	1 1%	2 1%	3 3%	- -	2 2%	1 1%	- -
Prefer not to say	12 1%	- -	3 2%	4 3%	- -	2 2%	1 1%	2 1%	- -

Source: Amnesty International 2017

Violence against Women: An EU-wide survey

The FRA survey on violence against women is based on face-to-face interviews with 42,000 women across the EU. The survey was carried out between March and September 2012 and presents the most comprehensive survey worldwide on women's experiences of violence.

The survey responds to a request for data on violence against women from the European Parliament, which was reiterated by the Council of the EU in its Conclusions on the Eradication of Violence against Women in the EU.

The survey asked women about their experiences of physical, sexual and psychological violence, including domestic violence, since the age of 15 and over the 12 month period before the interview. Questions were also asked about incidents of stalking, sexual harassment, and the role played by new technologies in women's experiences of abuse. In addition, the survey asked about respondents' experiences of violence in their childhood.

To assess the extent to which new technologies have been used for sexual harassment of women, two items from the survey – 'unwanted sexually explicit emails or SMS messages' and 'inappropriate advances on social networking websites' – can be analysed as forms of 'cyberharassment'. In this way, it can be seen that one in 10 women (11 %) has faced at least one of the two forms of cyberharassment since the age of 15, and one in 20 (5 %) in the 12 months before the survey. At EU Member State level, countries cluster at the upper and lower ends of the scale in close accord with the distribution of the overall lifetime prevalence of sexual harassment. Denmark and Sweden (both 18 %), and Slovakia and the Netherlands (both 17 %) show the highest prevalence rates. The lowest rates are in Romania (5 %), and in Lithuania and Portugal (both 6 %). The variation in the prevalence of cyberharassment ranges between 5 % and 18 % across Member States.

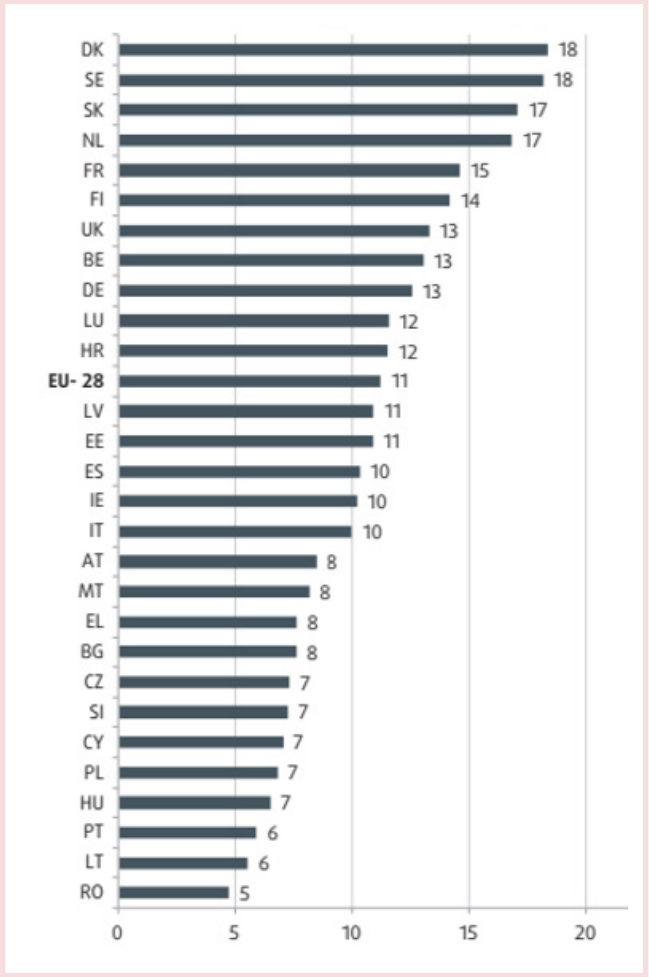
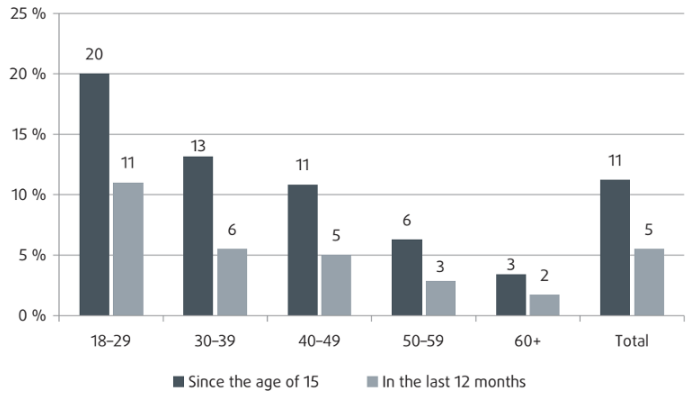


Figure 1: Cyberharassment since the age of 15, by EU Member State (%)

Figure 2: Forms of sexual cyberharassment since the age of 15 and in the 12 months before the interview, by age group (%)

Source: FRA gender-based violence against women survey dataset, 2012



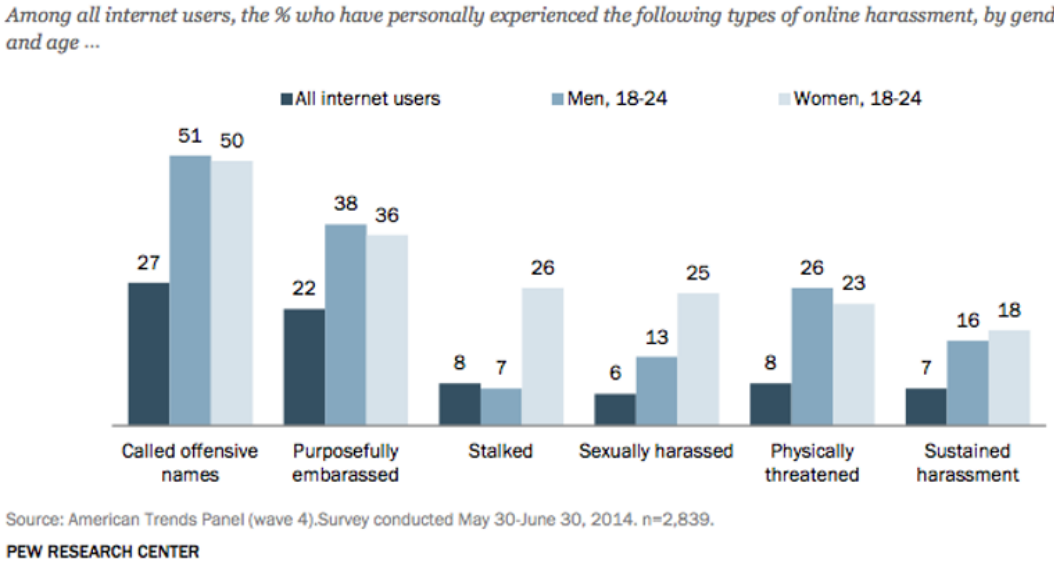
The risk of young women aged between 18 and 29 years becoming a target of threatening and offensive advances on the Internet is twice as high as the risk for women aged between 40 and 49 years, and more than three times as high as the risk for women aged between 50 and 59 years.

UK's Women's Aid survey in 2014

on online domestic abuse reports the following findings:

- For 85 % of respondents the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline.
- Nearly a third of respondents (29 %) experienced the use of spyware or GPS locators on their phone or computers by a partner or ex-partner.
- For half (50 %) of respondents the online abuse they experienced also involved direct threats to them or someone they knew.
- Nearly a third of those respondents who had received threats stated that where threats had been made online by a partner or ex-partner they were carried out.

Figure 3: Young women experience particularly severe forms of online harassment



Source: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

Childnet International – conducted project deSHAME
is a collaboration between Childnet, Save the Children (Denmark), KekVonal (Hungary) and UCLan (UK), co-financed by the EU. The project aims to increase reporting of online sexual harassment among minors and improve multi-sector cooperation in preventing and responding to this behaviour.

Research was conducted with 3275 young people (13–17) who answered the online survey, 107 young people participated in focus groups, 29 teachers took part in focus groups and 19 interviews with professionals (including police, helpline staff, other agencies) were conducted.

In the study, sexual harassment has been categorised in four main types. These different behaviours are often experienced simultaneously and can overlap with offline experiences of sexual harassment.

Non-consensual sharing of intimate images and videos
A person's sexual images and videos being shared without their consent or taken without their consent.

Exploitation, coercion and threats
A person receiving sexual threats, being coerced to participate in sexual behaviour online, or blackmailed with sexual content.

Sexualised bullying
A person being targeted by, and systematically excluded from, a group or community with the use of sexual content that humiliates, upsets or discriminates against them.

Unwanted sexualisation
A person receiving unwelcome sexual requests, comments and content.

Key findings of deSHAME project:

Non-consensual sharing of intimate images
- 6 % of respondents aged 13–17 years across Denmark, Hungary and the UK have had their nude or nearly nude image shared with other people without their permission in the last year, while 41 % have witnessed this happening.
- 68 % of respondents agree that people will think badly about a girl if her nude or nearly nude image is posted online, whereas a smaller proportion would think the same if it were a boy (40 %).
- 25 % have witnessed young people secretly taking sexual images of someone and sharing them online, while 10 % admitted they had done this in the last year.

Exploitation, coercion and threats
- 9 % of respondents aged 13–17 years across Denmark, Hungary and the UK have received sexual threats online from people their age in the last year, while 29 % have witnessed this happening.
- 6 % of respondents said that someone used sexual images of them to threaten or blackmail them in the last year.
- 10 % said their boyfriend or girlfriend had pressured them to share nude images in the last year, with girls being more likely to report this.

Sexualised bullying
- 25 % of respondents aged 13–17 years across Denmark, Hungary and the UK have had rumours about their sexual behaviour shared online in the last year, with over two-thirds of respondents (68 %) saying that girls are judged more harshly for this than boys.
- 31 % had seen people their age creating fake profiles of someone to share sexual images, comments or messages in the last year, while almost half (48 %) witnessed other young people sharing personal details of someone who is seen as 'easy'.
- 80 % had witnessed people their age using terms like 'sket' or 'slut' to describe girls in a mean way online in the last year, while over two-thirds (68 %) had witnessed people using homophobic or transphobic language online.

Unwanted sexualisation

- 24 % of respondents aged 13–17 years across Denmark, Hungary and the UK have received unwanted sexual messages and images in the last year, with girls being significantly more likely to experience this (30 %) compared to boys (13 %).
- 24 % reported that they had received sexual comments on a photo they posted of themselves in the last year, with girls being significantly more likely to experience this (26 %) compared to boys (18 %).
- 45 % of respondents aged 13–17 years said that they have witnessed people their age editing photos of someone to make them sexual, for example putting their face on a pornographic image or placing sexual emojis over them.

According to **CYBERVAW** (2018) study conducted in Slovenia, were the target population included primary and secondary school children between 12 and 19 years:

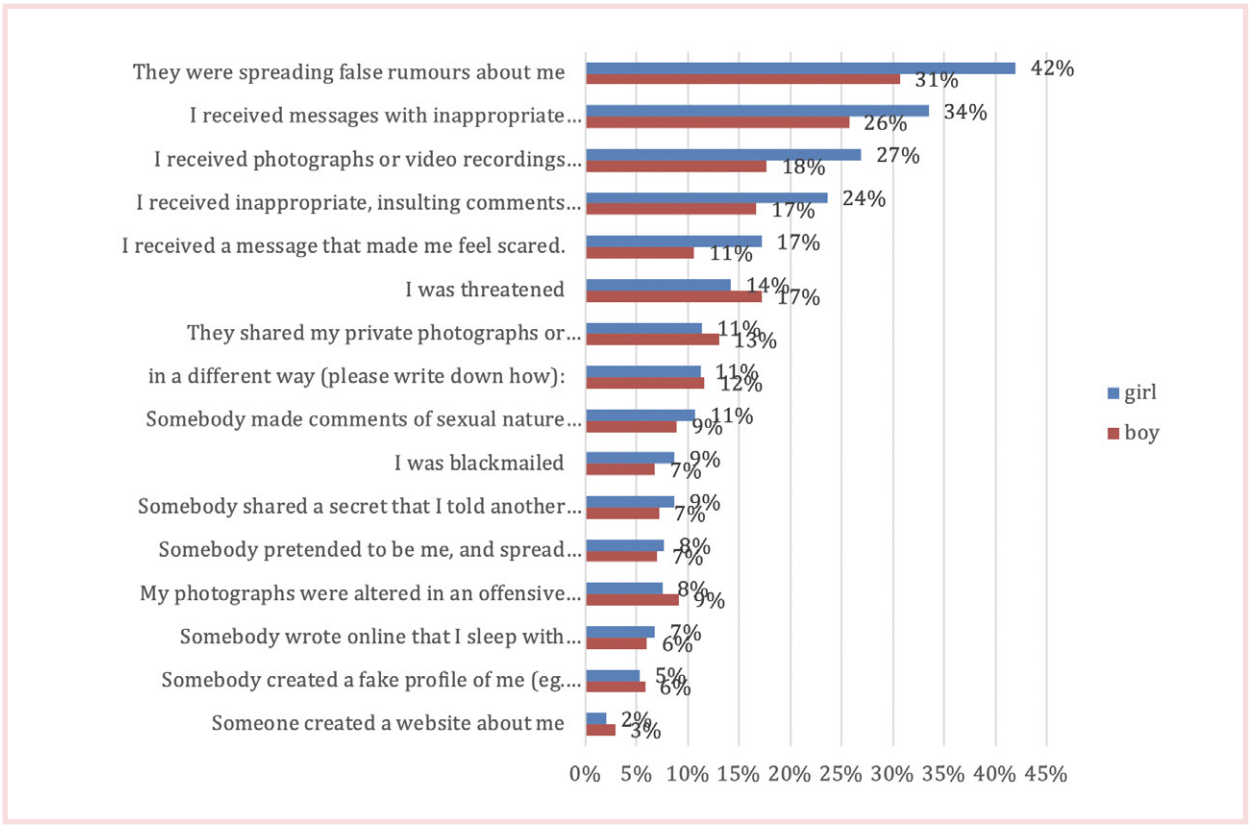
- 56 % of girls in primary school (12–15 years) have already experienced at least one form of cyberviolence
- 65 % of girls in secondary school (15–19 years) have already experienced at least one form of cyberviolence.

The most frequent forms of violence they experienced were the following:

- They were spreading false rumours about me
- I received messages with inappropriate content
- I received inappropriate, insulting comments about my appearance
- I received photographs or video recordings that I didn‘t want to see.

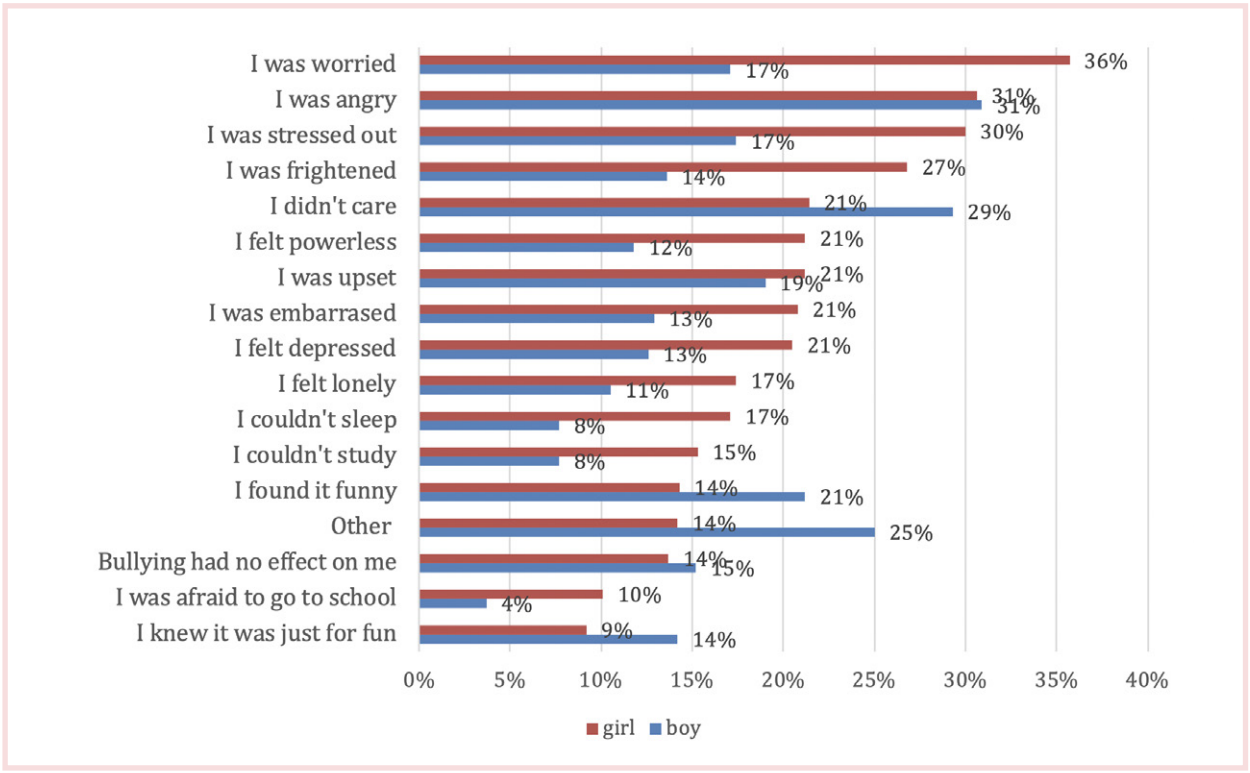
According to the study, girls are more often the victims of cyberharassment and they feel more vulnerable. Compared to boys they are more worried, stressed out, frightened, powerless, upset, embarrassed and depressed. Boys mainly see cyberharassment as a form of fun, or they just don’t care about it.

Figure 3: Forms of cyberharassment (boys and girls 12–19 years old)



Source: Cybervaw 2018

Figure 4: Feelings because of cyberharassment (boys and girls 12–19 years old)



Source: Cybervaw 2018

A similar finding was found by a survey on online harassment conducted by the Pew Research Center (July 2017), which "reveals that while men are somewhat more likely to experience any form of online harassment, women report higher levels of emotional stress from their experiences and differ in their attitudes toward the underlying causes of such incidents."

Existing interventions

The majority of interventions are aimed at raising awareness against cyberbullying, less for cyberviolence against woman and girls.

As Faith and Fraser point out, school-based interventions have the potential to take primary prevention of cyber VAWG to scale, by reaching large numbers of young people at a time when norms around gender and online violence are being shaped. Although systematic reviews have observed an increase in knowledge and decreases in risky behaviour, there are limited studies looking at long-term sustainability of changes, and most studies are based in the US or Canada. There is a need for school-based prevention programming around cyber safety to better integrate gender. (UKaid, 2018)

School-based interventions aim to prevent cyberviolence by using schools as an entry point for preventing different forms of bullying, abuse and harassment of women and girls online. Schools have huge potential to take primary prevention to scale by reaching a large number of students, teachers and parents in a teaching-learning environment. Schools are also uniquely placed to influence and shape young people's understanding of what sort of behaviour is acceptable online, at a time when young people are having their first experiences of online abuse and when unequal gender norms and attitudes around violence intensify (Chandra-Mouli et al, 2017).

Childnet international Step Up, Speak Up!

Teaching Toolkit

The Step Up, Speak Up! Teaching Toolkit is a practical, interactive and scenario-based resource which addresses the issue of online sexual harassment amongst 13–17 year olds. This toolkit is comprised of 4 lesson plans with accompanying films, an audio story, workshops and an assembly presentation.

Lesson plans: https://www.childnet.com/ufiles/Lesson_Plans_All_Step_Up_Speak_Up.pdf

deSHAME webinar (in Danish): https://www.youtube.com/watch?v=irFPbDDMhYo

Serious games

Conectado

Conectado is a serious videogame designed and developed to raise awareness around bullying and cyberbullying among young people, from 12 to 17 years old. This video game has been conceived as a tool to motivate a teacher-led classroom discussion once students have acquired a common experience of cyberbullying after playing the game.

Conectado is a graphic adventure where the player puts himself in the situation of a person who suffers bullying on a daily basis in his or her school. In this virtual world, the player lives through 5 days where he or she has to start at a new high school and make friends. Over the course of the days, the teammates he or she knows will turn their backs on him or her and interfere with him, both in person and through social networks. In this way, the player, experiences what it means to be a victim of bullying and cyberbullying in a safe way. The video game reflects the most common aggressions such as social exclusion, insults, nicknames, publication of images retouched to humiliate and laugh at a person, offensive messages, theft of passwords, blackmail, and so on. This is intended to increase the empathy of the players towards the victims, as well as to make them reflect on the final consequences of some of these acts by increasing their awareness.

The video game allows working with feelings and empathy and confronts the student with feelings such as helplessness, inferiority, frustration and loneliness through several mini-games in the form of nightmares. In these mini-games the player is incapable of increasing those feelings. In addition, through the numerous dialogues of the game, the player can respond in different ways to decrease the confrontation but never reaches a complete solution of the problem until the end of the game (nor responding violently). In this way the player becomes aware that the way to combat bullying and cyberbullying is to ask for help. The main idea is that cyberbullying is a serious social problem that cannot be solved by the player alone.

Conectado has been designed and developed with the teacher's use in class in mind. It has a duration of about 40 minutes, also in order to incorporate a small discussion guided by the tutor or teacher on the experience that the players experience through the videogame. The most common experience lived by the students allows the teacher to carry out a reflection session where the students talk and discuss the situation experienced through the video game (and in which the educator can spark discussions about whether any of these situations occur at the school and how their students experience it). Some of the interactions with the characters, as well as with the social network or mobile phone present within the game are simplified, being limited representations of the real systems.

Detailed description of the game: https://pubman.e-ucm.es/drafts/e-UCM_draft_333.pdf

Website: https://www.e-ucm.es/portfolio-item/conectado/

Friendly ATTAC
(Adaptive Technological Tools Against Cyberbullying)

Friendly ATTAC (Adaptive Technological Tools Against Cyberbullying) is a four-year (February 2012-February 2016), interdisciplinary research project funded by IWT (Agency for Innovation by Science and Technology). The project examines how technological means can be used in health interventions on cyberbullying among young people.

Given the limited number of intervention programmes available to address bystander behaviour and the importance of bystanders in ending or lessening cyberbullying's harm, the Friendly ATTAC aimed to design an intervention to increase positive bystander behaviour and decrease negative bystander behaviour in cyberbullying among young adolescents. The programme design was based on behaviour change theories and evidence specifically relating to bystander behaviour in cyberbullying. A serious game intervention was designed to promote positive bystander behaviour and reduce negative bystander behaviour.

Demo: https://www.youtube.com/watch?v=pUl9MAkSvSI

The aim of this study was to evaluate the efficacy of a digital serious game intervention component that targeted an increase in positive bystander behaviour and reduction in negative bystander behaviour, on: 1) bystander behavioural determinants; 2) bystander behaviour in cyberbullying incidents; 3) cyberbullying perpetration and victimisation; and on 4) youngsters' mental well-being.

Findings and practical implications of the intervention (source: DeSmet et al. 2018)
This intervention was a very brief, stand-alone game intervention that was intended as part of a whole-school approach but was evaluated as one component. Previous cyberbullying interventions have shown that the key to success can be close teacher involvement (Menesini et al., 2012, Palladino et al., 2012), and using an intensive programme of longer duration (Schultze-Krumbholz et al., 2016). Effects of this brief serious game can thus be expected to increase when integrated in a 'whole-school' programme rather than when using as a single component. This intervention was an individual component and the interactions with peers, parents and teachers provided in whole-school programmes can be expected to also change environmental influences in bystander behaviour, such as a class's moral norms (DeSmet et al., 2016a), appropriate teachers' interventions against cyberbullying (DeSmet et al., 2015), and parental involvement in online behaviour and their relationship with the adolescent (Cross et al., 2015).

FearNot

FearNot! is an interactive drama/video game that teaches children strategies to prevent bullying and social exclusion. It originates from the EU funded research projects Victec and eCircus. The software uses innovative psychology inspired character AI. (https://sourceforge.net/projects/fearnot/)

Online Pestkoppenstoppen
(Stop Bullies Online/Stop Online Bullies)

This intervention aims to reduce the number of cyberbullying victims and their symptoms of depression and anxiety (programme goal), by teaching cyberbullying victims how to cope in an adequate and effective manner with cyberbully incidents (programme's outcomes).

The Online Pestkoppenstoppenprogramme seems to be a promising start in solving current cyberbullying problems. The results of the evaluation studies may contribute to the knowledge about how to stop online victimisation and how to use tailoring and web-based interventions in this purpose. Additionally, this intervention may also affect offline victimisation, because despite their differences, cyberbullying and traditional bullying also have some overlapping characteristics .The results can be used as input for other web-based and computer-tailored interventions aimed at cyberbullying victims. If the studies point out that the intervention is effective in its purpose, we have an intervention ready for implementation on a larger scale.

Detailed description of the development and evaluation of the intervention: https://bmcpublichealth.biomedcentral.com/articles/10.1186/1471-2458-14-396

Support and Prevention

There are powerful international human rights frameworks which could be used to prevent cyber VAWG, even though they pre-date the growth of the Internet, such as the Convention on the Elimination of All Forms of Discrimination against Women, the Declaration on the Elimination of Violence against Women, and the Beijing Declaration and Platform for Action. In addition, there have been various UN resolutions recognising cyber VAWG in the international human rights framework on women's rights and violence against women, as noted by the Special VAWG Helpdesk Research Report No. 212 2 Rapporteur on Violence against Women, Ms. Dubravka Šimonović (Human Rights Council, 2018)

However, the effectiveness of international human rights frameworks and laws is constrained by gaps in specialised national legislative and policy measures, mechanisms, procedures and expertise/skills. Even in relatively well-resourced contexts like the UK there are challenges to the police effectively using the right approaches/digital tools.

http://www.sddirect.org.uk/media/1646/vawg-helpdesk-report-212-what-works-cybervawg.pdf

The outcome of the EU survey points out that "EU and Member State policies and national action plans to combat violence against women must be developed on the basis of evidence that draws directly from women's experiences of violence. Data on women's experiences of violence should be collected in addition to administrative and criminal justice data, which do not capture the majority of unreported victimisation. (Source: Violence against women: an EU-wide survey, European Union Agency for Fundamental Rights, 2014, page 168)

Jacobs, Goossens, Dehue, Völlink & Lechner (2015) had focus groups with young respondents, asking them about their **coping mechanisms** and received a wide variety of aggressive coping responses from participants. The most often used and discussed aggressive coping strategy was retaliation, the most often discussed passive coping strategy was doing nothing or ignoring the cyberbullying. Another way of doing nothing that was mentioned was sending the word "OK". Respondents, who were also victims mentioned several strategies that can be considered as active coping; blocking and deleting; standing up for oneself (sometimes the adolescents also stood up for someone else) and talking about the event. One girl mentioned that seeming self-assured is a good strategy to use. A lot of victims considered seeking social support as a good strategy to use. They mentioned support in general, but also specified their source of support (e.g., parents, teachers, siblings/family, and friends). When talking about parents as a source of support, respondents weren't sure; some received help from them, others didn't. Girls mentioned that they turned to their friends for help. Teachers were mentioned but talking to teachers was not always perceived as useful. Other sources of support mentioned were siblings (i.e., brothers and sisters) or family (i.e., aunts, nephews).

Völlink, Bolman, Dehue & Jacobs (2013) researched the use of **emotion-focused coping** to deal with cyberbullying and how it negatively impacts mental and physical health. Their findings emphasise the need for the children to learn problem-focused coping strategies and prevent them from using emotion-focused strategies. They additionally looked into coping mechanisms of victims of cyberbullying; how they use them in daily life, in cyber settings, how it affects depressive feelings and health complaints. Findings show that coping through emotional expression, avoidance and depressive coping in daily life also meant cyber-specific depressive coping when the victims were cyberbullied. This was linked to depressive feelings and/or health complaints.

Livingstone et al.'s (2011) study involving children aged 9–16 years old in 25 different countries found that 77% of the cyber victims **had talked to someone** about their experience; 52 % told a friend, 13% told a sibling, 42% talked to a parent, 8% to another adult they trust and 7% told a teacher.

Paul, Smith & Blumberg (2010) developed **Quality Circle**. Participants had to create an anti-bullying taskforce and, with guidance, go through problem-solving exercises over a limited/short/longer period of time. The process involved identifying key issues, analysing problems and generating solutions in a series of themed workshops. Their workshops spanned over 12 weeks: Week 1: Introduction and Discussion (information session and recorded discussion about bullying and cyberbullying). Week 2: Problem Identification (Students collect information from a range of sources by conducting a whole school survey). Week 3: Problem Analysis (students develop thought shower of initial ideas for the possible solutions). Week 4: Solution Formation (students complete a school opinion poll and collect votes for their ideas). Week 5: Presentation Preparation (students prepare a group video for senior teaching staff to view). Week 6: Presentation Delivery (students hear the panel decision to reject, consider or approve their project idea). Week 7: Project Planning (all members of the group collaborate on the project as a combined effort). Week 8: Project Preparation (group organises practical aspects, develops resources, and designs materials). Week 9: Project Delivery

(group undertakes initial stages of project idea and completes ongoing work). Week 10: Project Assessment (group reviews progress on project, compiles information gained and analyses problems). Week 11: Class Presentation (group prepares a script about project work to deliver to student peers during lessons). Week 12: Presentation Delivery (complete class presentation, group debrief and evaluation of participation in Quality Circles).

Projects that were proposed by groups were as follows (Paul, Smith & Blumberg, 2010: 161–162): creating private rooms for victims, bullies and parents, designing a mail box for students to report problems, organising a new lunch time queue system in the canteen; creating a verbal bullying dictionary, setting up IT support for students to pass on emails of cyberbullying; conducting a survey on prank calling; establishing a friendship themed film club and conducting an undercover report about cyberbullying. Collectively, they decided on: security spot checks, bag searches and handheld metal detectors, they proposed scanning the classrooms for Bluetooth devices, free phone number for offensive text messages to be passed on, school assemblies, after school activities for bullies and victims together, safe places for vulnerable students. In interviews, students emphasised the prevalence of verbal bullying – they have verbal matches that are not perceived as bullying behaviour. What was perceived as wrong was hacking into and misusing personal accounts on the computer or mobile phone. Again, general attitude towards cyberbullying was dismissive, it was not generally regarded as bullying, more of a nuisance, as was "prank calling". Sending video and picture content was perceived as entertainment and was frequently reported (Paul, Smith & Blumberg, 2010: 162–163).

Marczak & and Coyne (2010) discussed **good practices to prevent cyberbullying** and pinpointed five key areas that should be tackled in their opinion: First, understanding and talking about cyberbullying: the whole school community needs to be aware of the impact of cyberbullying and the ways in which it differs from other forms of bullying (young people and their parents' awareness of pupils' responsibilities in their use of ICT, and what the sanctions are for misuse). Secondly, schools should update existing policies and practices: review and update the school's anti-bullying policy plus other relevant policies and should keep good records of any incidents of cyberbullying and be able to conduct searches of Internet use records at school (disincentive for bullies to misuse school equipment and systems). Thirdly, schools should be making the reporting of cyberbullying easier (peer reporting, anonymous reporting, and provision of information about contacting service providers directly). Also, schools should be promoting the positive use of technology: engaging, positive and effective learning - netiquette, e-safety and digital literacy. Lastly, schools should be evaluating the impact of prevention activities.

NCGM study, conducted in seven EU countries showed that almost one third of participating youngsters decided upon a proactive coping strategy - the child attempting to solve the problem on his/her own (31 %). This was followed by the more fatalistic strategy – almost a quarter of children who had been bullied hoped the problem would go away by itself (24 %). A previous study, EU Kids Online, conducted in 25 EU states, has shown that most bullied children (four in five or 77 %) talked to somebody about it. Results of NCGM show that younger children are more likely to talk to their parents, and that both girls and boys are most likely to seek support from mothers (65% and 52 %). This parental support was shown to decrease with age - teenagers reported seeking support from a parent, but they also sought support from their peers. Less than a tenth of respondents or 7 % of children mentioned a teacher as a likely source of support with, younger children saying it is more likely they would talk to a teacher (O'Neill in Dinh, 2015: 394). These results, which show aggregated results of all seven countries are not surprisingly similar to the Irish sample, in which most young people reported talking to somebody about having been bullied online (71 %); in nearly half of the cases (42 %), that was a friend, followed by one of their parents (36 %), but only very few (just 6 %) spoke to a teacher about what had happened (O'Neill, Dinh, 2013).

Mascheroni and Cuman (2014) reveal some coping behaviours of respondents in the final report of NCGM; they assess that coping behaviours and preventive measures are strongly interconnected, because respondents aimed at avoiding a re-occurrence or an escalation. Five strategies were revealed: a) self-reliant strategies, that involved avoidance, self-monitoring- those were used mostly with location-tracking functions and when dealing with privacy issues and excessive use; b) other reliant strategies respondents used when they received nasty or sexual messages; c) technical measures require some skill to operate device or service; d) confrontation meaning personal confrontations or online or face-to-face discussions; mainly used to clarify misunderstandings and to avoid escalation; e) collective approaches – respondents reported that they used social support as an emotional support or technical assistance when dealing with bullying and lastly f) disengagements – sometimes youngsters reported just being disengaged with any preventive or reactive measure, mostly because they see other methods as ineffective; they reported not engaging adults because they will not be interested, they will not take it seriously, they would get angry or reprimand/punish them (Mascheroni and Cuman, 2014: 37).

A Canadian report points out that "trying to prevent abuse and harassment related to technology can feel like a game of "whack-a-mole" where trying to anticipate and react to sexual violence in the context of the next technological

trend to "pop up" is overwhelming and not productive as a long term strategy". They identify a number of strategies for the prevention of violence through social media, mainly focusing on education as an over-arching approach. Education and awareness campaigns should promote community awareness of consent and the applicability of consent to actions done through social media as well as challenging notions of victim-blaming and shaming of girls and women. Another aspect that should be addressed in community education and awareness programmes is challenging rape culture and toxic masculinity. Through rape culture, "boys are taught that they don't prove their masculinity through their appreciation for women, but through their callous conquering of them. Rape becomes a method to assert masculinity, and sharing the photo of your triumph becomes a way to document your place in the social order. (West J., Cyberviolence against women, 2014)

Furthermore, the research shows that men and women also differ on how best to prevent and manage online harassment. Men are somewhat more likely than women to believe that improved policies and tools from online companies are the most effective approach to addressing online harassment (39 % vs. 31 %), while women are more likely to favour stronger laws (36 % vs. 24 %). In addition, women are more likely than men to say that law enforcement currently does not take online harassment incidents seriously enough (46 % vs. 39 %) (http://www.pewresearch.org/fact-tank/2017/07/14/men-women-experience-and-view-online-harassment-differently/).

The United Nations Broadband Commission published the report "Combatting Online Violence Against Women & Girls: A Worldwide Wake-Up Call" in 2015, which revealed that almost three quarters of women online have been exposed to some form of cyberviolence, and urged governments and industries to work harder and more effectively together to better protect the growing number of women and girls who are victims of online threats and harassment

Key findings of the paper include:

- Women in the age range of 18 to 24 are likely to experience stalking and sexual harassment in addition to physical threats.
- One in five female Internet users live in countries where harassment and abuse of women online is extremely unlikely to be punished.
- In many countries women are reluctant to report their victimisation for fear of social repercussions.

Key Recommendations, proposing a global framework based around three 'S's – Sensitisation, Safeguards and Sanctions.

Sensitisation – Preventing cyber VAWG through training, learning, campaigning and community development to promote changes in social attitudes and behaviour.

Safeguards – Implementing oversight and maintaining a responsible Internet infrastructure through technical solutions and more informed customer care practices

Sanctions – Develop and uphold laws, regulations and governance mechanisms to deter perpetrators from committing these acts (http://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release).

Their further important recommendation is researching women's access to and use of the Internet: The Working Group calls on stakeholders to research women's access to and use of the Internet to improve understanding of the needs, circumstances, and preferences of women in different local contexts, and the factors limiting women's access to and use of the Internet, including cultural and social norms. This is critical in enabling effective and appropriately focused policy and strategies which address women's needs, priorities, and preferences in the diverse local contexts in which they live.

Source: http://broadbandcommission.org/Documents/publications/WorkingGroupDigitalGenderDivide-report2017.pdf

Existing interventions to prevent/raise awareness about cyberviolence in partner countries

Estonia

Web Constables

Since 2011, Estonian police has Web Constables. Currently (2019) there are three Web Constables in the Estonian Police and Border Guard Board. They are working in Estonian, and if needed, in Russian and English, in web environments which are most-used and foremost, primarily attractive to young people. In addition, they conduct knowledge raising actions in real life on Internet safety and other crime prevention issues. Web Constables are the main spokespersons on online safety and dangers relating to the use of digital devices in a web-environment and also by conducting trainings regarding safer use of Internet and digital devices.

More in Estonian at:
https://www.politsei.ee/et/juhend/ennetusalased-materjalid/kuberturvalisus
https://www.politsei.ee/et/juhend/taga-enda-ja-oma-laste-turvalisus/digiturvalisus

Smartly on the Web (Targaltinternetis)

https://www.targaltinternetis.ee/en/

Vihjeliin.ee

'Vihjeliin' (www.vihjeliin.ee) is a free online service of the Estonian Union for Child Welfare which enables Internet users to provide information about material being distributed online which depicts illegal content – the sexual abuse or exploitation of minors and child trafficking. Information can be submitted anonymously; your personal details are not investigated or recorded. Vihjeliin was opened in February 2011.

The Estonian Union for Child Welfare works closely with other national organisations, including law enforcement authorities, Internet service providers and non-profit organisations, and international networks such as INSAFE and INHOPE.

The child helpline service

The child helpline service was launched on 1st January 2009 using the nationwide free of charge round the clock operational helpline number 116 111. The objective of the service is to enable everybody to report about a child in need, forward the information to respective specialists and to offer children and other people primary social counselling and crisis counselling, if necessary. The service is provided in accordance with the Republic of Estonia Child Protection Act § 59, according to which every person is required to immediately notify the social services departments, police or some other body providing assistance if the person knows of a child who is in need of protection or assistance.

Recommendations for celebrating the Safer Internet Day (SID) on 5 February.

Soovitusi 2019. aastaturvaliseinternetipäevatähistamiseks, https://media.voog.com/0000/0034/3577/files/Soovitusi%202019%20turvalise%20interneti%20päeva%20tähistamiseks%20.pdf

Manual for young people, teachers and parents

about cyberbullying published in the framework of the Daphne project 'Peer support and youth participation in bullying prevention' (More in Annex 1). In 13 pilot schools, the project coordinated a comprehensive process where students, school staff and parents were engaged to adopt and update practices and structures for bullying prevention in their school. The participants from schools expanded their knowledge about bullying, cyberbullying and means to promote peer support and active bystander behaviour to prevent bullying. Teachers gained new pedagogical skills to promote inclusion and positive group behaviour in class. Schools built operational structures for peer supporters and other types of student engagement. Students improved their problem-solving, communication, and social skills, and became active participants in bullying prevention in their school.

Project manual in Estonian: Küberkius. Abimaterjalnoortele, õpetajatele, lapsevanematele (Cyber bullying: Manual for young people, teachers and parents) (2017). http://www.tore.ee/files/Kyberkiusamine_Materjal_2017.pdf

Greece

■ https://saferinternet4kids.gr/

The Institute of Technology and Research (ITE), has been promoting their campaign since 2018, for the education and awareness of young people and their families to cyberviolence, but the data used in the campaign is completely gender neutral. In addition, there is no mention of cyberviolence throughout their campaign, which leads to the conclusion of it rather being a prevention campaign.

Erasmus programmes, such as "Cyberviolence" has been researching the effects of cyber abuse, more specifically cyberbullying, on young children. As it states on their web page "The main problem that we will deal with during the project is the lack of knowledge and awareness about the problem of cyberbullying among young people, youth workers, teachers and parents. Among the youth, the problem is the lack of awareness of online threats, the lack of opportunities and the ability to respond to cyberbullying. Among the youth workers and teachers the problem is the lack of tools and methodologies for working with this topic, education and prevention. Among parents, there is no awareness of the problem and the ability to recognise the first signs of being a victim of cyberbullying".

There is also an electronic Serious Game developed for children, to bring them in touch with the subject of cyberbullying. Therefore, Cyber Violence Project investigates the subject in young children, but does not distinguish the gender role. It clarifies however the need to take all necessary precautions for the prevention of cyber-crimes.

The Department of Greek Police for Electronic crimes has been watching the subject closely, organising and carrying out events targeted at various parts of society, including schools, teachers and parents.

Awareness campaigns from NGOs and state authorities have proved effective over the last years, keeping parents and teachers alert for any signs of cyberbullying or abuse.

Northern Ireland

■ **NSPCC PANTS campaign and resources –**
https://learning.nspcc.org.uk/research-resources/schools/pants-teaching/?_ga=2.36688736.1776410372.1569571758-1854804115.1569571758

■ **NSPCC Share Aware campaign and resources –**
https://learning.nspcc.org.uk/research-resources/schools/share-aware-teaching/

■ **Net Aware –**
https://www.net-aware.org.uk/

■ **UK Safer Internet Centre – Safer Internet Day –**
https://www.saferinternet.org.uk/safer-internet-day/2019

■ **Alliance 4 Choice #BackOnTheBill campaign –**
http://www.alliance4choice.com/repeal-58/59/2019/4/make-sure-northern-ireland-isnt-left-behind-again-backonthebill

■ **CEOP (Child Exploitation and Online Protection Centre) –**
https://www.ceop.police.uk/safety-centre/

■ **Nexus NI schools interventions**

- PCSP Belfast Talking About Consent
- PCSP Belfast Cybersafety
- ARN Rural Education Omagh and Fermangh
- Peace IV Derry and Strabane Media Influence
- Derry and Strabane PCSP Consent Education
- Mid-East Antrim PCSP Cybersafety and Consent
- Digi Pal PCSP Causeway Coast and Glens
- RSE Derry

Italy

■ **National Plan to prevent bullying and cyberbullying at school (MIUR (Italian Ministry of Education)) –** http://www.cnos-fap.it/sites/default/files/rapporti/piano_azioni_definitivo.pdf

Within the aforementioned plan:

■ **Generazioniconnesse. Safer Internet Centre –** https://www.generazioniconnesse.it/site/it/cyberbullismo-scuole/; MIUR (Italian Ministry of Education) programme on cyberbullying, co-financed by the European Union

■ **Gender School –** http://www.indire.it/progetto/gender-school/

National plan for education and training on issues concerning both civil and pedagogical opposition to gender-based violence, pursuing these goals through the training of school staff and teachers and through the inclusion of a gender approach in educational practice and teaching. The plan was developed by Indire (Education Innovation Centre) and the Ministry of equal opportunities).

■ **CyberViolence – a project against violence in the network –** http://www.cyberviolence.eu/?fbclid=IwAR0oAPYSPNk0aM-mv73w56Gwn7BwjQbem9Tw6o9aCaBGT-d32z9wRvmXkL6U

Slovenia

■ **Project CYBERVAW –** http://odklikni.enakostspolov.si/o-projektu/ – there are several activities (interventions) to educate about cyber vawg – awareness raising and prevention. The activities are mainly held in the form of workshops. There are several target groups for whom the workshops were organised:

- police,
- justice,
- youth workers
- primary school pupils
- secondary school students.

More than 100 workshops have already been conducted for primary and secondary school students, and there is a huge interest and need for more. The workshops for primary and secondary school students are divided into several sections and cover the following topics:

SECTION 1: INTRODUCTION AND COOPERATION AGREEMENT: a brief presentation of the topic and the establishment of a safe and confidential environment within a group of young people and in relation to the person who carries out the workshop

SECTION 2: VIOLENCE: general definition of what violence is and who decides on what violence is

SECTION 3: CYBER VIOLENCE: Definition of the concept of online violence, its forms and consequences

SECTION 4: GENDER-BASED CYBER VIOLENCE AND GENDER-BASED STEREOTYPES – definition of the forms and causes of gender-based cyberviolence

SECTION 5: PARTICIPANTS IN CYBER VIOLENCE (VICTIM, OBSERVER, PERPETRATOR) – defining those involved in gender-based cyberviolence and their roles

SECTION6: ACTION, KNOWLEDGE FOR HANDBOOK - empowering young people for ethical and empathetic behaviour in cases of gender-based cyberviolence and the preparation of their own code of ethics.

Legislation

Criminalisation of cyberviolence
While most states have legislation criminalising conduct related to online sexual exploitation and the abuse of children, the criminalisation of other forms of cyberviolence such as cyberbullying, harassment, sextortion and others is a more recent development. Some laws include liability of service providers. Most states seem to apply regular criminal law and other provisions.

Legislation in partner countries

In **Estonia**, according to the Penal Code offences are criminal offences and misdemeanours. The word "cyber" is not used in the Penal Code. Criminal liability starts at the age of 14. A person is capable of guilt if, at the time of commission of the act, he or she is mentally capable and at least fourteen years of age (Article 33 of the Penal Code).

- Lastekaitseseadus (Child Protection Act), RT I, 12.12.2018, 49, https://www.riigiteataja.ee/en/eli/511012019009/consolide
- Isikuandmetekaitseseadus (Personal Data Protection Act), RT I, 04.01.2019, 11, https://www.riigiteataja.ee/en/eli/523012019001/consolide
- Karistusseadustik (Penal Code), RT I, 19.03.2019, 30, https://www.riigiteataja.ee/en/eli/516052019002/consolide
- Pornograafilisesisuga ja vägivaldavõijulmustpropageerivateteostelevikureguleerimiseseadus (Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty), RT I, 12.07.2014, 106, https://www.riigiteataja.ee/en/eli/520012015009/consolide
- Reklaamiseadus (Advertising Act), RT I, 12.12.2018, 6, https://www.riigiteataja.ee/en/eli/524012019003/consolide

In **Greece** the existing legislation that is in effect regarding crimes of cyberviolence comes under the law that was ratified in Greece in 2018 under the "Council of Europe Convention on preventing and combating violence against women and domestic violence Istanbul, 11.V. 2011". It clearly states and condemns any violation of human rights, but more specifically any form of violence against women as well as domestic abuse. It identifies the need of implementing equality with the aim of preventing violence against women.

Clarifying the subject of cyber abuse, in relation to violence against women, there was a modification which states that everyone, with no threat of violence or of any other illegal act, or lack of it, causes terror or anxiety to another individual by stalking or following them, especially by the pursuit of constant contact through any telecommunication or electronic media or by repeated visits of their family, social or working environment, despite and against their expressed will, will be punished with imprisonment.

The Greek Cybercrime Centre (GCC) is part of an emerging coordinated European effort which has the capacity to significantly improve education and research in the newly growing area of cybercrime. As a national project, GCC seamlessly complements transnational projects such as 2CENTRE (The Cybercrime Centres of Excellence Network), and B-CCENTRE.

As per legislation on gender-based violence, two crucial points should be mentioned. On the one hand, in 2018, Greece ratified by national law the Council of Europe's Istanbul Convention on preventing and combating violence against women and domestic violence. Introducing amendments to the existing legal framework [like the existing law on domestic violence and the Greek Penal Code), the new law underlines the obligation of the state to fully address gender-based violence in all its forms and to take measures to prevent violence against women, protect its victims and prosecute the perpetrators. The Convention also emphasises the prevention of gender-based violence through specialised education and awareness programmes and specialised measures are envisaged to protect women-victims of violence in order to prevent their secondary victimisation, to protect children witnesses of abuse and to establish a mechanism for the monitoring of its implementation.

In **Northern Ireland**, the following acts and orders are in use:

- Sexual Offences (NI) Order 2008
- Criminal Law Act 1987
- Protection from Harassment Order 1997
- Malicious Communications Order (NI) 1988
- Communications Act 2003
- The Education and Libraries (NI) Order 2003

In **the UK** it became a criminal offence with a maximum of two years of imprisonment to share private sexual photographs or videos without the subject's consent with the intent of causing distress to those targeted, in April 2015. In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect.

Italy adopted law no. 71/2017, entitled "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying" in May 2017. Article 1 of the law defines cyberbullying as "whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content also depicting one or more members of the minor's family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect serious abuse, a malicious attack or a widespread and organised ridicule.(Council of Europe 2018)

Also, there is a newly updated Law on Violence against women (Legge 19 luglio 2019, n. 69). This law modifies the penal code, the criminal procedure code and other provisions concerning the protection of victims of domestic and gender violence and introduces the crime often referred to as "revenge porn".

Slovenia is in the process of updating legislation to include cybercrime e.g.: Slovenian penal code (KZ-1 NPB6) addresses revenge porn (also called cyber rape) in article 143. Paragraph 6 states that any person who publishes videos or messages of another person with sexual content without the person's consent severely violating her privacy is punishable with imprisonment from 3 months to 3 years. (http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050)

In the area of sexual abuse of children, the offence follows the penal code against sexual integrity, namely:

- Sexual assault of a person under the age of 15 (paragraph 4 of Article 173),
- Acquisition of persons under the age of 15 for sexual purposes (Article 173a), and
- Display, production, possession and transmission of pornographic material (Article 176).
- The following offenses can also be punished according to the Slovenian penal code:
- Stalking (under Article 134a of KZ-1),
- Unjustified imaging (under Article 138 of the KZ-1),
- Misuse of personal data (paragraph 6 of Article 143 of the CC-1) when someone publicly publishes recordings or messages of another person with sexual content without the consent of that person and thus seriously affects his or her privacy;
- Blackmail (under Article 213 of the CC-1) and other crimes.

Legislation in other EU countries

Netherlands

The Dutch Department of Security and Justice published a first report on a national cyber security strategy (NCSS) on 29 February 2011.[3] Part of the strategy was the establishment of a Cyber Security Council (CSC) with representatives of relevant parties in the public and private sector in order to elaborate and evaluate the NCSS. A second aim was

3 https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2 (text in Dutch only).

the establishment of the National Cyber Security Center (NCSC) which officially started to function from 12 January 2012.[4] The task of the NCSC is defining the measures and instruments required in view of implementing the NCCS and serving as a centre of expertise. Its views were published on 28 October 2013.[5] The NCSC is part of the organization of the National Coordinator Fighting Terrorism and Security of the Department of Security and Justice[6]. Fighting cybercrime is an essential aspect of the NCSS.

Relevant for cybercrime, is the criminalisation of stalking in Article 285b DCC. This is defined as the unlawful systematic violation of another person's privacy (persoonlijkelevenssfeer) with the objective of forcing that person to do, not to do, or to tolerate something or of intimidating him/her; it carries a maximum penalty of three years' imprisonment. Few court cases have been published concerning cyberstalking as such; most stalking cases in practice comprise combinations of physical and electronic means of harassment. The Supreme Court has hinted that repeatedly making obscene phone calls to someone might constitute stalking. A lower court considered that posting threatening messages on a fan website of a famous person could not be considered stalking, since the time of posting – two days – was too brief for the behaviour to be considered systematic. Sending loads of email, SMS, and Hyves messages for months or years, however, is a clear case of stalking. Various courts have also punished the placing of announcements on dating websites purporting to be from another person, thus causing this person to receive email responses, as stalking. Similarly, creating a profile page with pictures of someone else on the social networking site Hyves – in combination with other harassing activities – can also be considered stalking. Somewhat related to cybercrime are the offences of secretly making visual images of people. If someone uses a camera, the presence of which has not explicitly been made known, to intentionally and unlawfully make pictures of someone, he/she can be punished with up to six months' imprisonment if it concerns non-public places (Article 139f DCC) or up to two months' imprisonment if it happens in public spaces (Article 441b DCC). (https://www.ejcl.org/143/art143-10.pdf)

Denmark
In relation to violence against women, the relevant sections of the penal code are:

- section 237 homicide
- section 244 less severe violence
- section 245 more severe violence
- section 246 severe violence, generally with permanent injury to the victim
- sections 216 – 217 regarding rape.

Danish criminal law has been taking regulative measures against stalking since 2012. The Danish Law on Gender Equality regulates sexual harassment: section 1 (6). By this act, sexual harassment is defined as follows:

It is sexual harassment when anyone is exposed to non-consenting (unwanted) verbal, non-verbal or physical conduct with sexual undertones with the purpose or effect of harming/violating the person's dignity – especially by creating a threatening, debasing, hostile, humiliating or unpleasant climate.

Best practice in VAWG legislation

VAWG legislation varies greatly in scope and applicability. The most effective characteristics and types of legislation for protecting women and girls from violence:

- Cover the main forms of VAWG (physical, sexual, emotional and economic violence) as well as types of violence, including sexual harassment in employment, education and public places, and violence within the family and interpersonal relationships;
- Specifically identify women as beneficiaries of the legislation;
- Provide for coordinated care and support services by promoting the role of various sectors;

4 https://www.ncsc.nl
5 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html
6 https://www.ncsc.nl

- Explicitly prohibit mediation;

- Clarify the relationship between customary and/or religious law and the formal justice system and codify the survivor's right to be treated in accordance with human rights and gender equality standards under both processes;

- Ensure states comply with the 'due diligence' standard in international law, which requires states to take 'reasonable' action to prevent, protect against, prosecute, punish and provide redress for violence against women; and

- Protect all women equally and does not contain provisions, and/or be applied by the justice system in a manner which discriminates between different groups of women.

Main EU conventions on gender equality, non-discrimination and violence against women mainly in relation to non-discrimination and domestic violence, or children sexploitation e.g.:

- Cybercrime Convention of 2001, (Budapest convention), Council of Europe https://www.coe.int/en/web/cybercrime/the-budapest-convention The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

- The Official Journal of the European Union published Own-initiative opinion of the Committee of the Regions on 'Priorities for regional and local authorities to prevent violence against women and improve support for victims' (2010/C 79/02): lists the following impacts of *"Economic impact of violence against women:*
  28. Draws attention to the direct and indirect economic cost of violence against women for local and regional authorities in Member States. Violence affects victims' working lives as well as their physical and mental health and social situation. It also impacts adversely the health and well-being of other members of a family who witness violence against women, particularly children and the costs of dealing with the long term health issues often falling on local and regional authorities. These indirect costs – which take their toll on goods, services and victims' well-being – go hand in hand with the direct cost of specific or general resources that are used to deal with the problem. Statistics support the use of prevention programmes as they are inexpensive in comparison with the social cost of violence;
  29. Draws attention to the effect of violence on society as a whole, noting that it is a social problem which must be tackled as a priority: violence not only has an impact on individuals, families and communities but also actually slows down the economic development of nations. …"
  http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52008IR0267&from=SL

- Regulation (EU) no 1381/2013 of the European Parliament and of the council: "Equality between women and men is one of the Union's founding values. "
  http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R1381&from=SL

- DIRECTIVE 2011/93/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography
  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093

- Convention on Elimination of All Forms of Discrimination against Women – (CEDAW UN)
  http://www.ohchr.org/en/hrbodies/cedaw/pages/cedawindex.aspx

- Istanbul Convention - Action against violence against women and domestic violence. The Council of Europe Convention on preventing and combating violence against women and domestic violence is based on the understanding that violence against women is a form of gender-based violence that is committed against women because of their sex. It is the obligation of the state to address it fully in all its forms and to take measures to prevent violence against women, protect its victims and prosecute the perpetrators. Failure to do so would make it the responsibility of the state. The convention leaves no doubt: there can be no real equality between women and men if women experience gender-based violence on a large scale and state agencies and institutions turn a blind eye.

Country monitoring work –
https://www.coe.int/en/web/istanbul-convention/country-monitoring-work:

- **Denmark:** https://rm.coe.int/16806dd217
- **Italy:** https://rm.coe.int/grevio-state-report-italy/16808e8133; https://rm.coe.int/16803060a7
- **Greece:** Upcoming
- **Netherlands:** https://rm.coe.int/netherlands-state-repot-grevio/16808d91ac
- **Slovenia:** https://rm.coe.int/grevio-inf-2019-15-eng/pdfa/1680989a54

The Budapest Convention addresses some types of cyberviolence directly through a number of substantive criminal law provisions. Other provisions address acts facilitating cyberviolence.

The procedural powers and the provisions on international cooperation of the Convention on Cybercrime will help investigate cyberviolence and secure electronic evidence. The Budapest Convention and treaties such as the Istanbul and Lanzarote Conventions complement each other.

It would seem that more could be done to emphasise such complementarity and to promote synergies between these three instruments.

In its 2016 annual report, Eurojust published that judicial cooperation in the field of cybercrime faced many distinct challenges, mostly stemming from the inherent borderless nature of this criminal phenomenon and the significant legislative differences existing on national level. Eurojust supported 60 cases, 13 coordination meetings and eight JITs, two of which were newly established. Within the framework of the EMPACT Cybercrime - Child Sexual Exploitation, Eurojust carried out an analysis of Eurojust cases of online CSE, outlining the challenges in investigations and prosecutions of CSE cases, as well as solutions and best practices (http://eurojust.europa.eu/doclibrary/corporate/Pages/annual-reports.aspx) to be private and to use for revenge purposes.

Focus groups among teenagers

One of the activities in CYBERSAFE was also the implementation focus groups (FGs) in partner countries. The methodology of the focus groups was developed beforehand, so in all countries the FGs were conducted in the same way.

Developing the comprehensive prevention model required an in-depth understanding of the state of cyber VAWG among targeted teenagers. CYBERSAFE partners carried out focus groups to identify the experiences, behavioural patterns, and causes that influence cyber VAWG among teenagers. The consultations with the key target group were vital to defining the framework of cyber VAWG applied in the project.

These FGs had three main goals:

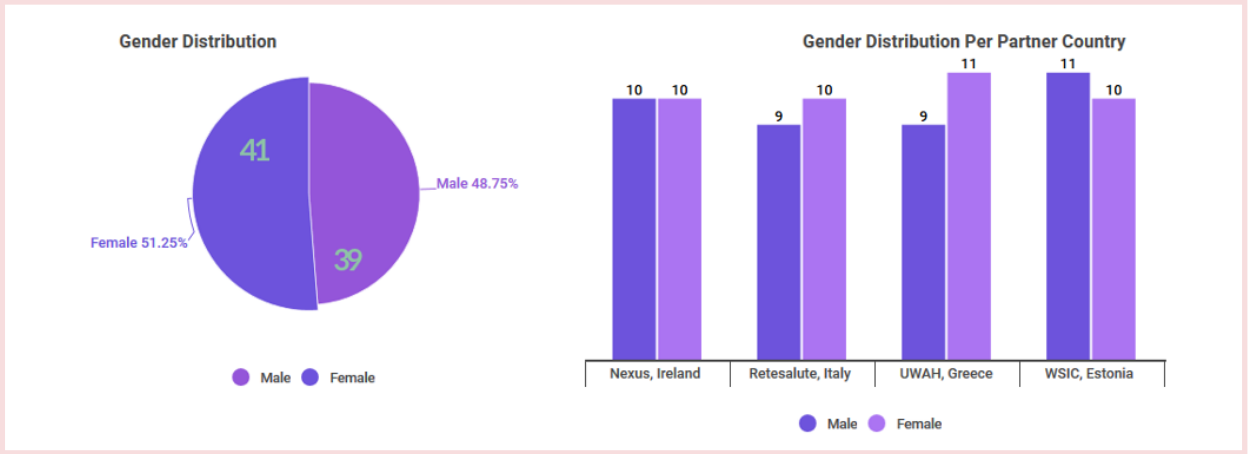
- Identifying knowledge and needs of Cyber VAWG among teenagers;
- Identifying the behavioural issues that trigger Cyber VAWG among teenagers;
- Gaining feedback on serious games concepts.

The feedback collected at the FGs is vital to identifying the framework for VAWG and providing input for developing the educational prevention programme.

The results of the FGs enable partners to set objectives for the serious online game and to define the intervention to be applied within the project.

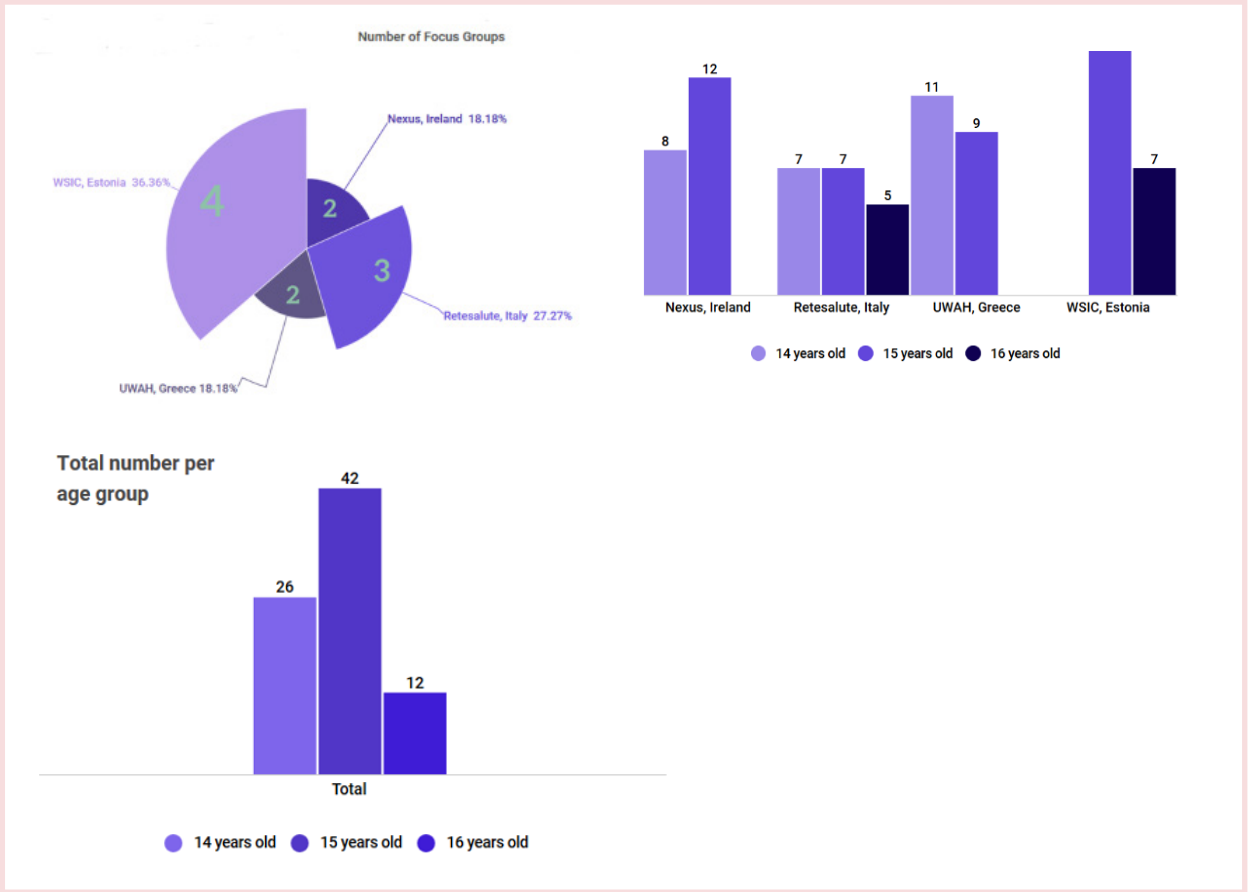
Participants Demographics

The following demographics reflect the reported information for the 80 participants in the 11FGs [7].



Summary of results of the focus groups

In May 2019, CYBERSAFE partner organisations – Azienda Speciale Retesalute (Retesalute, IT), Women's Support and Information Centre (WSIC, EE), Northern Ireland Rape Crisis Association (NEXUS NI, UK), and the Union of Women Associations of Heraklion Prefecture (UWAH, GR) - conducted 11 focus groups with 80 teenagers, respectively, in four partner countries - Italy, Estonia, UK Northern Ireland, and Greece.



7 To see the interactive figures, please visit the following link https://infogram.com/1pr9dr35gw17j2ig7pg3qjymzqamzrkny0e?live

Focus groups revealed that the majority of teenagers have already heard of or faced cyberviolence, either directed towards them or towards their peers. Consultations identified a strong sense of victim-blaming attitudes among teenagers. The consultations give valuable insight to the different underlying attitudes between male and female teenagers towards Cyber VAWG, behavioural causes, and triggers of violence. The results of initial consultations provide useful input for CYBERSAFE's educational prevention programme.

Key findings of the focus groups

- Teenagers trust people they meet online;
- They are aware they should be careful when meeting new people online;
- They agree it is important to talk to someone if cyberviolence happens (friends, family);
- They are aware of cyberviolence, although not all forms of cyberviolence are recognised as violent;
- Perpetrators are seen as weak, hiding behind the computer, because it gives them anonymity;
- Girls are more often victims of cyberviolence than boys;
- Girls are often victimised because of their looks;
- A frequent case of cyberviolence against girls is sharing intimate photos without consent;
- Partner violence online is often mentioned among teenagers (male controlling female);
- Teenagers often see perpetrators as victims (they are weak and alone, they are victims of violent behaviour);
- Teenagers agree cyberviolence happens more often to girls;
- There is a well-established pattern of victim-blaming behaviour;
- There are many gender stereotypes among teenagers which seem to be deeply rooted (girls are weak, boys are strong).

Identification of target behaviours & objectives – project framework

The purpose of the framework

In this framework we provide some theoretical and empirical background which will be used for the implementation in the CYBERSAFE project. The purpose of this framework is to define the target population of the project, to set definitions of cyberviolence against women and girls, to identify the categories of cyberharassment, which will be the basis for other Work Packages (specifically in the area of development of the educational prevention intervention in WP3). In the framework we identify the characteristics of abusive behaviour which will be tackled with educational activities of the CYBERSAFE project; as well as the behaviours which we will try to change with the developed intervention towards Cyber VAWG.

Theoretical and empirical background

Violence and discrimination against women are global social issues, where abuse is afflicted systematically, relentlessly and are often times tolerated, if not explicitly condoned. The United Nations Declaration on the Elimination of Violence against Women (GA Resolution 48/104, 20 December 1993) defines violence against women (VAW) as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."[8]

8 https://www.apc.org/sites/default/files/VAW_ICT_EN_0.pdf

In the last decade, the rise of technological advancement as a popular means of socialisation has extended gender violence to a new dimension. As a result, young women experience the digital world both as a site of empowerment and a source of sexual repression.

Studies show (E.g. FRA study (2012)) there are between 5 % and 18 % of women in the EU over 15 years of age who have already experienced cyberviolence. EIGE – The European Institute for Gender Equality (2017) notes that one in ten women older than 15 years, experience cyberviolence. This proportion is even higher among adolescents. A Slovenian survey finds that over 50 % of girls older than 13, has already experienced some form of cyberviolence. Cyberviolence victimisation is reported to be associated with depression and anti-social behaviour (Sargent et al. 2016), diminished self-esteem, fear and anxiety. Some assert that cyberviolence actually might be more damaging than in-person abuse because it has a wide audience, can be anonymous, and is insufficiently regulated.

Cyberviolence definition

When addressing cyberviolence, we are faced with a challenge, as literature review indicates a lack of consistent, standard definitions or methodologies used to conceptualise and measure cyberviolence. As also pointed out by the Council of Europe (2018) there is not yet a stable lexicon or typology of offences considered to be cyberviolence, and many of the examples of types of cyberviolence are interconnected or overlapping or consist of a combination of acts. There is a plethora of different terms, describing similar forms of violence. In this project we use the term **cyberviolence**, which includes all forms of violence/harassment/bullying that happens with the use of ICT.

In the project we propose the definition by Attrill et al (2015; 136–137), who defines cyberviolence *as accessing and distributing of injurious, hurtful or dangerous materials online to cause emotional, psychological or physical harm.* The most common form of cyberviolence is bullying and harassment. We understand cyberviolence as an umbrella term for many other forms of violence which happen with the use of ICT.

Cyberviolence against women and girls is gender-based violence that is perpetrated through electronic communication and the Internet. Although cyberviolence can affect both women and men, women and girls experience different and more traumatic forms of cyberviolence.

There are various forms of cyberviolence against women and girls, including, but not limited to, cyber stalking, non-consensual pornography (or 'revenge porn'), gender-based slurs, hate speech and harassment, 'slut-shaming', unsolicited pornography, 'sextortion', rape threats and death threats, and electronically facilitated trafficking.

Compared to boys, girls are more often victims of sexual harassment that also occurs online.

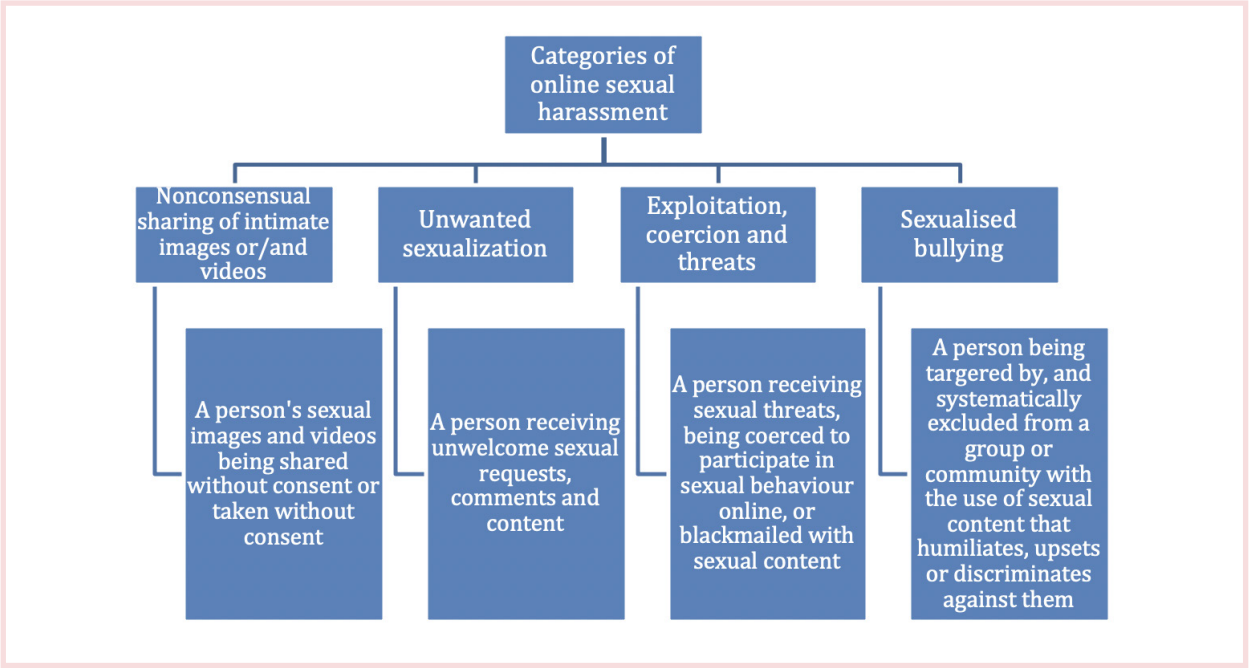
In the CYBERSAFE project we tackle gender-based cyberviolence – sexual harassment that happens to girls online.

As defined in the deSHAME project, **online sexual harassment** is any **unwanted sexual conduct** on any digital platform and is recognised as a sexual violence.

Online sexual harassment can include a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different online platforms (private or public). Victims and perpetrators can be numerous. It can make a person(s) feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against. Online sexual harassment is often focused around schools and local communities and can often play out online in front of an active, engaged audience which can add to the distress caused. Bystanders can also be affected by witnessing online sexual harassment regardless of whether they engage with it or not. Young people may or may not know the peer(s) who is committing the harassment. (However, as the research shows (Odklikni!, CYBERSAFE focus groups), victims mainly know their perpetrator's identity.

DeSHAME categorises online sexual harassment into four categories:

Picture 1: Categorization of sexual harassment



Source: deSHAME project, 2017

Characteristics of abusive behaviours

- **Non-consensual sharing of intimate images or/and videos**

  - Sexual images/videos taken without consent ('creep shots');
  - Sexual images/videos taken with consent, but shared without consent;
  - Non-consensual sexual acts (e.g. rape) recorded digitally and potentially shared.

- **Unwanted sexualisation**

  - Sexualised comments (e.g. on photos);
  - Sexualised viral campaigns that pressure people to participate;
  - Sending someone sexual content without them consenting;
  - Unwelcome sexual advances or requests for sexual favours;
  - Jokes of a sexual nature;
  - Rating peers on attractiveness/sexual activity;
  - Altering images of a person to make them sexual.

- **Exploitation, coercion and threats**

  - Harassing or pressuring someone online to share sexual images of themselves or engage in sexual behaviour online (or offline);
  - Threatening to publish sexual content (image, video, rumours) to threaten, blackmail or coerce someone (sextortion);
  - Online threats of sexual nature (e.g. rape);
  - Inciting others online to commit sexual violence;
  - Inciting someone to participate in sexual behaviour and then sharing the evidence of it;
  - Cyber dating abuse (CDA) using technology to monitor and control the actions of a partner; using a partner's password without permission to access his or her mail or social media accounts; installing tracking devices or apps to monitor a partner's location; or perpetrating emotional aggression and verbal threats through digital means during or after a relationship has ended.

- **Sexualised bullying**

  - Gossip, rumours or lies about sexual behaviour posted online;
  - Offensive/discriminatory sexual language or name calling online;
  - Impersonating someone and damaging their reputation by sharing sexual content or sexually harassing others;
  - Personal information shared non-consensually online to encourage sexual harassment (doxing);
  - Being bullied because of actual or perceived gender and/or sexual orientation;
  - Body shaming;
  - Outing someone where the individual's sexuality or gender identity is publicly announced online without their consent.

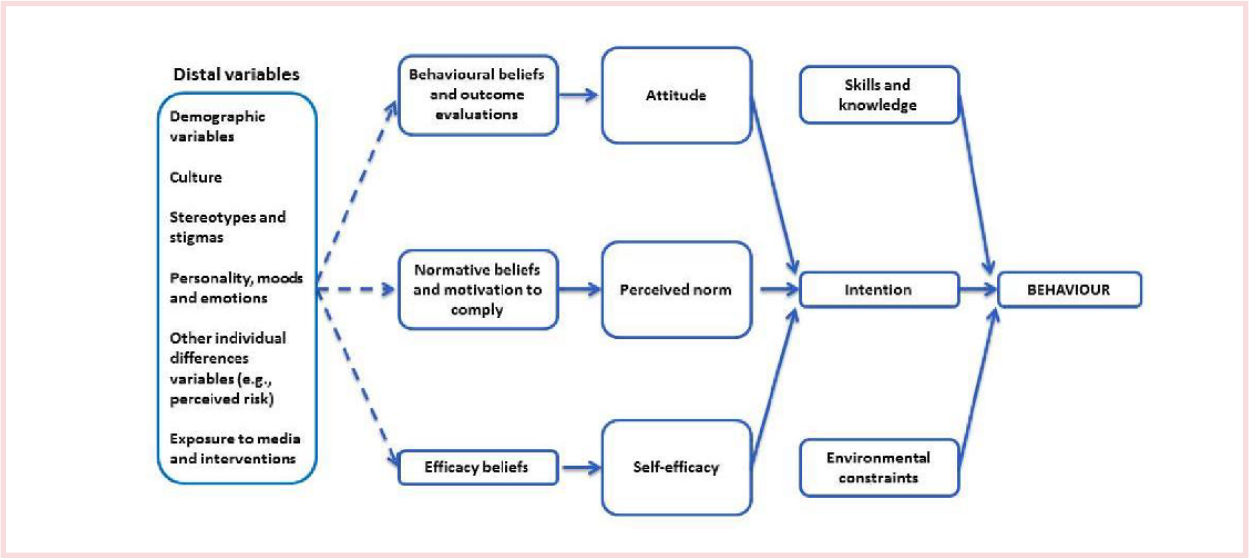
Behavioural elements and behaviour change

There are several behavioural elements connected to cyberviolence - there are behaviours related to the commitment of cyberviolence and the behaviours which can be changed with the implementation of the intervention.

The theory of planned behaviour (Ayzen, 1991) and integrative model of behavioural prediction (Fishbein and Yzer, 2003) offer frameworks, which enable us to understand the multiple layers of factors that may explain a given behaviour, such as violence against women or under-reporting among victims.[9]

The theory of planned behaviour states that a prerequisite for someone to perform a given behaviour is that this person has an intention in line with this behaviour. There are, three immediate conditions for an intention to take shape: one has to (1) hold a positive opinion towards the behaviour (i.e. **attitude**); (2) consider that this behaviour is socially acceptable (i.e. **norms**); and finally (3) believe that one is actually able to perform that behaviour (i.e. **self-efficacy**). The integrative model of behavioural prediction adds to those three factors more indirect layers of behavioural causes, such as beliefs, demographics, culture, personality and exposure to media. The model brings together a variety of factors into a single and very helpful framework of analysis that allows a thorough understanding of the very roots of violence against women.

Picture 2: An integrative model of behavioural prediction (adapted from Fishbein and Yzer, 2003)



Source: Almeida et. al. 2016

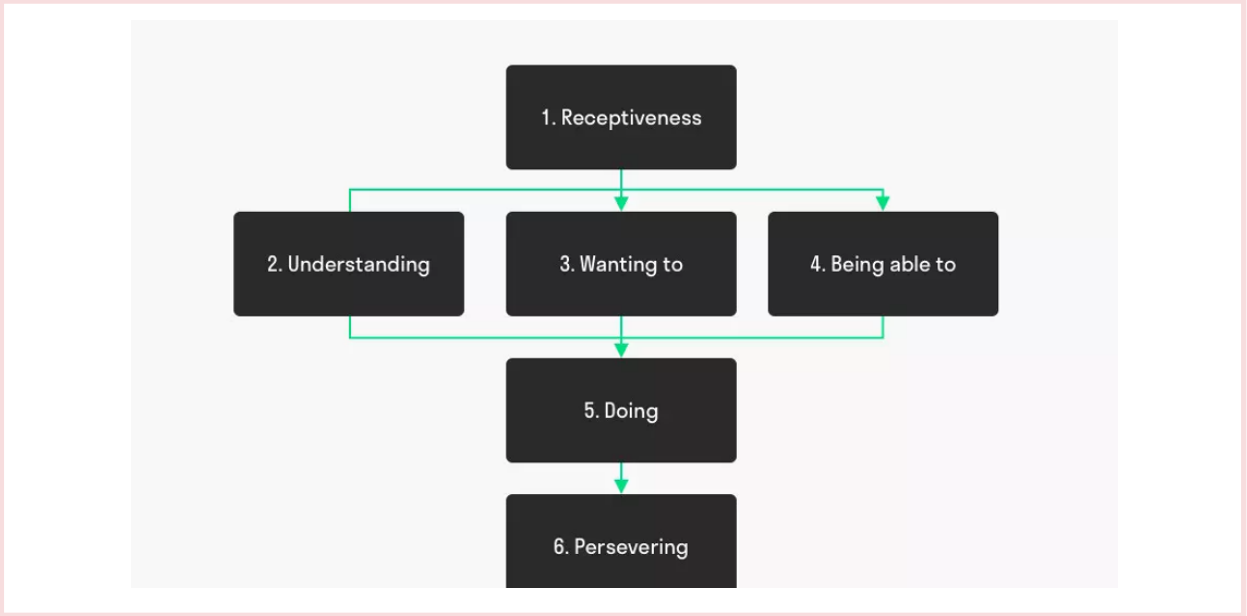
As behaviour is a complex process influenced by many factors, behavioural change is a very demanding task, as some of the variables cannot be changed (e.g. demographics, culture, personality…) and some are difficult (but not impossible) to change (e.g. attitudes, norms, efficacy).

9 Sara Rafael Almeida, Joana Sousa Lourenço, François J. Dessart and Emanuele Ciriolo, Insights from behavioural sciences to prevent and combat violence against women, EUR 28235 EN, doi:10.2788/412325

The behavioural change demands several conditions to be fulfilled first. As shown in one model example – Balm's Behavioural Change Model, there are 6 stages which need to be fulfilled for behaviour change. Among those are receptiveness (being open) to change, understanding the new behaviour, wanting and being able to change, change the behaviour and maintain the behaviour.

Behaviour change is not a simple or quick process. It takes time, the person needs to be motivated and able to change, and the final stage in the model is to maintain the new behaviour, which is more likely to happen when there is support from the environment.

Picture 3: Behavioural Change Model by M. Balm



Source: M. Balm 2002

Why cyberviolence happens?

As the CYBERVAW (2018) study and others show, there are several reasons for the occurrence of cyberviolence, most often it is perceived as a joke or fun. **Most persistent reasons for cyberviolence:**

- It was a joke, for fun;
- To hurt someone;
- Because someone did it to me;
- To get back at an ex;
- To get respect from friends;
- I was scared not to participate.

The needs identified

With the focus groups we identified the following needs:

- It is important to talk about stereotypes;
- It is important to emphasise that the victim should never be blamed for (cyber)violence;
- It is important they learn to recognise cyberviolence;
- Teenagers suggested the following topics to be included in a serious game:

- Sexting
- Online harassment and stalking
- Stereotypes about boys and girls
- Pressure put on boys and girls
- Body image and peer pressure;
- What to do when cyberviolence happens.

Behaviours to tackle in the project – Targets

With the help of the focus groups and existing research, we have identified several behaviours that need to be tackled in the project. Oftentimes cyberviolence is tolerated, especially by the boys, who may see cyberviolence as fun and not as a harmful behaviour. Cyberviolence is not always recognised nor by victim nor by perpetrator and it is important to raise awareness among teenagers that there are several different forms of cyberviolence. In a lot of cases, teenagers blame victims for cyberviolence (i.e. a girl, the victim, is guilty, because she sent the pictures) and it is important to change this opinion, as a victim is never guilty of the violence that happens to him or her, the one responsible for the violence is the perpetrator and there are no excuses for violence. When cyberviolence happens, the victim should talk to an adult person, if needed they need to be encouraged to go to the police, and friends who know about cyberviolence have to be encouraged not to be silent, but to tell someone about it.

Gender stereotypes represent generalised and simplistic characteristics, abilities and interests defined solely on the basis of gender. They create an unrealistic and unjust idea of men and women. Stereotypes are the forerunner of prejudice and can lead to gender-based violence.

- Tolerance of cyberviolence (Cyberviolence should not be tolerated, there is no excuse for cyberviolence);
- Recognition of cyberviolence (teenagers don't recognise all violent actions as cyberviolence);
- Victims should never be blamed for cyberviolence;
- Perpetrators are the ones responsible for violence;
- It is important to talk to someone when cyberviolence happens;
- Bystanders should not keep quiet about cyberviolence – react;
- Rooted gender stereotypes (gender stereotypes can lead to violence).

Glossary

This is a non-exhaustive list of the many forms of cyberviolence and hate speech online against women, in an attempt to paint a comprehensive picture of the phenomenon.

Violations of privacy

- **Revenge porn** or image-based sexual abuse/exploitation is the type of behaviour consisting of accessing, using or disseminating private graphical or video content without consent or knowledge of the victim, content sent by means of 'sexting' can also be shared without consent.
- **Creepshots**, upskirting or digital voyeurism consist of perpetrators taking non-consensual photos or videos of women's private areas and sharing them online.
- **Doxing** or **doxxing** refers to researching/manipulating and publishing private information about an individual, without their consent as to expose, shame and sometimes access and target the person in "real life" for harassment or other types of abuse.
- **Impersonation** is the process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation.
- **Hacking** or **Cracking** refers to the act of intercepting private communications and data, it can target women especially in the form of webcam hacking.

Stalking

- **Cyber stalking** is the action of spying, fixating or compiling information about somebody online and to communicate with them against their will. The tactic is often used and analysed as an extension of intimate partner violence.

Harassment

- **Cyberbullying** consists of repeated behaviour using textual or graphical content with the aim of frightening and undermining someone's self-esteem or reputation.
- **Threats** of violence, including rape threats, death threats, etc. directed at the victim and or their offspring and relatives, or incitement to physical violence.
- Unsolicited receiving of sexually explicit materials.
- **Mobbing**, refers to the act of choosing and targeting someone to bully or harass through a hostile mob deployment, sometimes including hundreds or thousands of people.

Sexist hate speech

- Sexist hate speech is defined as expressions which spread, incite, promote or justify hatred based on sex.
- Posting and sharing violent content portraying women as sexual objects or targets of violence.
- Use of sexist and insulting comments, abusing women for expressing their own views and for turning down sexual advances.
- Pushing women to commit suicide.

Direct violence

Some forms of cyberviolence against women have a direct impact on their immediate physical safety:

- **Trafficking** of women using technological means such as recruitment, luring women into prostitution and sharing stolen graphical content to advertise for prostitution.
- **Sexualised extortion**, also called sextortion and identity theft resulting in physical abuse.
- **Online grooming** consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations. The term "grooming" is criticised by victims, as it covers the child sexual abuse dimension of the act.
- In Real-World Attacks it is defined as cyberviolence having repercussions in "real life".

Sources

Attrill A. et al. Cyberpsychology, Oxford University Press, 2015

Agatston, P., Kowalski, R., Limber, S.(2012) Youth views on cyberbullying. In: Patchin, J. W., Hinduja, S. (eds) Cyberbullying prevention and response: Expert perspectives, New York, NY: Routledge, pp. 57–71.

Baker, C. &Carreño, P. (2016). Understanding the Role of Technology in Adolescent Dating and Dating Violence. *Journal of Child & Family Studies*, 25(1), 308-320. doi:10.1007/s10826-015-0196-5

Corcoran, L., Mc Guckin C. & Prentice G. (2015). Cyberbullying or Cyber Aggression?: A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. Societies, 5(2), 245-255. Available at: https://doaj.org/article/22ff3c4e25dd40b2af67f5e7c5e0f3ee EIGE cyberviolence against women and girls; http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls?lang=lt (viewed on July 25th, 2017)

Dempsey, A., Sulkowski, M., Nichols, R., &Storch, E. (2009). Differences between peer victimization in cyber and physical setting and associated psychosocial adjustment in early adolescence. *Psychology InTheSchools*, 46(10), 962–972. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.464.2397

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014). Cyberbullying in social networking sites: An adolescent victim's perspective. *Computers In Human Behavior*, 36, 13–20. doi: 10.1016/j.chb.2014.03.026

Duggan, M., Rainie, L., Smith, A., Funk, C., Lenhart, A., & Madden, M. (2014). Online harrassment. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/07/PI_2017.07.11_Online-Harassment_FINAL.pdf

Frisen, A.; Berne, S. &Lunde, C. (2014). Cybervictimization and body esteem: Experiences of Swedish children and adolescents. *Eur. J. Dev. Psychol.*, 11, 331–343. Available at: https://gup.ub.gu.se/publication/197994

Hinduja, S., &Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206–221. doi: 10.1080/13811118.2010.494133

Jacobs, N.C.L., Goossens, L., Dehue, F., Völlink T. &Lechner L. (2015). Dutch Cyberbullying Victims' Experiences, Perceptions, Attitudes and Motivations Related to (Coping with) Cyberbullying: Focus Group Interviews. *Societies*, 5(1), 43–64. Available at: https://doaj.org/article/411d004d28c343e7ba41755ca2035e6c

Korchmaros, J. D., Ybarra, M. L., & Mitchell, K. J. (2015). Adolescent online romantic relationship initiation: Differences by sexual and gender identification. *Journal Of Adolescence*, 40, 54–64. doi:10.1016/j.adolescence.2015.01.004

Lindfors, P.L.; Kaltiala-Heino, R.; Rimpelä, A.H. (2012). Cyberbullying among Finnish adolescents-A population-based study. BMC Public Health, 12, 1027. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3585473

Livingstone, S.,Haddon, L.; Görzig, A. & Ólafsson, K. (2011) Risks and Safety on the Internet: The Perspective of European Children. Full Findings. EU Kids Online: London, UK, 2011. Available at: http://eprints.lse.ac.uk/33731/

Marczak, M., & Coyne, I. (2010). Cyberbullying at School: Good Practice and Legal Aspects in the United Kingdom. *Australian Journal of Guidance & Counselling*, 20(2), 182–193. Available at: http://search.informit.com.au/documentSummary;dn=866657740309758;res=IELHEA

Mascheroni, G. & Cuman, A. (2014). *Net Children Go Mobile*. Final Report.Educatt: Milano, Italy. Available at: http://netchildrengomobile.eu/reports/

Mena-Rodriguez, E. & Velasco-Martínez, L. C. (2017). Gender Violence and Social Networks in Adolescents. The Case of the Province of Malaga, pp. 44-49, *7th International Conference on Intercultural Education "Education, Health and ICT for a Transcultural World"*, EDUHEM 2016, 15-17 June 2016. doi: 10.1016/j.sbspro.2017.02.009

Menesini, E.; Nocentini, A.; Palladino, B.; Frisen, A.; Berne, S.; Ortega-Ruiz, R.; Calmaestra, J.; Scheithauer, H.; Schultze-Krumbholz, A.; Luik, P.; et al. (2012). Cyberbullying definition among adolescents: A comparison across six European countries. *Cyberpsychol. Behav. Soc. Netw.*, 15, 455–462. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3443335

Navarro, R.; Serna, C.; Martínez, V.; Ruiz-Oliva, R. (2013). The role of internet use and parental mediation on cyberbullying victimization among spanish children from rural public schools. *Eur. J. Psychol. Educ.*, 28, 725–745. Available at: https://link.springer.com/article/10.1007%2Fs10212-012-0137-2

Navarro, R.; Yubero, S.; Larrañaga, E.; Martínez, V. (2012) Children's cyberbullying victimization: Associations with social anxiety and social competence in a Spanish sample. Child Indic. Res., 5, 281–295. doi: 10.1007/s12187-011-9132-4

No Bullying https://nobullying.com/gender-violence (viewed on September 9th, 2017)

Nocentini, A., Calmaestra, J, Schultze-Krumbholz, A., Scheithauer, H. , Ortega, R. &Menesini, E. (2010). Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance & Counselling*, 20(2), 129–142. Available at: http://search.informit.com.au/documentSummary;dn=866415511683401;res=IELHEAPew Research Center, http://www.pewresearch.org/fact-tank/2017/07/14/men-women-experience-and-view-online-harassment-differently/ (viewed on July 25th, 2017)

Paul, S., Smith, P.K., & Blumberg, H.H. (2010). Addressing Cyberbullying in School Using the Quality Circle Approach. *Australian Journal of Guidance & Counselling*, 20 (2), 157–168. Available at: http://search.informit.com.au/documentSummary;dn=866545942482208;res=IELHEA

Randa, R., Nobles, M.R. &Reyns, B.W. (2015). Is Cyberbullying a Stand Alone Construct? Using Quantitative Analysis to Evaluate a 21st Century Social Question. *Societies*, 5(1), 171–186. Available at: https://doaj.org/article/a7ebd5bf77d945a5ab0b52fcb709b1fe

Rivers, I., &Noret, N. (2010). 'I h8 u': findings from a five-year study of text and email bullying. *British Educational Research Journal*, 36(4), 643–671. Available at: http://bura.brunel.ac.uk/bitstream/2438/6462/3/Fulltext.pdf

Sari, S. V., &Camadan, F. (2016). The new face of violence tendency: Cyber bullying perpetrators and their victims. *Computers In Human Behavior*, 59, 317–326. doi: 10.1016/j.chb.2016.02.027

Slonje, R., & Smith, P. K. (2008). Cyberbullying: another main type of bullying? *Scandinavian Journal of Psychology,* 49, 147–154. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.532.4885

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. &Tippett, N. (2008) Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376–385. Available at: https://acamh.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1469-7610.2007.01846.x

Tsitsika, A., Janikian, M., Tzavela, E., Tzavara, C., Wójcik, S., Makaruk, K., & ... Richardson, C. (2015). Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. *Computers In Human Behavior*, 51, 1–7. doi: 10.1016/j.chb.2015.04.048

UN women http://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release

UN Broadband commission (2017). http://broadbandcommission.org/Documents/publications/WorkingGroupDigitalGenderDivide-report2017.pdf

Un Broadband Commission (2015). Cyber Violence Against Women And Girls. A Report by the UN Broadband Commission for Digital Development Working Group on Broadband and Gender.

Emma Louise Backe, Pamela Lilleston, PhD, MHS, and Jennifer McCleary-Sills (2018). Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence. Violence and Gender. Volume 5, Number 3. DOI: 10.1089/vio.2017.0056 https://www.liebertpub.com/doi/full/10.1089/vio.2017.0056

Violence against women: an EU-wide survey, European Union Agency for Fundamental Rights, 2014 http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

Völlink, T..Bolman, C.A., Dehue, F., Jacobs, N.C. (2013). Coping with cyberbullying: Differences between victims, bully-victims and children not involved in bullying. J. Commun. *Appl. Soc. Psychol*., 23, 7–24. doi: 10.1002/casp.2142

Wachs, S., Junger, M., &Sittichai, R. (2015). Traditional, Cyber and Combined Bullying Roles: Differences in Risky Online and Offline Activities. *Societies,* 5(1), 109–135. Available at: https://doaj.org/article/7494617060ea456682fb916604a95086

West J., Cyberviolence against women, 2014 for BWSS http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf (viewed on September 9th, 2017)

WomensAId UK: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

Ybarra, M.L., Alexander, C., & Mitchell, K.J. (2005). Deppressive symptomatology, youth Internet use, and online interactions: a national survey. *The Journal of Adolescent Health*, 36, 9–18. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.362.9357

Pashang S., Clarke J., Khanlou N., Degendorfer K. (2018) Redefining Cyber Sexual Violence Against Emerging Young Women: Toward Conceptual Clarity. In: Pashang S., Khanlou N., Clarke J. (eds) Today's Youth and Mental Health. Advances in Mental Health and Addiction. Springer, Cham

World Health Organization. (2013).Violence against women: Intimate partner and sexual violence against women. (Fact sheet N°239). Retrieved from: http://www.who.int/mediacentre/factsheets/fs239/en/

Klein, R. (2013). Framing Sexual and Domestic Violence through Language. Hampshire, UK: Palgrave Macmillan

Ruiz-Pérez, I., Plazaola-Castaño, J., &Vives-Cases, C. (2007). Evidence-based public health policy and practice: Methodological issues in the study of violence against women. *Journal of Epidemiology and Community Health*, 61, ii26-ii31. doi:10.1136/jech.2007.059907

K.S. Sargent, A. Krauss, E.N. Jouriles, R. McDonald (2016). Cyber victimization, psychological intimate partner violence, and problematic mental health outcomes among first-year college studentsCyberpsychol., *Behav. Soc. Netw.*, 19 (9) , pp. 545-550

Dr Becky Faith and Dr Erika Fraser (2018). What Works to Prevent Cyber Violence against Women and Girls? UKaid. VAWG Helpdesk Research Report

deSHAME (2017). Young people's experiences of online sexual harassment. A cross-country report from project deSHAME.

Council of Europe (2018). Mapping study on cyberviolence. (Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children).

A. DeSmet, S. Bastiaensens, K. Van Cleemput, K. Poels, H. Vandebosch, G. Deboutte, L. Herrewijn, S. Malliet, S. Pabian, F. Van Broeckhoven, O. De Troyer, G. Deglorie, S. Van Hoecke, K. Samyn, I. De Bourdeaudhuij (2018). The efficacy of the Friendly Attac serious digital game to promote prosocial bystander behavior in cyberbullying among young adolescents: A cluster-randomized controlled trial. *Computers and Human Behavior.* Volume 78, January 2018, Pages 336-347


CYBER
SAFE