Cyber violence against women and girls
## Introduction

1. Cyber violence as a form of gender-based violence
2. What is Cyber violence against women and girls?
3. Defining forms of cyber violence against women and girls

## Data availability and research

3. Law enforcement responses

## Conclusions and recommendations

5. Endnotes
Introduction

The increasing reach of the internet, the rapid spread of mobile information, and the widespread use of social media, coupled with the existing pandemic of violence against women and girls (VAWG) (1), has led to the emergence of cyber VAWG as a growing global problem with potentially significant economic and societal consequences (2).

Research shows (1) that one in three women will have experienced a form of violence in 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 cyber violence since the age of 15 (3). Access to the internet is fast becoming a necessity for economic well-being (4), and is increasingly viewed as a fundamental human right (5); therefore it is crucial to ensure that this digital public space is a safe and empowering place for everyone, including women and girls.

In order to better understand the nature and prevalence of cyber VAWG, the European Institute for Gender Equality (EIGE) has recently conducted desk research that aimed to identify and analyse the existing research on different forms of cyber VAWG and assess the availability of survey and administrative data on the phenomenon. The findings of this research and the resulting recommendations form the basis of this paper.

Cyber violence as a form of gender-based violence

What is cyber violence against women and girls?

To date, cyber VAWG has not been fully conceptualised or legislated against at EU level. Furthermore, there has been no gender-disaggregated EU-wide survey on the prevalence and harms of cyber VAWG and there is limited national-level research within EU Member States. However, the research that is available suggests that women are disproportionately the targets of certain forms of cyber violence compared to men. For example, in a survey of more than 9,000 German Internet users aged 10 to 50 years, women were significantly more likely than men to have been victims of online sexual harassment and cyber stalking, and the impacts of these forms of violence were more traumatic for victims (7).

This finding is corroborated by a 2014 survey by the Pew Research Center in the United States (8), which found that though men are slightly more likely than women to experience relatively ‘mild’ forms of online harassment (such as name-calling and embarrassment), women (particularly young women aged 18-24) disproportionately experience severe types of cyber harassment, namely cyber stalking and online sexual harassment.

The results of these studies are echoed by further research, exposing the limitations in taking a gender blind approach to cyber violence; the current evidence suggests that the forms of violence and the resulting harm is experienced differently by women and men (9).

In addition, experts have warned against conceptualising cyber VAWG as a completely separate phenomenon to ‘real world’ violence, when in fact it is more appropriately seen as a continuum of offline violence. For example, cyber stalking by a partner or ex-partner follows the same patterns as offline stalking and is therefore intimate partner violence (10), simply facilitated by technology (11). Evidence confirms this continuum: a UK study of cyber stalking found that over half (54 %) of the cases involved a first encounter in a real-world situation (12).
Cyber violence against women and girls

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.

**Cyber Harassment**

Cyber harassment can take many forms, but for the purposes of this paper, it can include:

- 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).

**Non-consensual Pornography**

Also known as cyber exploitation or revenge porn, non-consensual pornography 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 (such as getting them fired from their job).

There have been multiple publicised cases of female victims of non-consensual pornography in EU Member States and the US over recent years, several of whom committed suicide as a result (14). Research suggests that up to 90% of revenge porn victims are female (15) and that the number of cases is increasing (16). There are also a growing number of websites dedicated to sharing revenge porn, where users can submit images alongside personal information such as the victim’s address, employer and links to online profiles (17).

An additional related trend with equally devastating impacts on victims is the live-broadcasting of incidents of sexual violence.
Cyber violence against women and girls

Data availability and research

Data on cyber VAWG in the EU is scarce and consequently very little is known about the actual percentage of victims of cyber VAWG and the prevalence of harm. The best information available at EU level comes from the European Agency for Fundamental Rights’ (FRA) European Survey on Violence Against Women (VAW) (2014), which included questions on cyber stalking and cyber harassment. However, as this survey was the first to collect data on these forms of cyber VAWG across the EU, there is no means by which to trace the evolution of the phenomena and trends in victim numbers over time.

Apart from one (2008 Danish) survey, it was not possible to identify any nationally representative surveys at Member State level on the prevalence of cyber VAWG.

Given that in most Member States forms of cyber VAWG are not criminalised, police or justice data on the phenomenon is scarce. In Member States where forms of cyber VAWG are criminalised, the data collected is lacking disaggregation by sex of the victim and perpetrator, and the relationship between them, which limits the usefulness of the data. This lack of data hampers the ability to conduct a gendered analysis of cyber violence and a comparison of online and offline VAWG.

In addition to addressing the aforementioned gaps, more research is needed in the following areas:

1. Use of online adverts or postings to lure women into potentially harmful situations (‘recruitment’).

2. Assessment of the severity of harm experienced by victims of forms of cyber VAWG, and the impact on their lives.

3. Good practices in police and justice responses to cyber VAWG, including from a victim’s perspective.

4. Identification and analysis of risk factors and risk assessment procedures, to prevent harm and re-victimisation.
Law enforcement responses

Several Member States have recently adopted legislation targeting forms of cyber VAWG; for example, provisions criminalising revenge porn have been enacted in the U.K., France, Germany and Malta, with policies currently pending in Ireland and Slovenia. While this is a step in the right direction, studies suggest that current legal and policy approaches in the EU fail to adequately capture the social and psychological harm resulting from the use of sexual imagery to harass, coerce or blackmail women (26).

Furthermore, research reveals that the response of the criminal justice sector to women victims of cyber VAWG is inadequate. For example, of the 1 160 incidents of revenge porn reported during the first six months after its criminalisation in the U.K., 61% resulted in no further action pursued against the alleged perpetrator (27).

In 2013 the End Violence against Women Coalition (EVAW) gathered accounts at a roundtable on enforcement and prosecution of ‘violence and harassment’ online, reporting concerns that criminal justice authorities took a different, and less effective, approach to violence and harassment perpetrated online compared to offline. Several participants themselves had experienced ‘wholly inadequate police responses’ when reporting a crime perpetrated online (28).

Studies echo these concerns, revealing women’s frustration with police who tend to treat each individual online communication as a discrete act, rather than considering the cumulative impact of abuse (29). This reflects broader concerns about the criminal justice system’s response to VAWG in general (and particularly IPV). Moreover, victim blaming attitudes persist, especially in cases of revenge porn, demonstrating a lack of understanding and awareness. This is compounded by the fact that (according to a 2014 survey in the U.S.) more than half of stalking and cyber stalking victims did not acknowledge their own experience as a crime (30).

This inadequate criminal justice response can be attributed in part to the false dichotomy between online and offline VAWG, which results in police discounting and minimising the harms of cyber VAWG, and constructing victims’ experiences as ‘incidents’ rather than patterns of behaviour over time.

These findings reveal the need to design effective policy interventions at both the EU and Member State level, including but not limited to training for police and justice sector staff on cyber VAWG and awareness-raising campaigns.

Good practices

Legislation

In the UK, in April 2015 it became a criminal offence with maximum two-years imprisonment to share private sexual photographs or videos without the subject’s consent providing the intent of causing distress to those targeted (31). In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect (27).

Meanwhile in 2016, France adopted the ‘Digital Republic Law,’ which entails a harsher sanctioning of those found guilty of revenge porn. Under new legislation perpetrators face a two year prison sentence or € 60 000 fine (33).

Similar provisions were enacted by a German court, which in 2014 made it illegal to store intimate photographs of a former partner after they have called for their deletion (34).

Research and interventions

In 2009, the U.K. launched The National Centre for Cyber-stalking Research (NCCR) (35), which aims to provide research and analysis into the prevalence, motivations, impacts and risk assessment of cyber VAWG. In 2011 the centre published the results of a study on the prevalence, nature and impact of cyber stalking (36) and is currently conducting a survey investigating the impact and prevalence of revenge porn. Subsequently in 2015, a helpline for victims of revenge porn was established, receiving almost 2 000 calls in its first six months (37).

From July 2017, Slovenia will launch the project ‘CYBERVAW’, which aims to develop awareness-raising and education activities that spread a clear message of zero tolerance to VAWG, with a specific focus on prevention of gender-based cyber violence and harassment as a form of VAWG (38).
Conclusions and recommendations

In sum, due to the current lack of research and data at EU level, we cannot adequately quantify the prevalence or impact of cyber VAWG in the EU. However, the mounting evidence suggests that it is a growing phenomenon disproportionately affecting women and girls, with severe impacts on victims’ real lives. In order to better determine the prevalence and risk factors of, and effective policy responses to, cyber VAWG, a priority should be the development of measurement and quantification tools of these types of acts.

The following recommendations are in line with the international human rights legal framework, including the Istanbul Convention, and are based on a review of existing literature and evidence. They ultimately aim to support EU Member States to improve institutional responses to cyber VAWG, in order to protect women both online and offline.

1. Policy responses should be formulated in recognition of the fact that cyber VAWG is a form of VAW. Strategies for addressing cyber VAWG must also include the voices of women who are victims of the phenomenon.

2. In the immediate future, definitions of cybercrime on the Migration and Home Affairs website should be updated to include forms of cyber VAWG, or at the minimum, should include misogyny in the third part of its definition (39).

3. The EU should aim towards agreeing on definitions of forms of cyber VAWG and incorporate these forms of violence into EU legislation, to ensure that victims of cyber VAWG in Member States have access to justice and specialised support services.

4. A priority should be to improve gender-disaggregated data at EU level on the prevalence and harms of cyber VAWG, and to develop indicators to measure the effectiveness of interventions.

5. Any approach to tackling the phenomenon must not deny women and girls their place in the larger public space they gain from internet connection. The upcoming EU-wide Survey on GBV should include a question about whether women have avoided online spaces for fear of experiencing cyber VAWG.

6. There is a need for quantitative and qualitative research that examines system responses, based on a victims’ perspective.

7. Training on cyber VAWG with a gender perspective should be introduced to police responses to cybercrime.

8. There is a need for awareness-raising campaigns educating women and girls about cyber VAWG, their legal rights and available support services.

9. Prevention measures should be developed that include the ICT sector, including adoption of self-regulatory standards to avoid harmful gender stereotyping and the spreading of degrading images of women, or imagery that associates sex with violence.

10. It is important for EU level institutions and agencies combatting cybercrime to tackle gendered forms of cybercrime; particularly the online luring or ‘recruitment’ of women and girls into harmful situations such as trafficking.
Cyber violence against women and girls


(25) For example, England and Wales, which criminalised revenge porn in 2014. The BBC analysed freedom of information requests from 31 police forces in England and Wales between April and December 2015, though notably the sex of the victim and the relationship to the perpetrator is not recorded in the majority of cases, limiting the usefulness of the data: https://docs.google.com/spreadsheets/d/1T6bqWcss4JKu7L9LV11Ly-z8FeY-PUP42ZW-SNe3Gmw/edit?usp=sharing.


(29) See endnote 11.


Cyber violence against women and girls


(35) https://www.beds.ac.uk/research-ref/irac/nccr.


The European Institute for Gender Equality (EIGE) is the EU knowledge centre on gender equality. EIGE supports policymakers and all relevant institutions in their efforts to make equality between women and men a reality for all Europeans by providing them with specific expertise and comparable and reliable data on gender equality in Europe.

© European Institute for Gender Equality, 2017. Reproduction is authorised provided the source is acknowledged.