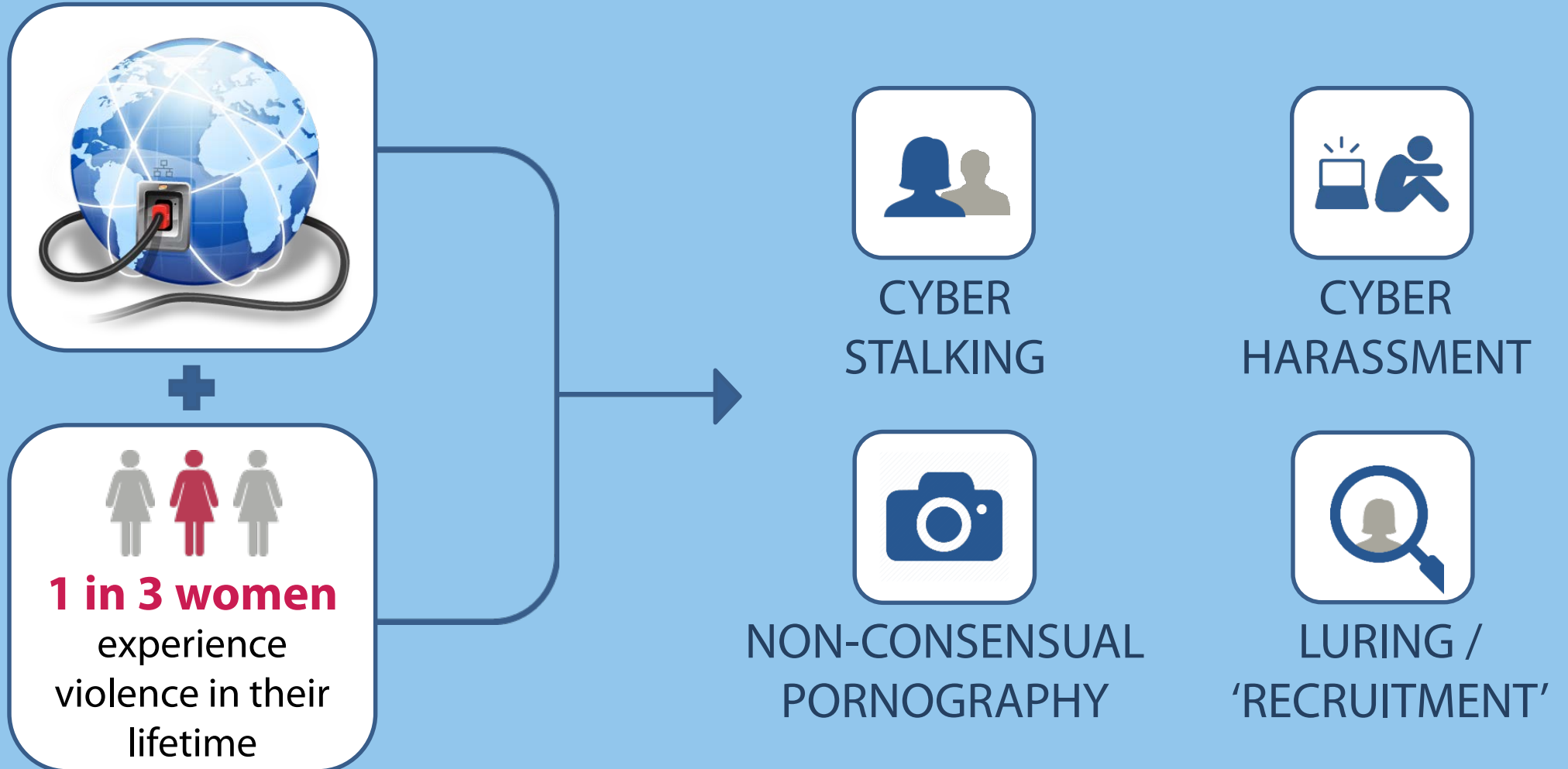


Cyber violence against women and girls

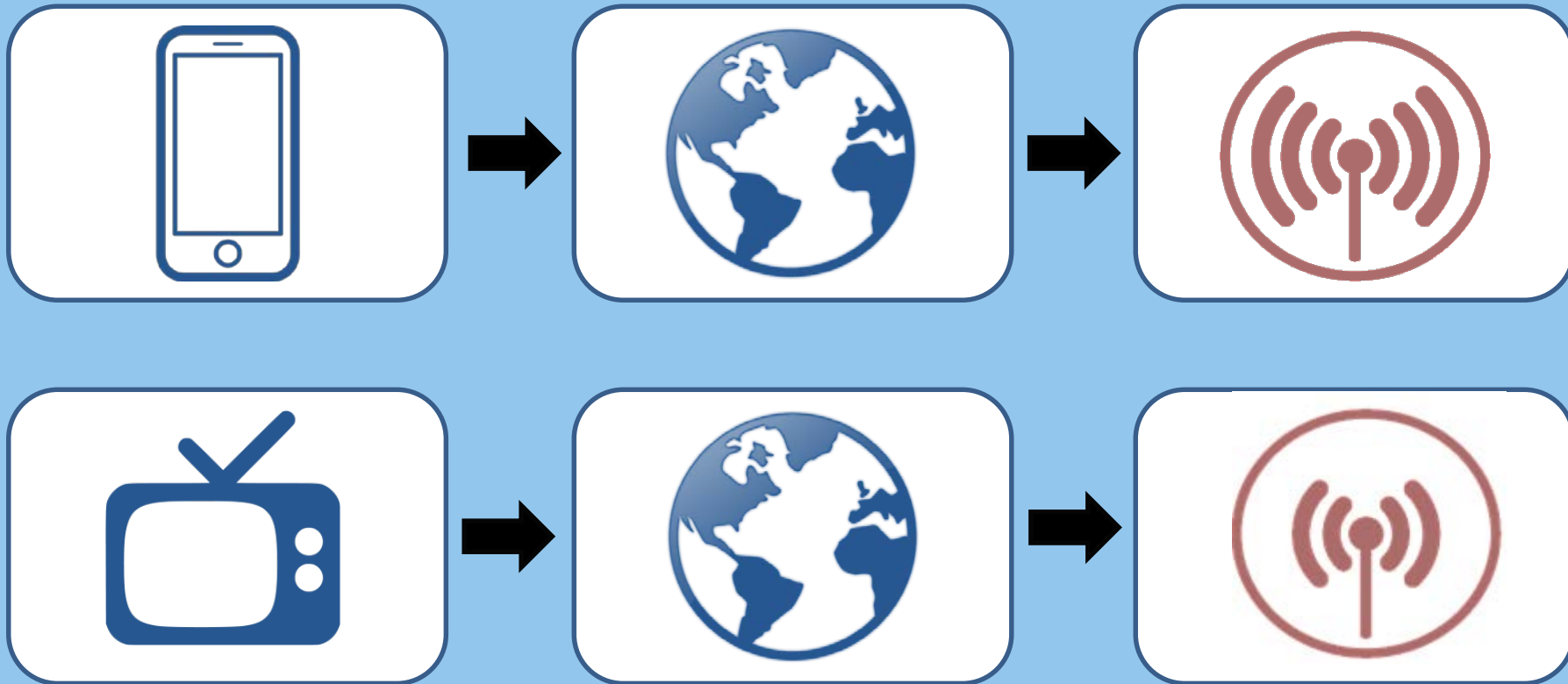


Jurgita Pečiūrienė

What is 'cyber VAWG'?



Information and Communication Technologies amplify severity



Differential harms by gender



**Moderate
severity**

Cyber insults
Embarrassment
**Mild online
harassment**

Cyber stalking
**Online sexual
harassment**
Revenge Porn



High severity

A continuum between online and offline

**VIOLENCE
AGAINST
WOMEN**

**CYBER
VAW**



70%

**Of cyber stalking
victims have also
experienced intimate
partner violence***

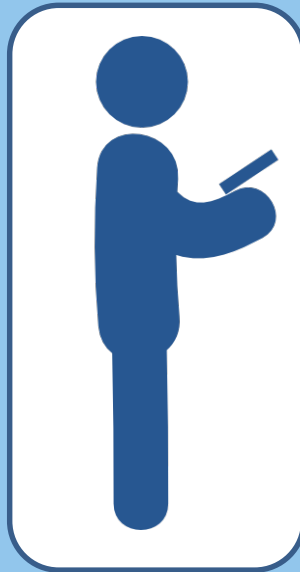
Victims of physical and sexual violence since the age of 15- IPV

* Cyber harassment since the age of 15 – IPV

		Cyber harassment	
		No. of physical and sexual IPV within cyber harassment	% physical and sexual IPV within cyber harassment
		Physical and sexual IPV since the age of 15	NO
	YES	518	76,5%
		677	



Social media facilitates violence



Potential Consequences

**Mental
health issues**



**Loss of
employment**



**Loss of
social status**



**Exclusion
from cyber-
space**



A lack of



Data



Research



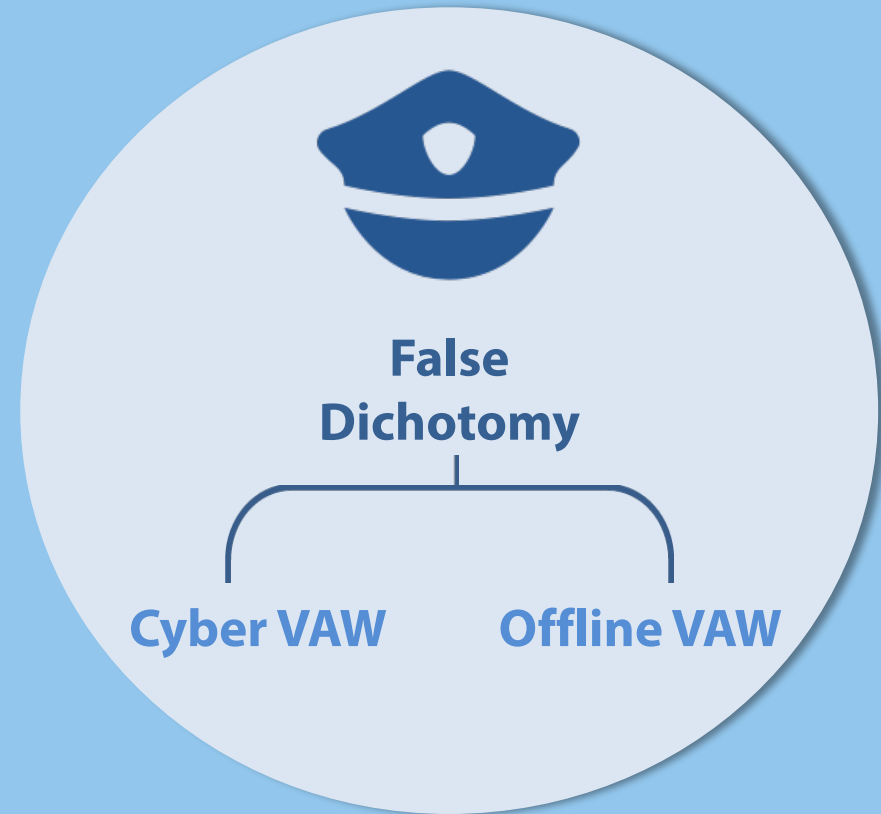
Legislature

Law enforcement responses are inadequate

61%



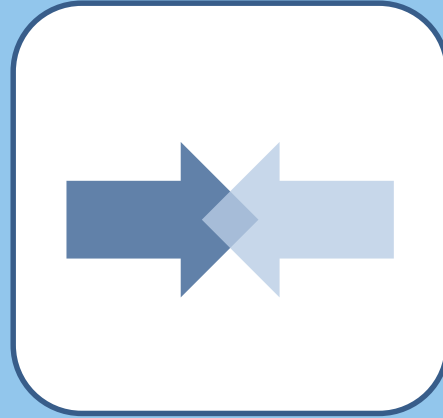
Of reported cases of revenge porn in the U.K. resulted in no further action taken against the perpetrator*



Training is needed for police and justice



Gendered
perspective



Links between
intimate partner
violence and
cyber VAW



Voices of victims

The need for policy interventions

A helpline for
victims of revenge
porn in the U.K.
received



Cyber VAW needs to be addressed at EU level

Cyber VAW is missing from EU definitions of cybercrime

At EU level, it is important to tackle **gendered forms of cybercrime** > **Trafficking**



The screenshot shows the 'MIGRATION AND HOME AFFAIRS' section of the European Commission website. The breadcrumb trail is: European Commission > Migration and Home Affairs > What we do > Policies > Organised Crime & Human Trafficking. The main navigation includes Home, What's New, Financing, Who We Are, What We Do (highlighted), and E-Library. A sub-navigation bar contains Policies (highlighted), Agencies, and Networks. The left sidebar lists various policy areas, with 'Organised Crime & Human Trafficking' selected. The main content area is titled 'Cybercrime' and features a yellow banner with 'CRIME SCENE' text. The text explains that European societies are increasingly dependent on electronic networks and information systems, leading to the development of criminal activity that threatens citizens, businesses, governments, and critical infrastructures alike: cybercrime. It defines cybercrime as criminal acts committed online using electronic communications networks and information systems, and classifies it into three broad categories: crimes specific to the Internet, online fraud and forgery, and illegal online content. A blue padlock icon is shown over a circuit board background.

MIGRATION AND HOME AFFAIRS

European Commission

European Commission > Migration and Home Affairs > What we do > Policies > Organised Crime & Human Trafficking

Home What's New Financing Who We Are **What We Do** E-Library

Policies Agencies Networks

Legal migration and Integration

Irregular Migration & Return

Common European Asylum System

Schengen, Borders & Visas

Industry for Security

Organised Crime & Human Trafficking

- > Trafficking in human beings
- > Trafficking in firearms
- > Child sexual abuse
- > **Cybercrime**
- > e-evidence
- > Drugs policy
- > Money laundering
- > Financial investigation
- > Corruption
- > Counterfeiting
- > Confiscation & asset recovery
- > Crime prevention

Cybercrime

European societies are increasingly dependent on electronic networks and information systems. The evolution of information communication technology has also seen the development of criminal activity that threatens citizens, businesses, governments and critical infrastructures alike: cybercrime.

What is cybercrime?

Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems. It is a borderless problem that can be classified in three broad definitions:

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
- Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

The ICT sector must form part of response



More EU data is needed

① Develop harmonised **definitions** for statistical purposes

② Develop **indicators** to measure effectiveness of interventions

③ Improve gender-disaggregated **data** on prevalence and harms of cyber VAW

Let's talk!



Gedimino pr. 16, LT-01103
Vilnius, Lithuania



eige.europa.eu



<https://twitter.com/eurogender>



facebook.com/eige.europa.eu



youtube.com/user/eurogender



eige.europa.eu/newsletter



Eurogender network

