Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Council of Europe Action on Cyberviolence

Initial steps to understand and tackle the issue

10 YEARS EaP Eastern Partnership

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC)

Mapping study – the background

Mapping Study on Cyberviolence sanctioned by the **Cybercrime Convention Committee of the Council of Europe** (T-CY) in November 2016 and completed/adopted in July 2018, aimed at:

- Mapping acts that constitute cyberviolence and drawing conclusions as to typologies and concepts;
- Providing examples of national experiences and responses to such acts (including policies, strategies, legislation, cases and case law);
- Discussing international responses under the Budapest Convention and other treaties (in particular the Istanbul and Lanzarote Conventions of the Council of Europe);
- Developing recommendations as to the further course of action.

Defining cyberviolence

Key definition adopted by the Mapping Study:

- **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.**

- In practice, acts of cyberviolence may involve different types of harassment, violation of privacy, sexual abuse and sexual exploitation and bias offences against social groups or communities.

- Cyberviolence may also involve direct threats or physical violence as well as different forms of cybercrime.

- Not all of 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.

Cyberviolence

ICT-related violations of privacy

- Computer intrusions
- Taking, sharing, manipulation of data or images, incl. intimate data
- Sextortion
- Stalking
- Doxing
- Identity theft
- Impersonation
- Etc.

ICT-related hate crime

Against groups based on

- race
- ethnicity
- religion
- sex
- sexual orientation
- disability
- etc.

Cyberharassment

- Defamation and other damage to reputation
- Cyberbullying
- Threats of violence, incl. sexual violence
- Coercion
- Insults or threats
- Incitement to violence
- Revenge porn
- Incitement to suicide or self-harm
- Etc.

ICT-related direct threats of or physical violence

- Murder
- Kidnapping
- Sexual violence
- Rape
- Torture
- Extortion
- Blackmail
- Swatting
- Incitement to violence
- Transmissions that themselves cause injuries
- Attacks on critical infrastructure, cars or medical devices
- Etc.

Cybercrime

- Illegal access
- Illegal interception
- Data interference
- System interference
- Computer-related forgery
- Computer-related fraud
- Child pornography

Online sexual exploitation and sexual abuse of children

- Sexual abuse
- Child prostitution
- Child pornography
- Corruption of children
- Solicitation of children for sexual purposes
- Sexual abuse via livestreaming
- Etc.

Coverage through European standards

- **Online sexual exploitation and sexual abuse of children** is covered by the Lanzarote Convention (Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse) which also applies if committed by means of computer systems (ICT) - specific procedural powers and means of international cooperation are offered by the Budapest Convention on Cybercrime.

- **Cybercrime** is addressed by the Budapest Convention on Cybercrime in terms of substantive criminal law, backed up by procedural powers and means of international cooperation.

- **Hate crime** is partly covered by the Additional Protocol to the Budapest Convention on Xenophobia and Racism – however not if motivated by gender, sexual orientation or disability.

- **Direct threats of and physical violence** - the mechanisms in the Budapest Convention may be used for domestic and international investigations.

- **Violations of privacy** partly addressed by the Budapest Convention and Article 34 on "Stalking" of the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention).

- **Cyberharassment** is the broadest category of cyberviolence and includes, among others, cyberbullying - the Istanbul Convention addresses "psychological violence" in Article 33 and "sexual harassment" in Article 40.

Issues identified

- Victims of cyberviolence frequently may not know **what to do to get help**.

- Law enforcement authorities are often not able to assist victims and cyberviolence may not be considered a **law enforcement priority** or may not be considered sufficiently serious (“we don’t do Facebook complaints”).

- While solutions to online violence, in particular sexual abuse, against children are available, there are gaps when it comes to responses to **online violence against adults**.

- **Social media providers** can play a role in the prevention and control of cyberviolence and in the protection of victims. This role is often considered insufficient.

- The prevention and control of cyberviolence may run counter to the **freedom of expression** and other rights (e.g. free speech versus hate speech). Where they do not actually conflict, their relationship must still be carefully considered.

- Etc.

5 recommendations by the T-CY

- The Council of Europe should create an **online portal** on existing policies, strategies, preventive, protective and criminal justice measures taken by public sector, civil society and private sector organisations.

- Ensure **synergies** between Budapest, Istanbul and Lanzarote Conventions by:
  - Raising awareness among Parties of the provisions of these treaties;
  - Drawing on these treaties in capacity building and advice to countries;
  - Introduce procedural powers and international cooperation means of the Budapest Convention in relation to online sexual violence against children and violence against women and family violence – consider accession to the Convention;
  - Address psychological violence, stalking and sexual harassment in an online context and address the sexual exploitation and the sexual abuse of children online – consider accession to Istanbul and Lanzarote Conventions;

- Better **training and awareness** raising for criminal justice authorities regarding cyberviolence, including its investigation, prosecution and sanctioning, where it constitutes a criminal offence – a call to action for Cybercrime Programme Office.

- Measures to prevent, protect against and – in cases where it constitutes a criminal offence – prosecute cyberviolence should be conceived as contributing to the implementation of the **UN Agenda 2030 for Sustainable Development**.

- Parties to the Budapest Convention to ensure greater **gender balance** in institutions dealing with cybercrime.

Thank you for your attention

Giorgi Jokhadze
Project Manager
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
Giorgi.Jokhadze@coe.int