

Cybercrime Convention Committee (T-CY)
Working Group on cyber bullying and other forms of online violence,
especially against women and children (CBG)

#### Update on the

# Mapping study on cyberviolence

T-CY 18, Strasbourg, 27-28 November 2017



# T-CY Working Group on Cyberviolence: Mandate

T-CY 16 (Strasbourg, November 2016) decided:

- to note strong support for the establishment of a T-CY Working Group on cyber bullying and other forms of online violence, especially against women and children – based on Article 1.1.j of the T-CY Rules of Procedure – and
- to task the Group to study the topic in the form of a mapping exercise, including comparative approaches to legislation as well as documentation of good practices in view of presenting interim results to the 17th Plenary and a final report to the 18th Plenary of the T-CY.

The WG held several physical and virtual meetings in 2017 and received case studies and other inputs from Parties and Observers.



## Aim of the mapping study

#### The study is 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 and case
- discussing international responses under the Budapest Convention and other treaties (in particular the Istanbul and Lanzarote Conventions of the Council of Europe), including possible gaps;
- developing recommendations as to the further course of action.

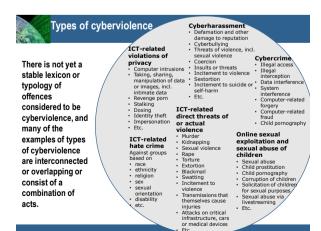


## Cyberviolence: working definition

The group proposes the following definition for the purpose of the 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

Note: This definition is an adaptation of the definition of "violence against women" in Article 3 Istanbul Convention.





#### Challenges to investigation and prosecution

- Victims don't know what to do.
- · Limited help by law enforcement.
- Protection of children versus protection of adult victims.
- Role of social media providers.
- Free speech versus hate speech.



## Cyberviolence under Lanzarote Convention

The Lanzarote Convention as a whole is aimed – through a holistic approach - at the protection of children against sexual violence:

- Prevention
- Protection and assistance to victims
- Substantive criminal law, including
  - sexual abuse (article 18),
  - child prostitution (article 19)

  - child pornography (article 20), participation of a child in pornographic performances (article 21),
  - corruption of children (article 22),
  - solicitation of children for sexual purposes (article 23);
- Investigation, prosecution, procedural law
- International cooperation
- Interpretative opinion of Lanzarote Committee (May 2017): Provisions apply also if committed or facilitated via ICT.
- ► Lanzarote and Budapest Conventions are complementary.



## Cyberviolence under Istanbul Convention

The "Council of Europe Convention on preventing and combating violence against women and domestic violence" (Istanbul Convention, CETS 210) contains a number of relevant provisions:

- Article 33 Psychological violence
- Article 34 Stalking
- Article 40 Sexual harassment
- Article 17 Participation of the private sector and the media

The Budapest and Istanbul Conventions appear complementary. A country implementing the Budapest Convention should thus consider also implementation of articles 33, 34 and 40 Istanbul Convention in order to combat psychological violence, stalking and sexual harassment in an online context.



### Cyberviolence under Budapest Convention

- Articles 2 11 apply directly or indirectly.
- Articles with a direct connection to cyberviolence:
  - Article 4 Data interference in a critical system
  - Article 5 System interference in a critical system
  - Article 9 Child pornography.
- Procedural law applies.
- International cooperation provisions apply.



#### Other national and international responses

- A wide range of initiatives are being undertaken by governments, civil society, private sector and international organisations - frequently in partnership - to PREVENT cyberviolence.
- PROTECTIVE measures often focus on the protection of children against sexual exploitation and sexual abuse (example of hotlines).
- Age is a decisive criterion when it comes to the PROSECUTION of cyberviolence (example of specialised units on sexual violence against children). This is less the case if victims of cyberviolence are adults (example of exception: UK prosecution guidance on hate crime).
- CRIMINALISATION of cyberviolence:
  - Often specific laws on online sexual violence against children.
  - Less the case for other forms of cyberviolence.
  - Most States seem to apply regular criminal law and other provisions.



#### **Preliminary findings**

## On the concept of cyberviolence:

- Provisional definition: 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.
- This includes cyberharassment (including cyberbullying), violation of privacy, the online sexual exploitation and sexual abuse of children. Some forms of cybercrime as well as direct threats of or actual violence may also constitute cyberviolence.
- ► Concept remains elusive and difficult to delimit.



#### **Preliminary findings**

## On scope, impact and issues

- Physical world solutions to violence may therefore also be applied to address acts of violence if computers are involved.
- However:
  - · Few barriers to cyberviolence vs physical world violence
  - Cyberviolence not simple extension of physical world violence. Nature and impact changes.
- ► Specific solutions are required.



## **Preliminary findings**

## On national and international responses

- Prevention and protection policies and measures by public, private and international organisations with primary focus on children and young adults.
- Criminalisation, investigation and prosecution of online sexual abuse of children.
- Less prevention, protection and criminalisation and prosecution for other forms of cyberviolence and for adults.
- Limited criminal justice response to specific forms of cyberviolence.
- ► Limited guidance by international instruments.



## **Preliminary findings**

#### On role of Budapest Convention

- The Budapest Convention through a number of substantive criminal law provisions addresses directly some types of cyberviolence. 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.
- ► Links between Budapest, Lanzarote and Istanbul Conventions to be reinforced.



## **Preliminary findings**

# On types of cyberviolence addressed/not addressed in international agreements

- Online sexual exploitation and sexual abuse of children ► Lanzarote Convention
- Cybercrime ▶ Budapest Convention
- Hate crime ➤ Protocol on Xenophobia and Racism and other instruments on discrimination and intolerance
- Direct threats of or actual violence ➤ Domestic law + procedural and international cooperation provisions of Budapest Convention
- Violations of privacy ➤ Budapest Convention and Article 34 Istanbul Convention on Stalking ➤ Additional international solutions may be needed
- Cyberharassment ➤ Istanbul Convention (Article 33 psychological violence, Article 40 – sexual harassment) ➤ Additional international solutions may be needed.



#### Recommendations

[in progress]



## Next steps proposed

- T-CY 18 to consider extension of the mandate of the Working Group to July 2018
- Working Group to present final study at T-CY 19 (9-10 July 2018)
- Workshop on cyberviolence at Octopus Conference (11-13 July 2018)