# 2019 OPEN CALL

# REQUEST FOR EXPRESSIONS OF INTEREST

# FOR

# TECHNOLOGY SOLUTIONS TO MAKE DIGITAL SPACES SAFE FOR CHILDREN

**Subject:** Technology Solutions to Make Digital Spaces Safe for Children
**Issue date:** 4 September 2019

**Submit Expression of Interest at: https://www.end-violence.org/2019-open-call-request-expressions-interest**

## I. Summary

The End Violence Fund invites **Expressions of Interest** focused on **solutions that leverage existing and new technologies to prevent and combat online child sexual exploitation and abuse (online CSEA).** The total funding envelope to be awarded through this Open Call is **~US$ 13 million.**[1]

The Fund will be looking into scaling/adapting existing and developing new technologies, such as artificial intelligence, machine learning, data science, blockchain, virtual reality and other innovative solutions that have the potential to enhance detection and response to online violence and prevent known and emerging online CSEA threats.

Funding is not necessarily limited to the above. We are interested in solutions that apply technology in innovative, groundbreaking ways that are scalable and globally applicable, enhancing the capacity of all stakeholders to address online CSEA and make children safe online.

We are looking for **solutions** that can help achieve one or more of the four specific objectives below:

(1) **Detect, remove and report images, videos** with sexual content involving children and adolescents (*often referred to as child sexual abuse material, or CSAM*)

[1] The total amount to be awarded will depend on the quality and volume of received applications i.e. the Fund may decide to slightly increase or lower the amount if specific opportunities arise or as a result of the initial assessment of applications.

(2) **Block adults' access to children on digital platforms** intended to sexually abuse them (*usually referred to as online sexual grooming or solicitation*)

(3) **Stop live-streaming of child sexual abuse** performed in front of a camera (*usually referred to as live-streaming of CSEA*)

(4) **Prevent online sexual abuse of children before it happens**, including prevention and solutions that directly target online child sexual offenders and adults with a sexual interest in children

If you are aligned with our general criteria, we want to hear from you.

You can read more on the nature and magnitude of online CSEA in Annex 1, and in Annex 2 you will find a list of examples of types of technology solutions we are looking into within each objective.

As in previous years, we are actively seeking submissions of ideas from nonprofit organisations, such as civil society organisations (CSOs), non-governmental organisations (NGOs), international organisations, research institutes and academic institutions, for the grant portion of this funding.

In addition, for the first time in the Fund's history, we will identify a small cohort of technology companies working on solutions for the prevention of online CSEA, for our equity-free seed investments.

The End Violence Fund does not provide core organisational funding for nonprofit organisations, nor does it support creation of new business lines for private companies. The Fund provides seed funds to support the development of solutions to the stage where these are proven to be workable and can be implemented and/or scaled. In addition, regarding investments to private companies, the End Violence Fund does not seek financial return, nor does it take equity, instead it requires that all code, content or hardware developed and tested be open source and be publicly available.[2]

All submitted ideas must meet the criteria required to be eligible for funding, as detailed below.

Funded projects will be connected to similar projects in other countries, which should enable projects to develop faster and better (here you can access the list of all Fund-supported grantees, and here you can see a map of all projects focused on online child sexual exploitation and abuse).

## II. General Conditions

The End Violence Fund invites nonprofit organisations (CSOs, NGOs, international organisations, research institutes and academic institutions) and private companies to respond to this Expression of Interest (EoI).

[2] The Fund will consider occasional exceptions to the open-source rule as justified by the nature and/or sensitivity of the proposed solution.

Please note that most of the available funds (~US$10 million) aim to support solutions which will benefit countries eligible for ODA support. The remaining funds (~US$3 million) are not subject to this restriction and can support work in non-ODA countries.

The 2019 End Violence Open Call funding will be available through two modalities: (A) project grants and (B) equity-free seed investments. See the summary of the funding modalities and available funding in the table below:

| Funding modality | Funding Focus | Total funds available | Who can apply | Max duration | Allocation amount |
|---|---|---|---|---|---|
| **A. Project grants** | Strengthen the use, adaptation and scale-up of existing technology solutions | Up to $12 million | NGOs, CSOs, academic institutions, research institutes and international organisations | 2 years | Up to $750,000 |
| **B. Equity-free seed investments** | Design and test new technology solutions | Up to $1 million | Private companies | 2 years | Up to $250,000 |

Under the 2019 Open Call, eligible submissions to this Request for Expressions of Interest will be invited to submit a full project proposal under one of two funding modalities, as follows:

- In the case of funding modality A, and upon rigorous assessment of the full project proposal, the successful proposal will result in signing of a Grant Confirmation Letter for a period of up to two years and up to US$750,000; and

- In the case of funding modality B, and upon rigorous assessment of the full project proposal, the successful proposal will result in signing of an institutional corporate contract with the successful vendor for a period of up to two years and up to US$250,000.

Considerations of Expressions of Interest with solutions that require more funding than the indicated amount will be considered by the Fund at its sole discretion and only if this is in the best interests of achieving the goals of the funding round.

**Description of requirements**

**Eligibility criteria:**

End Violence Fund is looking to provide project grants to nonprofits and investment-style, equity-free seed funding to private companies. Only entities that fulfill these mandatory requirements will be considered eligible:

- **legally registered** entity, either as nonprofit or private company
- the tech solution addresses one or more of the **four objectives** of the 2019 Open Call
- Your organisation has a safeguarding policy in place (including data privacy) or is willing to develop a policy *****
- the proposed solution responds to a **clear need/gap**, does not duplicate existing tools, and builds upon and/or interacts with existing solutions
- at minimum, an **existing prototype** of the open source solution with promising results from initial pilots

***** *The Partnership is committed to supporting organisations to improve their safeguarding capacity and practice. As part of this, we ask all grantees to complete the Grantee Self-assessment, which can be found on the materials sidebar. While this is not required as part of your expression of interest, please note all shortlisted organisations and companies will be expected to complete this as part of the proposal.*

## III. Submission of Expressions of Interest

All submissions must be made in English. Interested entities that meet the eligibility criteria are required to complete and submit the Expression of Interest form and provide the information and supporting documents indicated in the form. Response forms must be submitted through www.end-violence.org/fund.

Expressions of Interest will be reviewed on an ongoing basis. However, the last day for submissions of Expressions of Interest is **6 December 2019**.

Only shortlisted applicants will be contacted and thereafter invited to invited to submit a detailed proposal.

This Request for Expressions of Interest does not constitute a call for proposals and/or solicitation. End Violence Fund does not require proposals or bids at this stage; this request is merely seeking an expression of interest to participate in the Fund's 2019 Open Call.

A response to this Request for Expressions of Interest does not automatically guarantee that submitting entities will be selected to submit a detailed proposal.

The End Violence Fund reserves the right to change or cancel the requirement at any time during the Expressions of Interest and/or solicitation process. End Violence Fund also reserves the right to require compliance with additional conditions as and when issuing the final contracting/request for proposals document.

If you have any questions about the Request for Expressions of Interest, please submit questions through this FORM. Answers to all questions submitted will be shared publicly.

## IV. Additional Information

Expressions of Interest will be scored according to the following criteria:

| Criteria | Specific Criteria | Possible Score and Key Data Points |
|---|---|---|
| **MANDATORY CRITERIA** | | |
| **1. Legal registration** | Registered as a legal entity (nonprofit organisation or a private company) | Yes/No |
| **2. Alignment with key objectives** | The proposed solution addresses one or more of the four objectives of the End Violence Fund's 2019 Open Call | Yes/No |
| **3. Safeguarding** | The entity has a Safeguarding Policy and procedures in place (including data privacy) or is willing to develop a policy | Yes/No |
| **4. Builds on existing work** | The proposed solution responds to a clear need/gap, does not duplicate existing tools, and builds upon and/or interacts with existing solutions | Yes/No |
| **5. Existing prototype** | At minimum, an existing prototype of the open-source solution with promising results from initial pilots | Yes/No |
| **SCORING CRITERIA** | | |
| **1. Relevance of solution for tackling online CSEA,** | i. Alignment between problem described and solution proposed | **25 Points**<br>- Is the solution really solving the defined problem? |

| | | |
|---|---|---|
| **problem-solution fit** | ii. Relevance of the solution for tackling online CSEA | - Is the solution / product viable?<br>- How relevant is the project for tackling online CSEA? |
| **2. Novelty of solution and robustness of prototype** | i. Generating open source[3] technology by:<br>• Developing new technology;<br>• Expanding existing technology; or<br>• Developing a new application / use case of existing technology<br>ii. Robustness of the results of initial prototyping/piloting<br>i. Existence of code repository | **25 Points**<br>- Is the project developing / expanding existing open-source technology?<br>- Is the project working on a new application / use case of existing technology?<br>- How thorough are the results from the piloting to date?<br>- Do the initial results indicate that the solution is working/addresses the problem defined?<br>- Github/bitbucket/equivalent link |
| **3. Suitability of the team to implement the project** | i. Alignment of team members' proficiency and experience with skills and time commitment needed to implement project<br>ii. Team is diverse, including across gender<br>iii. Team is primarily composed of individuals with direct local knowledge and connections to the country where the solution is being built and piloted<br>iv. Existence of key advisers filling team's expertise gaps<br>v. Existence of relevant partners | **25 Points**<br>- Does the team have the right skills and experience to implement the project? (inc. technical relevant for the tech product, business strategy, UX, software / hardware, programmatic expertise)<br>- Are local people leading the project? Are they from the country where solution is being developed? If not, does the team have strong local networks showing in-depth understanding of the context and required for implementation of project? |

[3] The Fund will consider occasional exceptions from the open-source rule as justified by the nature and/or sensitivity of the proposed solution.

| | | |
|---|---|---|
| | | - Is there gender diversity in leadership team and in project team?<br><br>- If skills missing in core team, do advisors help fill the gaps? Is this enough?<br><br>- Does the entity have partnerships in place that they need for product development and testing? |
| **4. Alignment between budget ask and project goals** | i. Matching of overall budget ask for Fund investment with main objectives of the project<br><br>ii. Balance of funding sources: entity's own capital contribution to the project (human, capital, assets) and other investments | **25 Points**<br><br>- Is the budget ask consistent with the cost of employing/developing this technology? If the ask is not enough, does the team have enough resources or partners to cover gaps? |
| **TOTAL SCORE** | | **100 Points** |

**More background:**

**Global Partnership to End Violence Against Children**

Acknowledging its devastating impact, in 2015 world leaders committed to end all forms of violence against children by 2030, as part of the Sustainable Development Goals (SDGs). In July 2016, the UN Secretary-General launched the Global Partnership to End Violence Against Children (End Violence), and a Fund to invest in solutions on the ground.

Recognising that we will not solve world's biggest problems working in isolation, the End Violence Partnership represents a new model of delivering change. It includes governments from the global North and South, regional bodies, civil society organisations, UN agencies, private sector, young people, advocates and champions, all focused on one thing – making the world safe for children.

This new model is representative of the very nature of the SDGs and Agenda 2030 – it is universal, it is collaborative, it recognises interdependencies between sectors and actors at global, regional and national level, and it ensures an ability to drive change much more effectively with and through partners.

**The End Violence Fund**

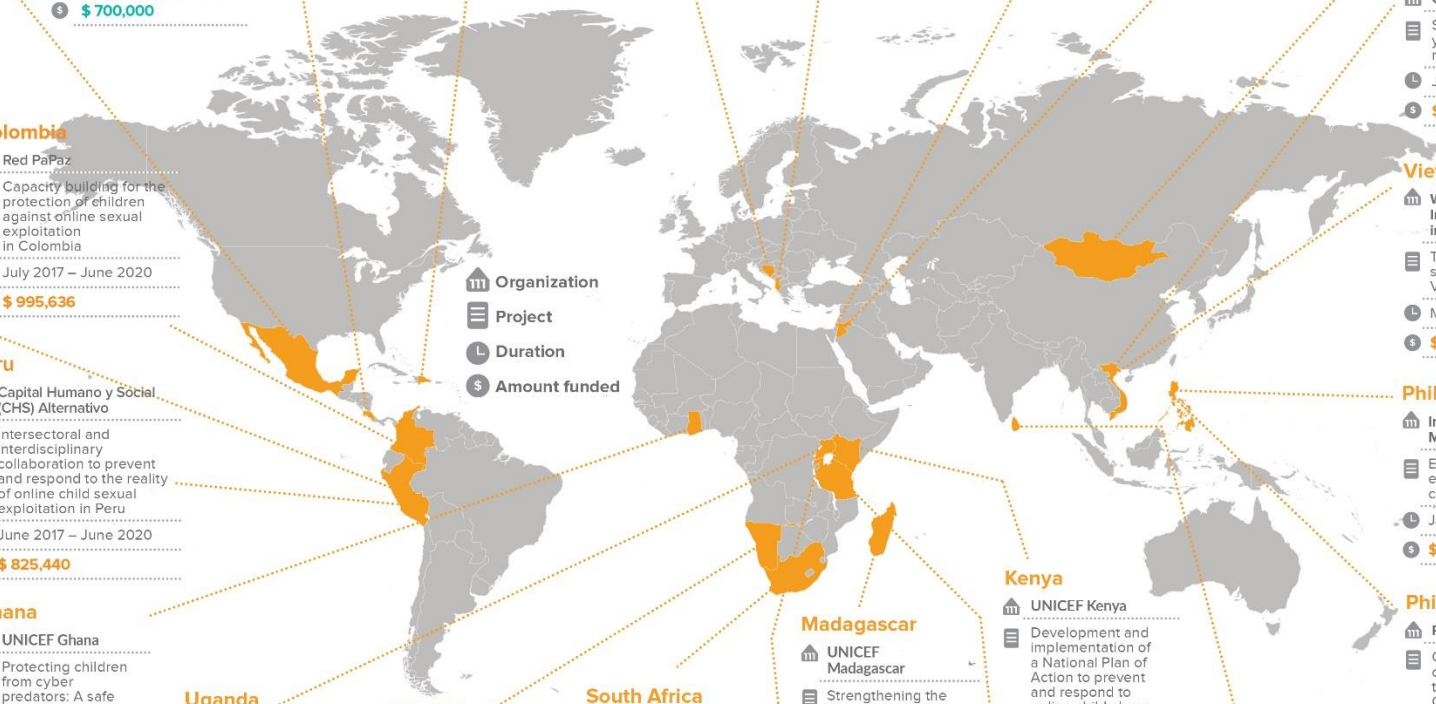
With three years of investing in online child safety and tackling online CSEA, the End Violence Fund has become a leading vehicle for creating solutions to this problem. So far, the Fund has invested $32 million in 37 projects across nearly 30 countries to combat online violence against children by providing financial support to programmes and activities that deliver practical and innovative solutions.

**The Fund's online grant portfolio is included on the following page.**

# ONLINE GRANT PORTFOLIO

**Total Funding Committed**

**$ 32,169,491**




## Mexico
- Oficina de defensoría de los derechos de la infancia
- Effective legal representation of child victims of online sexual exploitation
- Jan. 2017 – Sep. 2019
- $ 317,606

## Peru
- Save the Children Sweden
- Combating online exploitation and sexual abuse of children and adolescents in Peru
- July 2017 – Dec. 2019
- $ 369,147

## Global
- International Centre for Missing & Exploited Children in partnership with Child Helpline International
- Implementing the MNR: collaborative approach to combat CSEA in five countries (Jordan, Kenya, Peru, Philippines, Romania)
- Mar. 2018 - May 2020
- $ 855,406

## Global
- Internet Watch Foundation (IWF)
- IWF reporting portal project for 30 least developed countries (initially Zambia, Tanzania and Mozambique)
- July 2017 – June 2020
- $ 448,875

## Global
- ECPAT International
- Online CSEA-National Assessments-Contextual Research
- Feb. 2019 – Mar. 2021
- $ 2,438,246

## Costa Rica
- PANIAMOR Foundation
- Costa Rica says NO to online child sexual exploitation and abuse
- July 2017 – Dec. 2019
- $ 998,409

## Global
- Thorn
- Bringing Light to the Dark Web
- May. 2018 - Apr. 2021
- $ 700,000

## Colombia
- Red PaPaz
- Capacity building for the protection of children against online sexual exploitation in Colombia
- July 2017 – June 2020
- $ 995,636

## Peru
- Capital Humano y Social (CHS) Alternativo
- Intersectoral and interdisciplinary collaboration to prevent and respond to the reality of online child sexual exploitation in Peru
- June 2017 – June 2020
- $ 825,440

## Ghana
- UNICEF Ghana
- Protecting children from cyber predators: A safe online future for all children in Ghana
- June 2018 - May 2020
- $ 999,380

## Global
- New Venture Fund
- Communication and Advocacy Support for Ignite Philanthropy: Inspiring the End to Violence against Girls and Boys
- Dec. 2018 – Nov 2021
- $ 594,000

## Dominican Republic
- UNICEF DR with PLAN DR
- Protection for every child against sexual exploitation and abuse
- Mar. 2018 - Sept. 2021
- $ 999,312

## Uganda
- UNICEF Uganda
- Children in Uganda are safe online
- Dec. 2016 – Dec. 2020
- $ 977,777

## Global
- INTERPOL
- National Assessments of Online CSEA
- Feb. 2019 – Mar. 2021
- $ 1,675,402

## Namibia
- UNICEF Namibia
- End violence - Tackling online child sexual exploitation and abuse in Namibia
- Dec. 2016 – Dec. 2018
- $ 630,551

## Albania
- UNICEF Albania
- Safer and better internet for children and youth in Albania
- May 2017 – Apr. 2020
- $ 999,915

## South Africa
- UNICEF South Africa
- Strengthening children's online safety in South Africa
- May 2018 - Apr. 2021
- $ 999,615

## Global
- UNICEF Innocenti
- Investigating Online Violence Against Children
- Feb. 2019 – Mar. 2021
- $ 2,462,070

## Bosnia and Herzegovina
- Bosnia and Herzegovina Child Protection Consortium: UNICEF BiH, Save the Children, International Forum of Solidarity (EMMAUS)
- End Violence Against Children: Preventing and tackling online CSEA in Bosnia & Herzegovina
- Feb. 2018 - Jan. 2021
- $ 999,939

## Madagascar
- UNICEF Madagascar
- Strengthening the national protection system to prevent and respond to online child sexual exploitation and abuse in Madagascar
- Mar. 2018 - Jan. 2020
- $ 999,916

## Rwanda
- University of East London
- Rwanda Child Online Protection Policy and Implementation Plan
- Nov. 2018 -July 2019
- $ 186,094

## State of Palestine
- The Palestinian Center for Democracy and Conflict Resolution
- Safe online environment for children
- Mar. 2018 - Feb. 2021
- $ 504,797

## Kenya
- UNICEF Kenya
- Development and implementation of a National Plan of Action to prevent and respond to online child abuse and exploitation
- Mar. 2018 - Feb. 2021
- $994,931

## Tanzania
- UNICEF Tanzania
- Preventing and responding to online CSEA
- Mar. 2018 - Feb. 2021
- $ 952,300

## Jordan
- UNICEF Jordan
- Targeting online sexual exploitation of children in Jordan
- Jan. 2017 – Dec. 2019
- $ 999,380

## Sri Lanka
- Save the Children Denmark
- Developing a National Action Plan tackling the online sexual exploitation of children in Sri Lanka whilst providing remedial act
- Mar. 2018 - Feb. 2020
- $ 417,638

## Mongolia
- UNICEF Mongolia
- Adopting Model National Response in preventing and tackling CSEA in Mongolia
- Mar. 2018 - Feb. 2020
- $ 471,000

## Vietnam
- ChildFund Australia
- Swipe safe: Helping young people make the most of the online world
- July 2017 – June 2020
- $ 513,547

## Vietnam
- World Vision International in Vietnam
- Tackling online child sexual exploitation in Vietnam
- Mar. 2018 - Feb. 2021
- $ 680,951

## Philippines
- International Justice Mission
- Ending online sexual exploitation of children in Cebu
- Jan. 2017 – Dec. 2019
- $ 999,752

## Philippines
- Plan International UK
- Cyber-safe spaces for children and youth in the cities of Manila and Quezon City
- June 2017 – May 2020
- $ 1,000,000

## Regional
- South Asia Initiative to End Violence Against Children
- Strategic response to online child sexual exploitation
- Aug. 2017 – Nov. 2019
- $ 295,695

## Global
- UNICEF Child Protection, Programme Division, UNICEF Headquarters
- UNICEF Global Programme to build capacity to address online child sexual exploitation
- Mar. 2018 - Feb. 2020
- $ 999,430

## Global
- World Health Organization
- What works to prevent and respond to child online abuse
- May 2018 - Apr. 2021
- $ 306,020

## Global
- The Marie Collins Foundation
- The Global Protection Online Network
- Mar. 2019 – Feb. 2022
- $ 839,062

## Regional
- Council of Europe
- End online child sexual exploitation and abuse @Europe (Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Moldova, Montenegro, Serbia, Turkey, Ukraine)
- July 2018 - Dec. 2020
- $ 1,000,000

## Regional
- UNICEF East Asia and Pacific Regional Office (EAPRO)
- Strengthening regional commitment and collaboration to end online child sexual abuse and exploitation in East Asia and the Pacific
- Dec. 2016 – Apr. 2020
- $ 722,250

End Violence Against Children

## ANNEX 1: Online CSEA – the nature, threats and magnitude of the problem

**Online CSEA is a grave and growing problem that requires urgent action**.
One out of every three internet users worldwide is a child. Every day nearly 200,000 children go online for the first time. Their lives are shaped by experiences and interactions that are happening online - friendships, entertainment, learning - which are increasingly governed by commercial interest and engagement rules on platforms that have not been designed with children's interest and safety in mind.

**Any child can become a victim**. Online violence can affect children from all social backgrounds and from any country. Online CSEA is one of the worst manifestations of the failures to ensure children's safety online. It is a growing problem and it needs urgent, collective and global action. Online communities of child abusers are proliferating, many children are coerced or extorted into producing sexualised images or engaging in sexual activities via webcams. Online harm against children, including through the viewing of Child Sexual Abuse Material (CSAM), can be as severe in its impact as abuse committed offline, and in some cases can facilitate the transition to contact abuse. The photos and videos shared on online platforms can harm children for life, and have a direct impact on their development, health and ability to learn and fulfill their full potential.

**The statistics are alarming**. The numbers of violent and sexual images and videos of children uploaded, or live-streamed on the Internet and Dark Web are increasing at an incredible speed. For instance, the number of reported photos and images received by NCMEC (National Center for Missing and Exploited Children) grew nearly tenfold in 3 years, from 1.1 million in 2014 to 10.2 million by 2017, and almost doubled in 2018 with 18.4 million reports received. The Internet Watch Foundation also reports that in 2017 alone, online photos and videos with sexual abuse of children increased 37% compared to 2016.

The Global Threat Assessment conducted by the WePROTECT Global Alliance cited that one many hidden Internet services dedicated to the abuse of infants/toddlers contained over 18,000 registered members, with another similar forum receiving over 23 million visits. Moreover, some studies show that younger children are at higher risk. For instance, the international survivors survey conducted by the Canadian Center for Child Protection indicates that 56% of the abuse began before the age of four, and 42% were abused for more than 10 years. Reports received by the Internet Watch Foundation show that in the United Kingdom half of the reported online CSAM depicts the abuse of children under 10, and one-third of images involve rape and sexual torture.

**How does online CSEA happen? Three possible scenarios:**

1. *An adult takes photos or films sexual acts* involving children with a camera or a smartphone and use them for self-pleasure, sell them for financial gain, share them on online forums with other adults with sexual interest in children, or use them to blackmail the child in exchange of money or sexual favors.

2. *The sexual abuse of a child is live-streamed*. Adults with sexual interest in children do not need to travel, they can sit in their house in front of a computer, tablet or mobile phone and abuse the child for their sexual pleasure. It affects mostly children living in poverty and in most cases an adult well-known to the child facilitates the abuse in exchange for money.

3. *A child takes photos or makes videos with sexual content* and shares it via a mobile phone or the Internet with a peer or with an adult. These self-generated images and videos are often used to intimidate or blackmail the child in exchange of money, favors or to pressure to produce more sexual photos or to have sex in real life. This is commonly referred to as grooming, sexting, sextortion, sexual harassment, revenge porn, etc.

## ANNEX 2: Examples of technology solutions for each objective

| | |
|---|---|
| *Objective 1*: **Detect, remove and refer known and new CSAM, including self-generated CSAM in open and closed online environments and mobile networks** | • expansion and universalisation of hash-based filtering of CSAM<br>• use of crawlers to detect and refer content for removal<br>• Artificial Intelligence (AI) to detect, classify and refer known CSAM<br>• AI to detect conversations and behavior that may indicate (new) CSAM is shared<br>• tools to detect and distinguish between adult and child language and behavior to prevent the self-generation and sharing of CSAM and to refer the child to appropriate guidance or services<br>• establishment or strengthening of reporting mechanism (hotlines or other) for CSAM and/or other forms of online and offline CSEA, with national and international referral channels to facilitate removal and appropriate referral of illegal content |
| *Objective 2*: **Prevent and disrupt online sexual grooming of children in digital environments** | • lexicon-based, machine learning algorithms and text analysis of chat room conversations to detect online sexual grooming<br>• online platforms and games to raise awareness of digital dangers<br>• natural language processing (NLP) chatbots to alert the sites' administrator of the suspected grooming, and/or to pre-empt children if online grooming is suspected and offer real-time support via redirecting the child to appropriate services |
| *Objective 3*: **Prevent and disrupt the live-streaming of child sexual abuse** | • tools to detect, block and/or refer transactions before they occur, for instance via identifying and disrupting patterns of migration from one platform to another e.g. for introductions, online CSEA and payment<br>• tools to disrupt financial transactions and refer victims and/or offenders and potential offenders to appropriate services |

| | |
|---|---|
| | • establishing or strengthening reporting mechanisms to ensure anonymous reporting of known and suspected live-streaming activities |
| *Objective 4*: **Expand tools and services to prevent the victimisation of children and harmful behaviour by offenders and potential offenders in digital environment** | • chatbots, online helplines with instant messaging, AI powered services, etc. to provide services for child victims, and possibly offenders and adults with sexual interest in children<br>• establishment or strengthening of helplines and/or (self) referral mechanisms for offenders and people with a sexual interest in children, including through international exchange of expertise |