



Octopus Project

to support the implementation of the
Convention on Cybercrime and its Protocols

Version 15 December 2025

Cyberviolence in Southeast Asia

A series of webinars for criminal justice authorities

Organised by the Octopus Project¹ of the Council of Europe

in cooperation with Survivors & Tech Solving Image-Based Sexual Abuse (STISA)



16-22 December 2025, online

Outline

Background and justification

Cyberviolence - including non-consensual dissemination of intimate images (NCDII), online child sexual exploitation and abuse (OCSEA), and technology-facilitated trafficking in human beings - is an escalating threat globally, and in Southeast Asia in particular. Criminal justice authorities in the region confront increasingly complex cases involving:

- large volumes of harmful digital content, including deepfakes and extortion-related materials;
- livestreamed exploitation, grooming, and self-generated sexual content among children;
- online recruitment and exploitation linked to human beings trafficking networks, including scam compounds;
- cross-border data flows, jurisdictional fragmentation, and limited fast cooperation channels.

The [Mapping study on cyberviolence](#) by the Council of Europe provides a broad overview of these threats, highlighting the risks posed by ICT-enabled harms, especially against women and children, and identifying good practices to support effective national and international responses.

Complementing this, the [Cyberviolence Resource](#) offers a collection of guidance, case studies, and practical tools to assist criminal justice authorities in tackling cyberviolence effectively.

The Council of Europe through the [Octopus Project](#) builds on these insights to assist countries worldwide in strengthening their national and regional responses, drawing on relevant international standards and good practices, including those developed under the [Convention on Cybercrime](#) (Budapest Convention) and its expedited tools for access to electronic evidence.

¹ With the financial support of the Government of Japan

In order to address the challenges faced by the countries from the region and for enhancing their response to cyberviolence three webinars will be organised under the Octopus project targeting criminal justice actors.

Expected outcomes

The three webinars are expected to:

- increase the knowledge of participants on the legal, procedural, and operational approaches to addressing cyberviolence;
- facilitate the sharing of practical experiences of criminal justice authorities and partners in Southeast Asia and beyond;
- enhance the cooperation with online service providers, regional bodies, and international partners;
- identify capacity-building needs for effective criminal justice response in Southeast Asia.

Participants

The event is open to criminal justice authorities from Southeast Asian countries (prosecutors, police, judges), specialised cybercrime units, relevant government agencies and regional/international partners.

Administrative arrangements

The webinars will take place online via Zoom platform. The webinar will be held in English, the discussion will be recorded and hosted on [CYBOX platform](#).

Calendar of implementation:

Month	Topic
16 December 2025	Webinar on non-consensual dissemination of intimate images
09:00 - 10:30 CET	Register here
16:00 - 17:30 Philippines, Malaysia, Singapore	With digital communication becoming central to relationships across all age groups, the consensual sharing of intimate images has grown more common. However, alongside this shift, cases of the non-consensual dissemination of intimate images (NCDII) have risen sharply, disproportionately impacting women and girls. While often termed “sextortion”, NCDII covers different types of conduct that is primarily a violation of privacy rights.
15:00 - 16:30 Indonesia (Jakarta)	While several countries have made notable strides in strengthening laws and policies to combat NCDII, gaps remain, particularly in ensuring swift action by service providers to remove harmful content and prevent revictimization, and by criminal justice authorities to investigate such offences.
15:00 - 16:30 Thailand, Cambodia, Laos, Vietnam	The purpose of this workshop is to identify and promote evidence-based good practices for addressing NCDII, focusing on legislative frameworks, investigative challenges, and strategies for public-private cooperation in content removal and survivor support.

18 December 2025 09:00 - 10:30 CET 16:00 - 17:30 Philippines, Malaysia, Singapore 15:00 - 16:30 Indonesia (Jakarta) 15:00 - 16:30 Thailand, Cambodia, Laos, Vietnam	Livestreamed child sexual exploitation and abuse Register here Livestreaming of child sexual abuse has become one of the most urgent and complex OCSEA challenges in Southeast Asia. Unlike traditional CSAM, livestreamed abuse often leaves little to no visual record because the content is created, viewed, and erased in real time. These cases often involve cross-border offenders, communications across platforms, and children who may not understand the nature of the abuse, making identification and timely intervention extremely difficult. For investigators and prosecutors in Southeast Asia, livestreaming presents additional operational barriers. Evidence may disappear within seconds unless captured at the time of the offence, and investigators must rely heavily on metadata, CyberTipline reports, platform logs, and emergency preservation requests. This webinar will explore how livestreaming is used to facilitate online child sexual exploitation and abuse in Southeast Asia, and what criminal justice authorities can do to detect, investigate, and respond to these real-time offences
22 December 2025 09:00 - 10:30 CET 16:00 - 17:30 Philippines, Malaysia, Singapore 15:00 - 16:30 Indonesia (Jakarta) 15:00 - 16:30 Thailand, Cambodia, Laos, Vietnam	Technology facilitated trafficking in human beings Register here Technology-facilitated trafficking linked to scam compounds represents a significant dimension of cyberviolence, where technology is used not only to recruit and control victims but also to facilitate large-scale, digitally enabled harm. It poses major challenges for criminal justice authorities in Southeast Asia and globally, who must respond to crimes that are organised online, executed across borders, and supported by sophisticated digital infrastructures. Addressing these cases requires rapid preservation of digital evidence, coordinated cross-border information sharing, and the ability to act on intelligence originating from victims, platforms, embassies, or international partners. This webinar will discuss approaches for dismantling technology-enabled trafficking networks linked to scam compounds, improving digital evidence handling, and enhancing cross-border cooperation while ensuring that victim identification, protection, and safe recovery remain central to every stage of the response.

Contacts

At the Council of Europe:

Nina LICHTNER
Project Manager
Octopus Project
Cybercrime Programme Office of the
Council of Europe (C-PROC)
Strasbourg, FRANCE
Nina.LICHTNER@coe.int

Irina DREXLER
Senior Project Officer
Octopus Project
Cybercrime Programme Office of
the Council of Europe (C-PROC)
Bucharest, Romania
Irina.DREXLER@coe.int