CO-OPERATION ON CYBERCRIME & ELECTRONIC EVIDENCE

OCTOPUS CONFERENCE

Strasbourg, 14-16 October 2026

Public version 24 September 2026

Focus: 25th Anniversary of the Budapest Convention

Main sessions

- 25 years of the Budapest Convention: lessons from implementation and the road ahead
- Cybercrime-as-a-service: impact of AI
- Trafficking and scam compounds: threat to national security?
- Interplay between 2nd Additional Protocol and EU e-evidence package: cooperation with online service providers

Workshops and other sessions

- Disinformation and foreign manipulation: responding to cyber interference
- Transnational repression and international cooperation: safeguarding cybercrime frameworks
- Prosecuting cyber-enabled international crimes
- Denudification, AI-generated CSAM and NCDII: accountability across the digital ecosystem
- Illegal use of virtual assets: cooperation with VASPs
- Regional workshops for Africa, Americas, Asia, Pacific and Caribbean
- Lightning talks

Participation and registration

The conference will provide an opportunity to interface for cybercrime experts from public and private sectors as well as international and non-governmental organisations from all over the world. High-level interventions are envisaged. Participation is subject to registration and is free of charge.

Registration will be open from **1 May till 31 August 2026** at www.coe.int/Octopus2026.

The Conference will be preceded by:

- Plenary of the Cybercrime Convention Committee (T-CY) on **12 – 13 October 2026**. Participation in the T-CY plenary is restricted.

Side events:

- Treaty event on 14 October 2026
- Meeting of the 24/7 Network established under the Budapest Convention [restricted meeting on 15 October 2026]

Administrative arrangements

The Conference will be held at the Council of Europe in Strasbourg, France. Working languages will be English, French and Spanish.

The conference will also include an area where projects, partners and other initiatives will have the possibility to showcase their work. Should you wish to do so, please reach out to the Conference secretariat.

Contact

For any question please contact:

Cybercrime Programme Office of the Council of Europe, Bucharest, Romania
Tel +33-3-8841-2175
Email cybercrime.events@coe.int

The Octopus Conference is part of the Octopus Project which is currently funded by voluntary contributions. It is supported by other C-PROC projects as well.

www.coe.int/cybercrime

Présidence de / Presidency of MONACO
Conseil de l'Europe / Council of Europe
05/2026 - 11/2026

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Programme overview

<table>
<tr><th colspan="3">DAY 1 – 14 OCTOBER 2026</th></tr>
<tr><td>8h00-9h00</td><td colspan="2">Welcome coffee and registration</td></tr>
<tr><td>9h00-12h00

Coffee break
10h30-11h00</td><td colspan="2">Opening Plenary: 25 years of the Budapest Convention: lessons from implementation and the road ahead
EN/FR/ES
[livestream, recording]

This anniversary panel reflects on 25 years of practical experience with the Budapest Convention, focusing on what has enabled the Convention to remain operational and relevant across evolving technological and geopolitical contexts. Drawing on lessons from implementation, international cooperation, and practitioner use, the panel looks ahead to how the framework continues to evolve, including through the Second Additional Protocol, to address challenges in accessing electronic evidence and strengthening cooperation. The discussion offers forward-looking insights into how international cybercrime frameworks can remain effective, trusted, and adaptable over time.

• Opening [9h00 – 9h30]
• 25 years of impact of the Budapest Convention on cybercrime [9h30-10h00]
• How international cybercrime framework can remain effective, trusted and adaptable over time [10h00-10h30]
• Way forward – what next? [11h00-11h50]
• Introduction of the Protocol on asset recovery [11h50-12h00]</td></tr>
<tr><td>12h00 – 14h00</td><td colspan="2">Group photo and lunch break</td></tr>
<tr><td>12h15 - 13h15</td><td colspan="2">Treaty event and signing ceremony</td></tr>
<tr><td>14h00 – 17h30

Coffee break
15h30-16h00</td><td>Main session 1: Interplay between the 2nd Additional Protocol and EU e-evidence package: cooperation with online service providers

[14:00-17:30] Hemicycle, EN/FR/ES
[livestream, recording]

The Second Additional Protocol to the Budapest Convention and the EU e-Evidence package are reshaping how electronic evidence is obtained across borders, placing service providers at the centre of new cooperation models. This session examines what these instruments mean in practice for law enforcement authorities, judicial bodies, and</td><td>Workshop 1: Disinformation and foreign manipulation: responding to cyber interference
[14:00-15:30], Room 1, EN/FR/ES
[livestream, recording]

Disinformation and foreign manipulation increasingly take the form of cyber interference. The session examines how existing tools and cooperation mechanisms can be used to identify, investigate, and disrupt the digital enablers of interference, while respecting safeguards and freedom of expression. The discussion also takes account of ongoing Council of Europe work on democratic resilience highlighting how criminal justice responses can complement broader policy, regulatory, and resilience-building approaches.</td></tr>
</table>

	providers, and where expectations, obligations, and safeguards intersect.	**Workshops 2,3,4,5: Regional workshops** [16:00-17:30] WS 2 Americas [EN/ES] Room 1 WS 3 Africa [EN/FR]| Room 2 WS 4 Asia [EN] Room 3 WS 5 Pacific and Caribbean [EN] Room 6
17h45 – 20h00	**Evening reception** Foyer of the hemicycle	
DAY 2 – 15 OCTOBER 2026		
08h00 – 09h00	*Registration*	
09h00-17h30	**Side event: Meeting of the 24/7 POC Network under the Budapest Convention** *Room 9 _[restricted, upon invitation]* EN	
9h00 – 12:30 Coffee break [10:30-11:00]	**Main session 2: Trafficking and scam compounds: threat to national security?** [9:00-12:30] **Hemicycle**, EN/FR/ES [livestream, recording] Large-scale online scams are no longer just a cybercrime problem. Increasingly, they are run by organised crime groups that rely on victims working in purpose-built scam compounds, generating enormous criminal profits and causing widespread social harm. This session explores how these operations are evolving into a broader security threat, with growing links to corruption, regional instability, and other forms of serious crime. Drawing on the outcomes of the 2025 Octopus Conference, the session will explore at what point does scam centres stop being a crime problem and start being a security problem and how does that distinction change how the international community responds.	**Workshop 6: Transnational repression: safeguarding cybercrime and e-evidence frameworks** [9:00-10:30] Room 1, EN/FR/ES This session examines how transnational repression intersects criminal investigations and cooperation frameworks, focusing on the responsible application of safeguards under the Budapest Convention. It highlights the role of proportionality, informed decision-making, and trust-based cooperation in ensuring that cybercrime and e-evidence tools are not misused in ways that undermine human rights or the integrity of international cooperation **Workshop 7: Nudification, AI-generated CSAM and NCDII: accountability across the digital ecosystem** [11:00-12:30] Room 1, EN/FR/ES Advances in generative technologies are enabling new forms of non-consensual image abuse (NCDII), including AI-generated CSAM and nudification tools that create fake nude images of real people. This session focuses on practical responses across the digital ecosystem - platforms, developers, service providers, and criminal justice authorities - to prevent, detect, and address these harms. Participants will examine concrete tools and measures for platform accountability, rapid removal and reporting mechanisms, victim support, cross-border cooperation, and proportionate safeguards.
12h30-14h00	*Lunch break*	

14h00 – 17h30 Coffee break [15:30-16:00]	**Main session 3: Cybercrime-as-a-service: impact of AI** [14:00-17:30] **Hemicycle** EN/FR/ES [livestream, recording] Artificial intelligence is rapidly transforming the cybercrime ecosystem, lowering barriers to entry and amplifying the reach of crime-as-a-service models. From automated phishing and social engineering to AI-assisted malware, deepfake fraud, and large-scale scam operations, generative tools are enabling more sophisticated and scalable criminal services. This session examines how AI is reshaping the structure, speed, and economics of cybercrime, and what this means for investigations, attribution, and international cooperation. Focusing on practical responses, participants will discuss how existing legal frameworks and investigative tools can be applied to AI-driven crime-as-a-service, where new gaps are emerging, and which operational and capacity-building measures can help disrupt these evolving business models.	**Workshop 8: Prosecuting cyber-enabled international crimes** [14:00-15:30] Room 1 EN/FR/ES [livestream, recording] Cyber operations are increasingly used to facilitate serious international crimes, including crime of aggression, war crimes and crimes against humanity, raising new questions for accountability and prosecution. This workshop explores how international criminal law and emerging policy frameworks - including the International Criminal Court's policy - can be applied to the investigation and prosecution of international crimes. Attribution and accountability are key solutions but remain also key challenges. **Workshop 9: Illegal use of virtual assets: cooperation with VASPs** [16:00-17:30] Room 1 EN/FR/ES [livestream, recording] Virtual assets are now central to many forms of cybercrime, Virtual assets are now central to many forms of cybercrime, making effective cooperation with Virtual Asset Service Providers (VASPs) essential for successful investigations. This workshop focuses on the practical realities of obtaining evidence, tracing transactions, preserving data, and freezing or seizing virtual assets through engagement with VASPs. Participants will discuss legal bases, procedural challenges, and differing national approaches and practices for timely and rights-respecting cooperation. The discussion will also take into account the T-CY's recently adopted Mapping study on virtual assets and the relevance of the Convention on Cybercrime and its Second Protocol, which confirms the continued relevance of the Budapest Convention framework for investigations, international co-operation and access to electronic evidence. The session aims to identify concrete steps to improve clarity, speed, and mutual trust between criminal justice authorities and VASPs.
17:30	***End of Day 2***	

DAY 3 – 16 OCTOBER 2026	
08h00 - 09h00	*Registration*
09h00 – 13h00	**Closing Plenary – Outlook for 2027-2028** **Hemicycle** EN/FR/ES [livestream, recording] - Lightning talks (youth and cybercrime, etc) - Key takeaways (reports from MS and WS) - Responses and capacity building on cybercrime: outlook for 2027-2028 - Keynote speeches - Conclusions
13h00	***End of the event***