

KEY TAKEAWAYS

14-16 October 2026 | Strasbourg, France

We hope you enjoyed last week's Octopus Cybercrime Conference. We certainly enjoyed hosting you all and had many meaningful conversations. It was a truly global gathering, with nearly **500 participants** from **106 countries** travelling to be there in person, with many more joining our livestream sessions.

The Conference was opened by Alain Berset (Secretary General of the Council of Europe), Samuel Vuelta Simon, Secretary of State for Justice, Monaco, Caroline Simard, Commissioner of Canada Elections and Parinda Ranasinghe, Attorney General, Sri Lanka. We came together to celebrate the **25th anniversary of the Convention on Cybercrime (Budapest Convention)**, the world's leading cybercrime instrument. We thank the vision and leadership of the original drafters and commit to carrying that passion forward for the next 25 years and beyond.

Our shared mission, to help countries fight cybercrime across borders in a manner which is consistent with human rights, democracy and the rule of law, is as valid today, as it was in 2001.

We want to thank each and every one of you for investing your valuable time to come to the Octopus Conference and connect with each other and with us. We are stronger together as a community, and we hope your connections will carry you forward with individual cases and collective challenges.

This was the **16th Octopus Conference on Cybercrime**. We hope to see you in spring 2028 for the next one.

KEY MESSAGES

01 Interplay between the 2nd Additional Protocol (2AP) and EU e-evidence package

The 2AP modernises international co-operation and fills important gaps in existing legal frameworks, while providing a suitable, safeguarded basis for co-operation that preserves national control: orders are not enforced without the involvement of national authorities, and making the Protocol effective requires ongoing implementation and trusted co-operation between national authorities and service providers.

02 Scam compounds

Scam compounds are simultaneously a trafficking problem, an organised-crime problem, a cybercrime problem, a corruption problem and a financial-crime problem. The effectiveness of the response depends on whether institutions accustomed to treating those problems separately can begin to address them together. In many countries, the problem has reached the threshold of being a threat to national security.



03 Cybercrime-as-a-service: impact of AI

AI is accelerating cybercrime-as-a-service, helping criminals reach more victims, personalise deception and operate faster. The **T-CY Mapping Study** confirms that the Budapest Convention remains broadly applicable to cases involving AI. Practical action includes disrupting criminal services and obtaining electronic evidence across borders. Closer co-operation with service providers and relevant actors in the AI sector should be encouraged, with applicable safeguards respected. Looking ahead, the evolving capabilities of AI agents may warrant further examination of the challenges they pose for criminal justice, in particular the issue of criminal liability for agentic AI.

04 Disinformation and foreign manipulation: responding to cyber interference

Democracy around the world is under contact attacks, with disinformation and foreign manipulation increasingly take the form of cyber interference in elections, referenda, and general public discourse surrounding democracy. Democratic resilience is one of the defining concepts, based on the rule of law, that enables states and societies to employ tools and co-operation mechanisms can be used to identify, investigate, and disrupt the digital enablers of interference, while respecting safeguards and freedom of expression. Recently initiated work of the Council of Europe on putting forward a legal instrument on foreign interference and manipulation is based on the framework of already existing and applicable standards, including the Convention on Cybercrime. Co-operation between public authorities and private entities, including civil society, is crucial to ensure democratic resilience.

05 Transnational repression: safeguarding cybercrime and e-evidence frameworks

International co-operation must be protected from misuse for transnational repression. Effective implementation of the conditions and safeguards under the Budapest Convention is essential to that effort. Even a formally valid request for electronic evidence may warrant closer scrutiny when credible concerns arise about its purpose, the breadth of the data sought or the people it could put at risk. Authorities need reliable information to make informed, proportionate decisions about whether and what data to share. **Service providers, civil society and other stakeholders play a crucial role in identifying and helping to address risks of misuse.** Putting these safeguards into practice, supported by co-operation among relevant stakeholders, helps prevent misuse for transnational repression and builds the trust needed for effective international co-operation.

06 Nudification, AI-generated CSAM and NCDII: accountability across the digital ecosystem

Nudification tools harm victims of all ages, and these crimes have serious consequences in their real lives, from shame and stigma to self-harm and violence. Most countries criminalise AI-generated CSAM depicting a real child, in line with international standards such as the Lanzarote, Budapest and Hanoi Conventions, while the legal position for adult victims remains uneven, which hampers detection, takedown and prosecution. Responses should also target access to these tools and the services that sustain them, through domain takedowns, action by payment providers and limits on how they are promoted. Recent cases show that coordinated action across borders, supported by prompt evidence sharing under existing co-operation instruments, delivers results. Platforms should pair safety by design with fast, accessible reporting and removal, while all measures remain proportionate and keep victims' access to swift redress at their centre.

07 Prosecuting cyber-enabled international crimes

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. Public international law is still catching up with developments in this area. Nevertheless, existing 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.

08 Illegal use of virtual assets: co-operation with VASPs

Effective investigations into virtual assets require more than the ability to trace transactions. They depend on making better use of existing legal frameworks, acting quickly across jurisdictions, obtaining reliable evidence through co-operation with VASPs and ensuring that criminal assets can be frozen, seized and confiscated where legally justified. The key challenge is to turn technological capabilities into timely, legally sound operational results through trusted public-private partnerships and effective international co-operation.

09 Lightning Talks

We need early-in-career academics and civil society practitioners to help us understand emerging challenges and trends. Their voices are crucial to ensuring that policy makers and criminal justice professionals are keeping abreast of changing environments and taking an active role in integrating intergenerational voices in legislative responses. In addition, our defence legal community are absolutely crucial actors in the fight against improper State actions, and we are all indebted to their vigilance to ensure human rights are vindicated, even in the most difficult of criminal cases.