OCTOPUS CONFERENCE ON CYBERCRIME 2025

4 – 6 JUNE 2025 – STRASBOURG, FRANCE

Version 26 March 2025

The Conference is organised in cooperation with the **Presidency of Malta in the Committee of Ministers of the Council of Europe**, May – November 2025

Programme overview

<table>
<tr><th></th><th>AM</th><th>PM</th></tr>
<tr><td>Wed 4 June</td><td>Opening Plenary (9h00 – 12h30)
Hemicycle | EN/FR/ES

- Opening
- Cybercrime and e-evidence: global perspectives
- Update: implementation of the Convention on Cybercrime and its Protocols
- International treaties on cybercrime: “Hanoi” and “Budapest” Conventions.</td><td>Main session 1 (14h00 – 17h30)
Hemicycle | EN/FR/ES

► E-evidence: implementing the second protocol

WS 1
(14h00 – 15h30)
Room 11, EN/FR/ES

► Youth and cybercrime

WS 2
(16h00 – 17h30)
Room 11, EN/FR/ES

► Cyberviolence: NCDII</td></tr>
<tr><td>Thu, 5 June</td><td>Main session 2 (9h00 –12h30)
Hemicycle | EN/FR/ES

► Cyber-interference with democracy

WS 3 (9h00-10h30)
Room 11, EN/FR/ES

► Crypto-investigations

WS 4 | 5 | 6 | 7
(11h00-12h30)
Room 11, EN/ES
R10, EN/FR
R3, no interpretation
R2, no interpretation

► Regional Africa, Americas, Asia, Pacific</td><td>Main session 3 (14h00 – 17h30)
Hemicycle | EN/FR/ES

► Pig-butchering/romance scams

WS 8
(14h00 – 15h30)
Room 11, EN/FR/ES

► Cyberviolence: CSAM

WS 9
(16h00 – 17h30)
Room 11, EN/FR/ES

► Cybercrime as war crime?</td></tr>
<tr><td>Fri, 6 June</td><td>Main session 4 (9h00 – 12h00)
Hemicycle | EN/FR/ES

► Cybercrime, e-evidence and AI</td><td>Concluding plenary (12h15 – 13h30)
Hemicycle | EN/FR/ES

► Concluding panel: the way ahead</td></tr>
<tr><td></td><td>13h30 End of the conference</td><td>14h30 C-PROC project steering committees</td></tr>
</table>

www.coe.int/cybercrime

Presidency of Malta
Council of Europe
May - November 2025

Présidence de Malte
Conseil de l'Europe
Mai - Novembre 2025

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Detailed Programme

Wednesday, 4 June 2025	
9h00-12h30	**Opening plenary** Location: Hemicycle Languages: EN/FR/ES Purpose: This plenary session is designed to set the scene for subsequent conference sessions and exchanges between participants. Moderator: Alexander Seger, Head of Cybercrime Division, Council of Europe Secretariat: Nina Lichtner, Octopus Project Manager, Council of Europe ► **Opening** ▪ Minister of Justice of Malta, Presidency of the Committee of Ministers of the Council of Europe ▪ Alain Berset, Secretary General of the Council of Europe ► **Cybercrime and electronic evidence: global perspectives** ► **Update: Global state of cybercrime legislation and implementation of the Convention on Cybercrime and its Protocols** ► **International treaties on cybercrime: the new United Nations Convention Against Cybercrime ("Hanoi Convention") and its links to the Convention on Cybercrime ("Budapest Convention")** ► **Conclusions**
Coffee break 10h30-11h00	
12h30-14h00	Group photo (Hemicycle) and lunch break
14h00-17h30 Break 15h30-16h00	**Main session 1 – E-evidence: Implementing the Second Protocol to the Convention on Cybercrime** Location: Hemicycle Languages: EN/FR/ES Purpose: The Second Additional Protocol to the Convention on Cybercrime (2AP) provides solutions to challenges faced by criminal justice authorities regarding the disclosure of electronic evidence across borders. Opened for signature in 2022, many Parties to the Convention on Cybercrime are now in the process of implementing this Protocol in domestic law prior to ratification. The purpose of this session is to explore the expectations and benefits of this Protocol from the perspectives of (a) criminal justice practitioners and (b) private sector entities,

	that is, service providers in particular. It will furthermore provide examples of how governments go about implementing this Protocol in domestic law. ► **Introduction to the session and to the Second Protocol** ► **Use cases: Obtaining the disclosure of electronic evidence now and in the future under the 2AP** ► **Expectations** ► **Towards implementation and ratification of the Second Protocol** ► **Conclusions**
14h00-15h30	**Workshop 1 – Youth and cybercrime: engagement, challenges and solutions** Location: Room 11 Languages: EN/FR/ES Purpose: Young people are both key actors and vulnerable groups in the digital space, making their engagement crucial in addressing cybercrime. This workshop aims to provide a platform for youth representatives from diverse regions to share their perspectives on cybercrime challenges and expectations from law enforcement, private sector actors, and policy responses. By fostering dialogue between youth, experts, policymakers, and industry representatives, this session will identify priorities for youth engagement, discuss digital rights and responsibilities, and explore strategies to enhance youth involvement in cybercrime prevention and response. ► **Introduction and objective of the workshop + results of the survey and winners of the competition** ► **Keynote speech** ► **Youth and cybercrime: risks, responsibilities, and threats** ► **Protecting youth from cybercrime: the role of law enforcement and the private sector** ► **Conclusions**
16h00-17h30	**Workshop 2 – Cyberviolence: non-consensual dissemination of intimate images (NCDII)** Location: Room 11 Languages: EN/FR/ES Purpose: 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 “sextorsion”, NCDII covers different types of conduct that is primarily a violation of privacy rights.

	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. NCDII is to be made a criminal offence under Article 5 of the EU Directive on combating violence against women and domestic violence of 2024. And under Article 15 of the new UN Convention against Cybercrime. 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 ► **Introduction and objective of the workshop** ► **Strengthening responses to NCDII** ► **What strategies, policies and measures to counter NCDII?** ► **Conclusions**
17h45- 20h00	► **Evening reception**
Thursday, 5 June 2025	
9h00-12h30 Coffee break 10h30-11h00	**Main session 2 – Cyber interference with democracy** Location: Hemicycle Languages: EN/FR/ES Purpose: "Cyber interference with democracy" refers to the use of information and communication technologies to manipulate or undermine democratic institutions, processes, or public trust in governance. Elections are at the core of democracy. Interference with elections through malicious cyber activities undermines free, fair and clean elections and trust. It may target computers and data used as well as officials and candidates participating in elections and election campaigns, and involve information operations, the misuse of social media, evading transparency, circumventing rules on elections and political finances, and other activities. Such threats have been experienced in particular since 2014. In 2019, the Cybercrime Convention Committee (T-CY) adopted a Guidance Note on election interference with a focus on criminal law aspects. In 2024/2025, the challenge of cyber interference compromising elections has again come to the forefront in multiple countries. The purpose of this session is to identify: - the different types of malicious actions and actors involved in cyber interference with democracy; - the rules and laws that are being violated; - the measures needed to prevent and respond to such cyber interference in accordance with principles of human rights, democracy and the rule of law. ► **Introduction and objective of the session: about cyber interference with democracy** ► **Cyber interference with democracy – actions and actors**

	► **Preventing and responding to cyber interference with democracy** ► **Conclusions**
9h00-10h30	**Workshop 3 – Crypto-investigations: application of the Convention on Cybercrime and the Second Protocol** Location: Room 11 Languages: EN/FR/ES Purpose: The rise of digital assets is reshaping global finance. Virtual Asset Service Providers (VASPs) play a crucial role in this respect. They facilitate the exchange, transaction, and storage of virtual assets, fostering innovation and financial inclusion. However, virtual assets are also exploited for criminal activities such as fraud, ransomware payments, money laundering and financing of terrorism due to their decentralized and borderless nature. Enhancing cooperation among criminal justice authorities, financial intelligence units (FIUs) and VASPs across borders is crucial for effective investigations. The question to be addressed by this workshop is how international treaties such as the Convention on Cybercrime with its Protocols, can be used to investigate the criminal use of virtual assets and for international cooperation and cooperation between criminal justice authorities and VASPs. In 2024, therefore, the Cybercrime Convention Committee (T-CY) decided to undertake an exercise to map current practices related to virtual assets and in particular the relevance of the Convention on Cybercrime and its Second Protocol in this context. This workshop will thus also feed into the work of the T-CY. ► **Introduction and objective of the workshop** ► **Setting the scene** ► **Use of investigative powers to obtain data from VASPs** ► **Conclusions**
11h00-12h30	**Workshop 4 – Regional workshop for Africa** Location: Room 10 Languages: EN/FR/ES Purpose: Regional workshop will focus on priority topics identified in coordination with hub countries under C-PROC capacity building projects, addressing key challenges and opportunities specific to the region
11h00-12h30	**Workshop 5 – Regional workshop for Americas** Location: Room 11 Languages: EN/ES

	Purpose: Regional workshop will focus on priority topics identified in coordination with hub countries under C-PROC capacity building projects, addressing key challenges and opportunities specific to the region
11h00-12h30	**Workshop 6 – Regional workshop for Asia** Location: Room 3 Languages: EN Purpose: Regional workshop will focus on priority topics identified in coordination with hub countries under C-PROC capacity building projects, addressing key challenges and opportunities specific to the region
11h00-12h30	**Workshop 7 – Regional workshop for Pacific** Location: Room 2 Languages: EN Purpose: Regional workshop will focus on priority topics identified in coordination with hub countries under C-PROC capacity building projects, addressing key challenges and opportunities specific to the region
12h30-14h00	Lunch break
14h00-17h30 Coffee break 15h30-16h00	**Main session 3 - Pig-butchering/romance scams** Location: Hemicycle Languages: EN/FR/ES Purpose: The growth so-called “pig-butchering” scams has become a complex form of fraud with global impact that combines traditional romance scams with virtual asset-based investment schemes. Originating primarily in Southeast Asia, these scams involve perpetrators cultivating deceptive relationships with victims over extended periods, ultimately persuading them to invest substantial amounts of money, often in the form of virtual assets. According to Crypto Scam Revenue 2024 Report[1], the phenomenon has evolved to diversify their business model beyond the “long con” of pig butchering scams to quicker turnaround employment or work-from-home scams that typically yield smaller victim deposits and from small schemes to scam camps, using human trafficking networks. With billions of Euros lost annually and significant impact on victims worldwide, it is crucial for criminal justice authorities and financial institutions to understand both the modi operandi and criminal infrastructure of perpetrators, and the legal and law enforcement tools available to investigate these forms of crime and to seize the related virtual assets. Therefore, the purpose of this session is to examine the main types of scams and their impact, and in particular criminal justice responses in terms of

[1] https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/

	investigation strategies, follow-the-money-approaches, and domestic and international cooperation between criminal justice authorities, financial intelligence units (FIU) and Virtual Asset Service Providers (VASP). The relevance of frameworks such as the Convention on Cybercrime in this connection will also be discussed. ► **Introduction and objective of the workshop** ► **Typologies and modus operandi of pig-butchering/romance scams** ► **Strategies for investigations** ► **Avenues for international and public/private cooperation** ► **Conclusions**
14h00-15h30	**Workshop 8 – Cyberviolence: Child sexual exploitation and abuse materials (CSAM) in the era of artificial intelligence** Location: Room 11 Languages: EN/FR/ES Purpose: The rapid advancement of artificial intelligence is reshaping the landscape of online child exploitation and abuse. AI-generated CSAM presents a growing challenge for criminal justice systems, as synthetic content can be used to evade detection, obscure the identity of offenders, and complicate victim identification. This workshop will explore how investigators, prosecutors, judges and policymakers can adapt to this evolving threat by addressing legislative gaps, strengthening investigative techniques, and enhancing international cooperation. Experts will discuss strategies for identifying, prosecuting, and preventing AI-generated CSAM while ensuring that justice systems remain effective in distinguishing between AI generated and real-victim content. ► **Introduction and objective of the workshop** ► **Setting the scene: case study** ► **Challenges for investigation and prosecution** ► **Conclusions**
16h00-17h30	**Workshop 9 – Cybercrime as war crime?** Location: Room 11 Languages: EN/FR/ES Purpose: Armed conflict may be accompanied by cyberattacks and cybercrime as experienced by Georgia in 2008 and by Ukraine since 2014, and these could be equally destructive and impactful as kinetic attacks. This raises the question of whether and under what conditions such cyberattacks and -crime could amount to war crime or other international crimes covered by domestic law or under the Rome Statute. In March 2025, the Office of the Prosecutor at the International Criminal Court published a "draft policy on cyber-enabled crimes under the

	Rome Statute" which also helps frame this workshop.[2] Against this background, the purpose of this session is to identify: - examples of cyberattacks and cybercrime that may represent underlying crimes or that may aid the commission of war crimes (and other international crimes) - the conditions and criteria to be met to prosecute cyberattacks and cybercrime as war crimes (and other international crimes) - obstacles encountered and possible solutions to prosecute such crimes in domestic and international courts. ► **Introduction and objective of the session** ► **Perspectives** ▪ "Cyber-enabled crimes under the Rome Statute" ▪ The Tallinn Manual: emerging standards and principles ▪ A look at the battlefield: perspective from Ukraine ► **Discussion** ► **Conclusions by rapporteur**
Friday, 6 June 2025	
9h00-12h15 Coffee break 10h20-10h40	**Main session 4 – Cybercrime, e-evidence and AI** Location: Hemicycle Languages: EN/FR/ES Purpose: Artificial intelligence (AI) is reshaping cybercrime, both in terms of the threats it enables and in the opportunities to investigate crime and collect electronic evidence. AI-powered tools allow cybercriminals to carry out more sophisticated and large-scale attacks, such as automated phishing campaigns that dynamically adapt to individual targets. On the other hand, AI is enhancing capabilities for the detection, prevention and prosecution of cybercrime and the collection of electronic evidence. Machine learning algorithms can analyse massive amounts of data to detect threats and extract evidence. The question is to what extent current domestic and international legal frameworks (including the Convention on Cybercrime) are applicable to AI in terms of (a) offences, (b) procedural powers to investigate crime and collect electronic evidence, and (c) international cooperation. In December 2024, the Cybercrime Convention Committee (T-CY), therefore, established a working group tasked to explore this question in the form of a mapping study. This session of the Octopus Conference will feed into the work of the T-CY Working Group on AI. The purpose of this session is to: - Exchange views on underlying concepts regarding AI, cybercrime and e-evidence

[2] Note: Any crime, including war crime or other international crimes may involve evidence on computer systems (electronic evidence) to which the procedural powers and international cooperation provisions of the Convention on Cybercrime and its Second Protocol apply

	- Provide an update – with examples – of offences committed against, by and by means of AI systems - Identify legal and practical challenges to the use of AI for the collection of e-evidence and international cooperation. ► **Introduction and objective of the session** ► **The dark side of AI: offences against, by and by means of AI systems** ► **The bright side of AI: leveraging AI for investigations, the collection of electronic evidence and international cooperation** ► **Conclusions by moderator or rapporteur**
12h30-13h30	**Closing plenary and conclusions** Location: Hemicycle Languages: EN/FR/ES Moderator: Gianluca Esposito, Director General of Human Rights and Legal Affairs, Council of Europe ► **Key takeaways from workshops** ► **Outlook for 2025/6** ► **Conclusions**
13h30	End of the Conference [3]

[3] Followed by the C-PROC Projects Steering Committees (14h30-17h30)