Octopus Conference on cybercrime 2025

4 – 6 June 2025 – Strasbourg, France

Version 30 May 2025

Programme overview

<table>
<tr><th></th><th colspan="2">Morning</th><th colspan="2">Afternoon</th></tr>
<tr><td>Wed 4 June</td><td colspan="2">Opening Plenary (9h00 – 12h30)
Hemicycle | EN/FR/ES
Broadcasted | Open to media
- 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 colspan="2">Main session 1 (14h00 – 17h30)
Hemicycle | EN/FR/ES
Broadcasted | Open to media
E-evidence: implementing the Second Protocol</td></tr>
<tr><td></td><td colspan="2"></td><td>WS 1
(14h00 – 15h30)
Room 11, EN/FR/ES
Broadcasted | Open to media
Youth and cybercrime</td><td>WS 2
(16h00 – 17h30)
Room 11, EN/FR/ES
Cyberviolence: NCDII and violence against women</td></tr>
<tr><td>Thu, 5 June</td><td colspan="2">Main session 2 (9h00 –12h30)
Hemicycle | EN/FR/ES
Broadcasted | Open to media
Cyber-interference with democracy</td><td colspan="2">Main session 3 (14h00 – 17h30)
Hemicycle | EN/FR/ES
Pig-butchering/investment scams</td></tr>
<tr><td></td><td>WS 3 (9h00-10h30)
Room 11, EN/FR/ES
Broadcasted | Open to media
Crypto-investigations</td><td>WS 4 | 5 | 6 | 7
(11h00-12h30)
Regional workshops
Broadcasted, Open to media
Africa, Room 10, EN/FR,
Asia, Room 3, EN
Pacific, Room 11, EN
NOT broadcasted
Americas, Room 2, EN/ES</td><td>WS 8 (14h00 – 15h30)
Room 11, EN/FR/ES
Cyberviolence: Child Sexual Abuse material in the era of AI</td><td>WS 9 (16h00 – 17h30)
Room 11, EN/FR/ES
Broadcasted | Open to media
Cybercrime as war crime?</td></tr>
<tr><td>Fri, 6 June</td><td colspan="2">Main session 4 (9h00 – 12h00)
Hemicycle | EN/FR/ES
Broadcasted | Open to media
Cybercrime, e-evidence and AI</td><td colspan="2">Concluding plenary (12h15 – 13h30)
Hemicycle | EN/FR/ES
Broadcasted | Open to media
Concluding panel: the way ahead</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2">13h30 End of the conference</td><td colspan="2">14h30 C-PROC project steering committees</td></tr>
</table>

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. Moderators: Pedro Verdelho, Chair of the Cybercrime Convention Committee (T-CY), Portugal / Tupou'tuah Baravilala, Director General, Ministry of Trade, Co-operatives and Communications, Fiji / Alexander Seger, Head of Cybercrime Division, Council of Europe Secretariat: Nina Lichtner, Octopus Project Manager, Council of Europe **Opening [9h00 – 9h30]** ▪ Jonathan Attard, Minister of Justice of Malta, on behalf of the President of the Committee of Ministers of the Council of Europe ▪ Alain Berset, Secretary General of the Council of Europe ▪ Samuel Nartey George, Minister for Communication, Digital Technology and Innovations, Ghana **Cybercrime and electronic evidence: global perspectives [9h30 – 10h30]** ▪ Panel: – William Cameros Martinez, Vice-Minister, Ministerio de Gobernación República de Guatemala – Laurence Hortas-Laberge, Legal Officer, Criminal, Security, and Diplomatic Law Division at Global Affairs Canada – Jamila Akaaga Ade, Head of the Cybercrime Unit, Federal Ministry of Justice, Nigeria – Edora Binti Ahmad, Deputy Chief Executive, National Cyber Security Agency (NACSA), Malaysia – Michele Socco, Cybercrime Unit, DG Migration and Home Affairs, European Commission – Dong Uk Kim, Interpol Global Complex for Innovation, Singapore
Coffee break 10h30-11h00	
	Update: Global state of cybercrime legislation and implementation of the Convention on Cybercrime and its Protocols [11h00 – 11h30] ▪ Alexander Seger, Head of Cybercrime Division, Council of Europe

	International treaties on cybercrime: the new United Nations Convention Against Cybercrime ("Hanoi Convention") and its links to the Convention on Cybercrime ("Budapest Convention") [11h30 – 12h30] ▪ Welcome remarks – Nguyen Minh Vu, Ambassador, Viet Nam – Glen Prichard, Chief, Cybercrime and Technology Section, UNODC ▪ Panel on criminalisation – Benefits and challenges of criminalizing conduct in cybercrime conventions – The similarities and differences between criminalisation of the Convention on Cybercrime (Budapest Convention) and the UN Convention against Cybercrime (Hanoi Convention) – Panellists: - Mariana Kiefer, Cybercrime Regional Adviser for Latin America, UNODC - Nathan Whiteman, Director and Principal Legal Officer, Cybercrime, Child Abuse Policy and Engagement Section (CCAPES), Australia ▪ Panel on international cooperation – Framework on digital evidence, tools for international cooperation, partnerships – Panellists: - Joshua James, Cybercrime Regional Adviser for Southeast Asia and the Pacific, UNODC - Michele Socco, European Commission - George-Maria Tyendezwa, Director Legal Services, Federal Ministry of Justice, Nigeria - Aisling Kelly, Assistant General Counsel, Law Enforcement and National Security, Europe, Microsoft ▪ The Signing Ceremony in Hanoi – Nguyen Huu Phu, Deputy Director General, Ministry of Foreign Affairs ▪ Closing remarks – Nayelly Loya, Head of the Global Programme on Cybercrime, UNODC / Glen Prichard, Chief, Cybercrime and Technology Section, UNODC
12h30-14h00	Group photo (Hemicycle) and lunch break
14h00-17h30	**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

Break 15h15-15h45	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. Moderator: Pedro Verdelho, Chair of the Cybercrime Convention Committee (T-CY), Portugal Rapporteur: Claudia Pina, Investigating Judge, Central Criminal Investigation Court of Lisbon, Portugal Secretariat: Jutta Dinca, Programme Manager, CyberSPEX project, C-PROC **Introduction to the session and to the Second Protocol [15 min]** ▪ Content, agenda and objective of the session ▪ Introduction to the 2AP **Use cases: Obtaining the disclosure of electronic evidence now and in the future under the 2AP [60 min]** ▪ Criminal justice practitioners will discuss brief use cases on how to obtain e-evidence from other jurisdictions currently and how they will do so under the 2AP: – Panellists: - Eirik Trønnes Hansen, Senior adviser, National Criminal Investigation Service, Norway - Maria Elvira Tejada de la Fuente, Prosecutor, National Coordinating Chamber against Cybercrime, Attorney General's Office, Spain - Gareth Sansom, Deputy-Director, Technology & Analysis, Department of Justice, Canada - Antonio Segovia, Legal Expert, Chile **Expectations [60 min]** ▪ Private sector perspectives: Representatives of private sector entities will discuss with criminal justice experts their current challenges and what they expect from the 2AP – Panellists: - Aisling Kelly, Assistant General Counsel, Law Enforcement and National Security, Europe, Microsoft - Kate McCormack, Legal counsel, Ireland, Google - Benjamin Fitzpatrick, Associate General Counsel, Meta - Dean S. Marks, Emeritus Executive Director, Coalition for Online Accountability - Klaus Landefeld, Head of Infrastructure and Networks, Eco – Association of the Internet Industry - EuroISPA - Erica O'Neil, Assistant Deputy Chief, USDoJ - Eirik Trønnes Hansen, Senior adviser, National Criminal Investigation Service, Norway - Maria Elvira Tejada de la Fuente, Prosecutor, National Coordinating Chamber against Cybercrime, Attorney General's Office, Spain - Gareth Sansom, Deputy-Director, Technology & Analysis, Department of Justice, Canada - Antonio Segovia, Legal Expert, Chile

	Towards implementation and ratification of the Second Protocol [40 min] ▪ Examples will illustrate how governments go about legislative reforms necessary for the implementation and ratification of the 2AP – Karin Henriksson, Legal Advisor, Division for Criminal Cases and International Judicial Cooperation, Ministry of Justice, Sweden – Tupou'tuah Baravilala, Director General, Ministry of Trade, Co-operatives and Communications, Fiji **Conclusions [5 min]**
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. Moderator: TBC Rapporteur: Reinout Vermaercke, European Youth delegate, Flemish Youth Council Secretariat: Nina Lichtner, Programme Manager, Octopus Project **Introduction and objective of the workshop** **Youth and cybercrime: risks, responsibilities, and threats** ▪ Panellists: – Oluwatobi, Ayodele, Co-Founder, Cybersecurity Education Initiative (CYSED) – Winner of the Youth and Cybercrime Competition – Julieta Micaela Ríos, Faculty of Law, University of Buenos Aires - Winner of the Youth and Cybercrime Competition – Dubravko Šopar, Executive Director, Association for promoting positive affirmation of youth in society „Impress", Croatia **Protecting youth from cybercrime: the role of law enforcement and the private sector** ▪ Panellists: – Gabriel-Andrei Brezoiu, President, GEYC - Group of the European Youth for Change, PRISMA European Network – Irene Oduor, Investigator, Directorate of Criminal Investigation, Anti-Human Trafficking and Child Protection Unit, National Police Service, Kenya – Fernanda Teixeira Souza Domingos, Federal Prosecutor, Coordinator of the Advisory Group on Cybercrime, Federal Prosecution Service, Brazil [TBC]

	– Houda Cherif, Conseil de l'Europe, Tunis Office, HEY (Human Rights Education for Youth) Programme **Conclusions**
16h00-17h30	**Workshop 2 – Cyberviolence: non-consensual dissemination of intimate images (NCDII) and violence against women** 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 "sextortion", 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. GREVIO's General Recommendation No. 1 on the digital dimension of violence against women recognises NCDII as falling within the scope of sexual harassment as defined by the Istanbul Convention. Moreover, 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 16 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 Moderator: Nathan Whiteman, Director / Principal Legal Officer, Cybercrime, Child Abuse Policy and Engagement Section (CCAPES), Attorney-General's Department, Australia Rapporteur: Hania El Helweh, Judge, President of the First Instance Court, North of Lebanon Secretariat: Ana Elefterescu, Programme Manager, CyberSouth+ project, C-PROC **Introduction and objective of the workshop [15 min]** ▪ Introductory presentation: NCDII – the issue **Strengthening responses to NCDII [45 min]** ▪ Panel – Nayelly Loya – Head of the Global Programme on Cybercrime, UNODC – Anne-Marie Le Bel, Senior Legal Counsel, Department of Justice, Canada – Nueebu Leyii Mikko, Assistant Chief State Counsel, Cybercrimes Unit, Federal Ministry of Justice, Nigeria

	– Guido Edmundo Valenti Argüello, Chief of Staff to the Undersecretary of Criminal Policy, Ministry of Justice, Argentina – Catherine Van de Heyning, Focal point prosecutor on cyberviolence, Cybercrime Division, Public Ministry of Antwerp, Belgium – Jean-Christophe Le Toquin, Co-founder, Operations, STISA – Survivors & Tech Solving Image-Based Sexual Abuse **What strategies, policies and measures to counter NCDII? [25 min]** ▪ Discussion **Conclusions [5 min]**
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. Moderators: Simona Granata-Menghini, Director, Venice Commission, Council of Europe / Alexander Seger, Head of Cybercrime Division, Council of Europe Secretariat: Jan Kralik and Giorgi Jokhadze, Cybercrime Division, Council of Europe **Introduction and objective of the session: about cyber interference with democracy [15 min]** ▪ Alexander Seger, Council of Europe **Cyber interference with democracy – actions and actors [80 min]**

	▪ Setting the scene: – Oleksii Tkachenko, National Security and Defence Council of Ukraine: The case of Ukraine: continuous attack on democracy – Paul Radu, Co-founder, Organized Crime and Corruption Reporting Project: The enabling infrastructure for cyber interference and the role of organised crime groups ▪ Panel discussion: - Victor Lăpușneanu, Head of Multilateral Department, Ministry of Foreign Affairs of Moldova - Clint Watts, Microsoft Threat Analysis Center - Isabel Linzer, Centre for Democracy and Technology - Geronimo Sy, Professor of Law, Silliman University, AI LegalTech Founder and Adviser, The Philippines ▪ Open discussion with the audience **Preventing and responding to cyber interference with democracy [80 min]** ▪ Panellists: - Albert Antwi-Boasiako, Cybersecurity expert and author, Ghana - Daniel Cimpean, Director, National Directorate for Cyber Security, Romania - Nienke Palstra, Global Witness - Pablo Maristany de las Casas, Analyst, Institute for Strategic Dialogue - Eirik Holmøyvik, Bureau of the Venice Commission, Norway ▪ Open discussion with the audience **Conclusions [5 min]**
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. Moderator: Robert Golobinek, Ministry of Justice of Slovenia

	Rapporteur: Ana Gogovska Jakimovska, Public Prosecutor of North Macedonia, Secretariat: Dan Cuciurianu, Programme Manager, CyberSEE project, Council of Europe **Introduction and objective of the workshop [5 min]** **Setting the scene [20 min]** ▪ Typologies of cyber offences involving virtual assets, examples of investigation and the role of VASPs – Nenad Bogunović, Chief Inspector, Ministry of Internal Affairs of Serbia **Use of investigative powers to obtain data from VASPs [60 min]** ▪ Panellists: – Fernanda Teixeira Souza Domingos, Prosecutor, Brazil – Subhani Keerthiratne, Director of Financial Intelligence Unit, Sri Lanka – Christian Beyer, University Lecturer, Academia, Germany – Nick Pailthorpe, Global Director of Government Relations, Kodex – Scott Johnston, Director of Business Development, Chainalysis, – Maksym Dragunov, Director Policy and Advisory, Crystal Intelligence **Conclusions [5 minutes]**
11h00-12h30	**Workshop 4 – Regional workshop for Africa - Strengthening regional and domestic cooperation to combat online fraud and cyber-enabled scams in Africa"** Location: Room 10 Languages: EN/FR Purpose: One of the top cyber threats identified by African member countries in 2023 was online fraud, particularly in terms of their volume and overall financial impact. The type of fraud ranges from advance-fee fraud, to romance scams, business email compromise or phishing, related threats such as ransomware offences, and challenges related to digital forensics, dark web investigations and proceeds of crime, including virtual assets. Initiatives such as INTERPOL's Africa Surges and Serengeti facilitate and streamline cooperation between African law enforcement agencies to prevent, mitigate, investigate, and disrupt online scams and not only. Building on the results of these successful operations, the workshop will examine case studies and models of cooperation in the investigation of online fraud and present experience of the countries in dealing with such cases. Moderator: Dong Uk Kim, Coordinator, GLACY-e Project, Cybercrime Directorate, INTERPOL Rapporteur: Sêvi Rodolphe Adjaïgbe, Head of Cyberdiplomacy and Legal Affairs, National Agency for Information Systems Security, Benin Secretariat: GLACY-e project, C-PROC

	Introduction and objective of the workshop [10 min] **Domestic interagency cooperation: [30 min]** ▪ Panel on challenges and lessons learned: – Jamila Akaaga Ade, Deputy Director, Head, Cyber Crime Unit, Department of Public Prosecutions, Federal Ministry of Justice, Nigeria – George Eduah Beesi, Lead, Law Enforcement Liaison Unit, Cybersecurity Agency, Ghana – Michael L. Ilishebo, Cyber Crime Investigator, Zambia Police Service ▪ Open discussion with the audience **How to enhance cross-border investigations and cooperation in online scam cases [40 min]** ▪ Brief overview of the operations Africa Surge & Serengeti – Kevin Kiban, Cybercrime Operations Officer Cybercrime Directorate (AFJOC PROJECT) ▪ Discussion on regional interagency groups – Alexander Oppong, Director, Capacity Building & Awareness Creation, Cybersecurity Agency, Ghana – Daniel Monteiro, Director General of the FIU, Cabo Verde **Conclusions [15 min]**
11h00-12h30	**Workshop 5 – Regional workshop for Americas** Location: Room 2 Languages: EN/ES Purpose: Cybercrime involving virtual assets is rapidly growing in Latin America and Caribbean, driven by the region's increasing adoption of digital financial services and limited regulatory enforcement. Criminal actors leverage the anonymity and decentralized nature of cryptocurrencies to facilitate fraud, ransomware attacks and the laundering of illicit proceeds. Dark web marketplaces and peer-to-peer exchanges, often operating with minimal oversight, provide a fertile ground for illegal transactions. While some countries in the region are making strides to strengthen their regulatory frameworks, e.g. in alignment with the Budapest Convention and its Second Additional Protocol, the absence of standardized protocols and robust international cooperation remains a major obstacle. As a result, judicial authorities often struggle to access key evidence stored on foreign servers or through decentralized exchanges, making it challenging to prosecute money laundering, fraud, and other financial crimes linked to cryptocurrencies. The regional workshop will offer the opportunity for LAC delegates to engage in an international cooperation simulation exercise, racing against time to solve 5 challenges that will address the follow the money and follow the data principles and enable participants to identify gaps and possible solutions enabling criminal justice authorities to fight against illegal financial flows in the region. Moderators: Marcela Toledo, Deputy Director, Cybercrime and Money Laundry Unit, Public Ministry, Chile

	Jane Lee, Prosecutor, U.S. Department of Justice Marcos Salt, Director of the postgraduate program cybercrime and digital evidence, University of Buenos Aires Rapporteur: Claudio Peguero, Cyber Ambassador, Ministry of Foreign Affairs, Dominican Republic Secretariat: Javier Gomez Prieto, Programme Manager, GLACY-e project, C-PROC **Introduction and objective of the workshop [5 min]** **Simulation exercise on follow the money and follow the data principles** ▪ Challenge 1 [16 min] ▪ Challenge 2 [16 min] ▪ Challenge 3 [16 min] ▪ Challenge 4 [16 min] ▪ Challenge 5 [16 min] Each challenge will have one main topic, with two injects for the participants to debate and conclude. Mentimeter will be used to enhance the participants' experience. **Conclusions [5 min]**
11h00-12h30	**Workshop 6 – Regional workshop for Asia - enhancing the role of women in the fight against cybercrime** Location: Room 3 Languages: EN Purpose: In an increasingly digital world, the complexities of cybercrime continue to evolve, presenting challenges that extend beyond technological concerns. From a human perspective, the gender disparity within this field is apparent, with women underrepresented in roles across the judiciary, law enforcement, cybersecurity, and digital forensics. This imbalance limits the diversity of perspectives in investigations, which can lead to biases in understanding and addressing cybercrime. Additionally, it highlights structural barriers, such as unequal access to training, skills development, and leadership opportunities, that can impede women's involvement and contributions. Addressing this gap is important for fostering more inclusive, effective, and victim-centered responses to cybercrime. Integrating a gender-sensitive perspective on cybercrime within the criminal justice system requires an understanding of how cybercrimes affect women and men differently and the development of tailored responses to these differences. Additionally, it is crucial to involve women in various roles within law enforcement to ensure the proper documentation and investigation of cybercrimes that specifically target women. This workshop will showcase the important contributions women are making to the effective investigation, prosecution, and adjudication of cybercrime throughout Asia.

	Moderators: Wendala Gamaralalage Subhani Sulochana Keerthiratne, Director, Financial Intelligence Unit, Sri Lanka Judge Rainelda H. Estacio-Montesa, Judge, Supreme Court of the Philippines Rapporteur: Edora binti Ahmad, Deputy Chief Executive (Legal Management) National Cyber Security Agency, Malaysia Secretariat Catalina Stroe, Programme Manager, GLACY-e project, C-PROC **Introduction and objective of the workshop [10 min]** **Women in the law enforcement - responding to digital threats [35 min]** ▪ Integrating gender sensitivity in cybercrime and financial investigations**:** – Wendala Gamaralalage Subhani Sulochana Keerthiratne, Director, Financial Intelligence Unit, Sri Lanka ▪ Open discussion on best practices and challenges in implementing gender-sensitive strategies in policing **Women in the judiciary - leading the fight against cybercrime [35 min]** ▪ The role of gender sensitivity in cybercrime prosecution and adjudication – Judge Rainelda H. Estacio-Montesa, Judge, Supreme Court of the Philippines ▪ Open discussion on obstacles and solutions for implementing gender-sensitive approaches within the judiciary **Conclusions [10 min]**
11h00-12h30	**Workshop 7 – Regional workshop for Pacific** Location: Room 11 Languages: EN Purpose: Pacific countries find themselves at various stages of implementation of cybercrime legislation. Some have recently passed standalone cybercrime legislation, some meet international standards through separate pieces of legislation, while others are only starting their cybercrime legal policy reform. This workshop builds on the ongoing work jointly with Pacific Islands Law Officer's Network (PILON) to draft a Handbook intended to support the Pacific Island jurisdictions to enact reforms on cybercrime and electronic evidence. It will explore the legal policy issues to be considered in the transposition of international frameworks as well how to successfully implement cybercrime legislation in the region. Moderator**:** Marko Jurić, Associate Professor, University of Zagreb, Croatia Rapporteur**:** Madeleine Lavemai, Crown Counsel, Tonga Secretariat**:** Anastasia Gadja, Senior Project Officer, GLACY-e project, C-PROC

	Introduction and objective of the workshop [10 min] **Legal policy considerations in cybercrime reform and national legislative traditions [35 min]** ▪ Open discussion – Proposing Cybercrime Reform – Working with subject matter experts across agencies – Reflections on challenges and opportunities of working with capacity-building partners – Specific consultation processes in the region **Developing an implementation plan [35 min]** ▪ Open discussion – Legislative design and drafting instructions – Preserving the option to join international frameworks – Allocating responsibilities and functions under legislation **Conclusions [10 min]**
12h30-14h00	Lunch break
14h00-17h30	**Main session 3 - Pig-butchering/investment 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 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. Moderator: Sylke Gruhnwald, Reporter

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

Coffee break 15h30-16h00	Rapporteur: Jose Midas Marquez, Associate Justice, Supreme Court of the Philippines Secretariat: Catalina Stroe, Programme Manager, GLACY-e project, C-PROC **Introduction and objective of the workshop [10 min]** **Typologies and modus operandi of pig-butchering/romance scams [40 min]** ▪ Setting the scene - Pig-butchering in Southeast Asia: modus operandi, criminal infrastructure and impact – William Hall, ICHIP Southeast Asia (Cybercrime), U.S. Department of Justice – Puvadet Prommakrit, Provincial Public Prosecutor, International Affairs Department, Office of the Attorney General, Central Authority of Mutual Legal Assistance and Extradition, Thailand ▪ Open discussion with the audience **Session 2: Strategies for investigations [60 min]** ▪ Panel – Nino Goldbeck, Senior Public Prosecutor, Office of the Public Prosecutor General in Bamberg, Bavarian Central Office for the Prosecution of Cybercrime, Germany – Erin West, Founder and President, Operation Shamrock, USA – Daniel Nwaka, Chief Superintendent of the Economic and Financial Crimes Commission, Nigeria ▪ Open discussion with the audience **Session 3: Avenues for international and public/private cooperation [60 min]** ▪ Panel: – Joshua James, Regional Counter-Cybercrime Coordinator, UNODC, Connecting the dots: identifying links between crypto-scams, human trafficking, and organised crime – Lilija Mazeikiee, Head of Investigations, EMEA, BINANCE, Importance of public/private cooperation – Fernanda Teixeira Souza Domingos, Federal Prosecutor, Brazil, Leveraging the framework of the Convention on Cybercrime and its Second Protocol in cross-border investigations, public/private cooperation and sharing of spontaneous information ▪ Open discussion with the audience **Conclusions [10 min]**
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. Moderator: Naomi Trewinnard, Children Rights Division, Council of Europe Rapporteur: Mariana Kiefer, Chief of Office, UNODC Programme Office in Uruguay Secretariat: Cristiana Mitea, Octopus Project, Cybercrime Programme Office of the Council of Europe **Introduction and objective of the workshop [5 min]** **Setting the scene: case study [15 min]** ▪ Mike Frend, UK Online CSEA Covert Intelligence Team (OCCIT) **Challenges for investigation and prosecution [65 min]** ▪ Panellists – Nathan Whiteman, Director, Cybercrime, Child Abuse Policy and Engagement Section, Attorney General's Chambers, Australia – Hannah Swirsky, Internet Watch Foundation – Madeleine Van der Bruggen, Deputy Director, Offlimits ▪ Open discussion of practical solutions **Conclusions [5 min]**
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.[2] 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 provides a helpful background for discussions during this Workshop. The purpose of this session is to identify:

[2] Please note that 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.

	– 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 to prosecute such crimes in domestic and international courts. Moderator: Givi Baghdavadze, Head of International Cooperation Unit, Office of the Prosecutor General of Georgia Rapporteur: TBC Secretariat: Giorgi Jokhadze, Project Manager CyberEast+ Project, Cybercrime Division, Council of Europe **Introduction and objective of the session [5 min]** **International perspectives: "Cyber-enabled crimes under the Rome Statute" and other international norms [30 min]** ▪ Panellists: – Matthew Cross, Appeals Counsel, Office of the Prosecutor, International Criminal Court – Markko Kunnapu, Adviser, Ministry of Justice and Digital Affairs of Estonia – Branko Stamenkovic, Public Prosecutor and Head of the MLA and Cybercrime Department of the Supreme Public Prosecution Office of Serbia **Domestic perspectives: prosecuting cyberattacks as war crimes [30 min]** ▪ Introductory presentation: A look at the battlefield: perspective from Ukraine, – Viktoriia Litvinova, Deputy Prosecutor General of Ukraine ▪ Panel discussion – Viktoriia Litvinova, Deputy Prosecutor General of Ukraine – Matthew Cross, Appeals Counsel, Office of the Prosecutor, International Criminal Court – Markko Kunnapu, Adviser, Ministry of Justice and Digital Affairs of Estonia – Branko Stamenkovic, Public Prosecutor and Head of the MLA and Cybercrime Department of the Supreme Public Prosecution Office of Serbia **Open discussion with audience [20 min]** **Conclusions [5 min]**
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
- 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.

Moderator: Gareth Sansom, Department of Justice, Canada

Rapporteur: Jayantha Fernando, Hon Director, Data Protection Authority & Sri Lanka CERT and former T-CY Bureau

Secretariat: Javier Gomez Prieto, Programme Manager, GLACY-e project, C-PROC / Jan Kralik, Programme Manager, T-CY Secretariat, Council of Europe

Introduction and objective of the session [10 min]

- Objective of the session
- Information about the T-CY Working Group on AI
- Underlying concepts

The dark side of AI: Offences against, by and by means of AI systems [70 min]

- Abuse of generative AI techniques – example of offences against, by and by means of AI systems
  - Steven Masada, Digital Crimes Unit, Microsoft

- Panel discussion:

  - Sara Pangrazzi, Federal Office of Justice, Switzerland
  - Sabine Gless, University of Basel, Faculty of Law
  - Marcela Toledo, ULDDECO, Prosecutor's Office, Chile

- Open discussion with audience

Topic 2: The bright side of AI: Leveraging AI for investigations, the collection of electronic evidence and international cooperation [70 min]

- Use of AI in law enforcement:
  - Emmanuel Kessler, EC3, EUROPOL

- Panel discussion:
  - Albina Ovcearenco, Head of Digital Development Unit, Council of Europe

	– Yves Vandermeer, European Cybercrime Training and Education Group – Marcos Salt, Law University of Buenos Aires, Argentina ▪ Open discussion with the audience **Conclusions by moderator or rapporteur [10 min]**
12h15-13h30	**Closing plenary and conclusions** Location: Hemicycle Languages: EN/FR/ES Moderator: Hanne Juncher, Director of Security, Integrity and the Rule of Law, Council of Europe **Key takeaways from workshops** ▪ Rapporteurs to present the conclusions of each session **Outlook for 2025/6** ▪ Panel discussion on priorities for enhanced cooperation on cybercrime and electronic evidence in 2025/2026 – Viktoriia Litvinova, Deputy Prosecutor General of Ukraine – Glenn Micallef, Commissioner for Intergenerational Fairness, Youth, Culture and Sport, European Union – James Juma Kimuyu, Director, NC4 National Computer and Cybercrimes Cordination Committee, Kenya **Conclusions** ▪ Key take-aways from the Octopus Conference (Alexander Seger, Council of Europe)
13h30	End of the Conference [3]

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