



Octopus Conference 2023

13-15 December 2023 – Bucharest, Romania

Conference Programme - Overview

Version 10 December 2023

WED, 13 DECEMBER 2023			
8h30-9h30	Welcome coffee and registration		
9h30-13h00	Opening plenary session (livestream) – Rosetti Room EN/FR/ES <ul style="list-style-type: none"> ▶ Cybercrime and e-evidence: global perspectives ▶ Cybercrime and e-evidence of war crimes: Lessons learned from the Russian aggression against Ukraine ▶ Cybercrime v. freedom of expression ▶ The framework of the Convention on Cybercrime: Update 		
Coffee break 10h30-11h00			
13h00-14h30	Group photo and Lunch break		
14h30-16h00	Workshop 1 (livestream) EN/FR/ES/RO <ul style="list-style-type: none"> ▶ Global state of cybercrime legislation Iorga Room	Workshop 2 EN/FR/ES/RO <ul style="list-style-type: none"> ▶ Spontaneous information sharing Brătianu Room	Workshop 3 EN/FR/ES <ul style="list-style-type: none"> ▶ Automatic detection of child sexual exploitation and abuse materials Balcescu Room
16h00-16h30	Coffee-break		
16h30-18h00	Workshop 4 (livestream) EN/FR/ES/RO <ul style="list-style-type: none"> ▶ Synergies between the Budapest, Lanzarote, Istanbul and Trafficking Conventions Iorga Room	Workshop 5 EN/FR/ES/RO <ul style="list-style-type: none"> ▶ The interplay of cybercrime and financial investigations Bălcescu Room	Workshop 6 EN/FR/ES <ul style="list-style-type: none"> ▶ Cybercrime and artificial intelligence Brătianu Room
18h00-20h00	Social event – Take Ionescu Room		
THU, 14 DECEMBER			

9h30-13h00 <i>[coffee-break 11h00-11h30]</i>	Project event: EN ▶ From CyberEAST to CyberEast+ Iorga Room	Project event: EN ▶ From iPROCEEDS-2 to CyberSEE Bălcescu Room	Project event: EN/FR/ES/PT (passive) ▶ From GLACY+ to GLACY-e Brătianu Room	
13h00-14h30 Lunch break				
14h30-15h30		Project event: EN/FR/ES ▶ From CyberSouth to CyberSouth+		
15h30-16h00	<i>Coffee-break</i>			
16h00-18h00	Lightning talks (livestream) EN/FR/ES/RO Iorga Room	Bălcescu Room		
FRIDAY, 15 DECEMBER				
9h30-11h00	Workshop 7: EN ▶ Regional Workshop for Asia Human Rights Room	Workshop 8: EN ▶ Regional Workshop for Pacific Bălcescu Room	Workshop 9: EN/FR/ES/PT (passive) ▶ Regional Workshop for Africa Brătianu Room	Workshop 10 EN/ES/RO ▶ Regional Workshop for Latin America and the Caribbean Iorga Room
11h00-11h30	<i>Coffee-break</i>			
11h30-13h00	Workshop 11: (livestream) EN/FR/ES/RO ▶ Capacity building as a game changer: what makes a difference? Iorga Room	Workshop 12: EN/FR/ES/RO ▶ Online xenophobia and racism v. freedom of expression Human Rights Room	Workshop 13: EN/FR/ES ▶ Strengthening 24/7 points of contact Bălcescu Room	Workshop 14: EN/FR/ES/RO ▶ The interplay between cybersecurity and cybercrime Brătianu Room
13h00-14h30	<i>Lunch break</i>			

	<ul style="list-style-type: none"> – Moderator: Patrick Penninckx, Head of Information Society Department, Council of Europe – Introduction to the issue: Krešimir Kamber, Lawyer, European Court of Human Rights, Strasbourg – Panel: Jayantha Fernando, Sri Lanka / Gatembu Kairu, Kenya / Gareth Sansom, Canada <p>▶ The framework of the Convention on Cybercrime: Update [12h30-13h00]</p> <ul style="list-style-type: none"> – Alexander Seger, Council of Europe
14h30-16h00	<p>Workshop 1 - Global state of cybercrime legislation (livestream)</p> <p>Languages: EN/FR/ES/RO</p> <p>Purpose: Legislation is the basis for criminal justice action on cybercrime and electronic evidence. Many governments around the world have undertaken legal reforms, often using the Budapest Convention on Cybercrime as a guideline. However, cybercrime legislation also needs to meet human rights and rule of law requirements to prevent misuse. The aim of this workshop is to review progress made worldwide in terms of cybercrime legislation and to identify possible risks and challenges.</p> <p>Moderator/s: Zahid Jamil, Barrister-at-law, Jamil & Jamil, Pakistan</p> <p>Rapporteur : Fernanda Teixeira Domingos, Prosecutor’s Office, Brazil</p> <p>Secretariat: Giorgi Jokhadze / Tatiana Bastrighin</p> <p>▶ Introduction and objective of the workshop [5 min]</p> <ul style="list-style-type: none"> – Moderator’s notes – Secretariat <p>▶ From 2013 to 2023: Ten years of progress in legislation on cybercrime and electronic evidence [10 min]</p> <ul style="list-style-type: none"> – Results of a survey by the Cybercrime Programme Office of the Council of Europe (C-PROC) - Giorgi Jokhadze, Programme Manager, C-PROC <p>▶ Examples of recent reforms [30 min]</p> <ul style="list-style-type: none"> – Jamila Akaaga Ade, Nigeria – Germán Ortega, Ecuador – Glenys E. Andrews, Fiji <p>▶ Challenges and risks [40 min]</p> <ul style="list-style-type: none"> – Second Additional Protocol: implementing legislation – Ioana Albani, Romania – Human rights safeguards/freedom of speech - Jan Kralik, Council of Europe – Discussion: do’s and don’ts for cybercrime/e-evidence legislation (open discussion and examples) <p>▶ Conclusions [5 min]</p>

14h30-16h00

Workshop 2 - Spontaneous information sharing

Languages: EN/FR/ES/RO

Purpose: Criminal justice authorities often possess valuable information that they believe may assist the authorities of another country in a criminal investigation but of which these other authorities are not aware of. Parties to the Budapest Convention may share this type of information through Article 26 on "spontaneous information":

"A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter...."

The relevance of Article 26 has been increasing over time, including within the context of cases related to the dark web or to the sharing of data retrieved from encrypted communications.

The aim of the workshop is to identify current practices of using Article 26 of the Convention on Cybercrime.

Moderators: Jan Kerkhofs, Federal Magistrate, Head of the Cyber Unit, Belgian Federal Prosecutor's Office
Antonio Segovia Arancibia, Transnational criminal law professor, UAI University, Chile

Rapporteurs: Jorge Espina, Chair of the Cybercrime Team, Deputy National Member of Spain, Eurojust
Catalina Stroe, Programme Manager, Cybercrime Programme Office of the Council of Europe

Secretariat: GLACY+ team

► **Introduction and objective of the workshop [5 min]**

- Jan Kerkhofs, Federal Magistrate, Head of the Cyber Unit, Belgian Federal Prosecutor's Office

► **Application and interpretation of the concept of spontaneous exchange of information between judicial authorities in the EU Member States and the countries with a Liaison Prosecutor present at EUROJUST [10 min]**

- Sofia Mirandola, Judicial Cooperation Advisor at the Casework Unit, Operations Department, Eurojust

► **Panel discussion on the use of Article 26 of the Convention by Parties providing information: what are the procedures and conditions? [35 min]**

- Benjamin Fitzpatrick, Senior Counsel, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice
- Open debates – moderated by Jan Kerkhofs

► **Panel discussion on receiving spontaneous information: How can it be used as evidence? [35 min]**

	<ul style="list-style-type: none"> – Anastasiia Ponarina, Senior International Cooperation Officer, Department of Cybersecurity, State Security Service, Ukraine – Esteban Aquilar Vargas, Prosecutor, Coordinator of the Cybercrime Unit, Public Ministry, Costa Rica – Open debates – moderated by Antonio Segovia Arancibia, Transnational criminal law professor, UAI University, Chile <p>▶ Conclusions by the rapporteurs [10 min]</p> <ul style="list-style-type: none"> – Jorge Espina, Chair of the Cybercrime Team, Deputy National Member of Spain, Eurojust – Catalina Stroe, Programme Manager, Cybercrime Programme Office of the Council of Europe
14h30-16h00	<p>Workshop 3 – Automatic detection of child sexual exploitation and abuse materials</p> <p>Languages: EN/FR/ES</p> <p>Purpose: Over the past decade multi-national service providers deployed technology for the automated detection of child sexual abuse materials (CSAM) that was uploaded or disseminated via their services. Tens of millions of CSAM have been identified and reported in this way, and in many cases have helped rescue victims and identify and prosecute offenders worldwide. At the same time, the use of such techniques have raised rule of law and human rights concerns, for example, that they interfere with the privacy of communications or involve the transborder transfer of personal data or violate due process requirements. The aim of the workshop is to continue the search for solutions that permit governments to meet their positive obligation to protect children against online sexual violence and enable service providers to use automated technologies to identify and report CSAM with the necessary privacy, data protection and rule of law safeguards.</p> <p>Moderator: Maria José Castello-Branco, Chairperson, Lanzarote Committee Bureau</p> <p>Rapporteur: Ana Elefterescu, Council of Europe Programme Office on Cybercrime</p> <p>Secretariat: Naomi Trewinnard, Legal Advisor, Lanzarote Committee Secretariat Nina Lichtner, Programme Manager, Octopus Project, Council of Europe</p> <p>▶ Introduction and objective of the workshop [5 min]</p> <ul style="list-style-type: none"> – Reflection & progress post Octopus Conference 2021 workshop <p>▶ Advancements in automated detection & report optimization</p> <ul style="list-style-type: none"> – Christophe Boissier, INTERPOL [online] – Susanna Pettersson, ECPAT Sweden – Philip Attwood, Director of Impact, Child Rescue Coalition [online] <p>▶ Enhancing obligations & overcoming challenges</p> <ul style="list-style-type: none"> – Discussion with the audience

	<ul style="list-style-type: none"> ▶ Collaborative solutions & policy implementation <ul style="list-style-type: none"> – Ms Soyoung Park, Korea Communications standards Commission – Discussion with the audience ▶ Conclusions [10 min]
<p>[13 Dec, 16h30-18h00]</p>	<p>Workshop 4 - Synergies between Budapest, Lanzarote, Istanbul and Trafficking Conventions for safer cyberspace (livestream)</p> <p>Languages: EN/FR/ES/RO</p> <p>Purpose: The standards of the Conventions maintained by the Council of Europe in the areas of cybercrime, protection of children against sexual abuse, trafficking in human beings and violence against women are not simply complementary, but meant to encourage work between criminal justice authorities, protection officers and policy makers to ensure better criminal justice and related action in these areas. Substantive law offences, use of procedural tools for investigation and preventive/protective work with victims and witnesses are just examples where harmonisation would be key, while concepts such as action on cyberviolence could serve to indicate where and how such synergies should work.</p> <p>The aim of this workshop is to further enhance synergies between four different – but interconnected – Conventions:</p> <ul style="list-style-type: none"> - Convention on Cybercrime (ETS No. 185) - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) - Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210) - Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197) <p>Moderator: Miriam Bahamonde Blanco, Ministry of Justice, Spain</p> <p>Rapporteur: Ovidiu Majina, Children’s Division, Council of Europe</p> <p>Secretariat: Giorgi Jokhadze / Ana Vlad</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [5 min] <ul style="list-style-type: none"> – Moderator’s notes – Secretariat ▶ Criminal justice action: need to address the gaps before pursuing the synergies [40 min] <p>Interventions from:</p> <ul style="list-style-type: none"> – Council of Europe Study on substantive law aspects of the three Conventions: Budapest, Istanbul, Lanzarote (Betty Shave, T-CY consultant) – US perspective: making standards work together (Nate Brooks, ICHIP Zagreb, USDOJ) <p>Committee views:</p>

	<ul style="list-style-type: none"> – Judith Herrnfeld, T-CY Bureau – Naomi Trewinnard, Lanzarote Convention Committee – María Rún Bjarnadóttir, GREVIO (<i>online</i>) – Mesut Bedirhanoglu, DGII: Directorate General of Democracy and Human Dignity, Trafficking in Human Beings (GRETA) <p>▶ Work on prevention and protection: a different perspective [30 min]</p> <p>Examples of good (and bad) practices/panel interventions:</p> <ul style="list-style-type: none"> – Judith Herrnfeld, T-CY Bureau – Naomi Trewinnard, Lanzarote Convention Committee – María Rún Bjarnadóttir, GREVIO (<i>online</i>) – Mesut Bedirhanoglu, DGII: Directorate General of Democracy and Human Dignity, Trafficking in Human Beings (GRETA) – Examples from the floor <p>▶ Countering cyberviolence: potential for synergies [10 min]</p> <ul style="list-style-type: none"> – The concept of cyberviolence: a “bridge” between these treaties? – Discussion and examples: views from Committees present <p>▶ Conclusions [5 min]</p>
<p>[13 Dec, 16h30-18h00]</p>	<p>Workshop 5 – The interplay of cybercrime and financial investigations</p> <p>Languages: EN/FR/ES/RO</p> <p>Purpose: Establishing efficient collaboration between criminal justice authorities investigating cybercrime and those institutions responsible for financial investigations is vital to protect societies against criminal activities. The aim of the workshop is to identify practices of collaboration, fostering domestic and international cooperation, effective models for interagency teamwork, and principles governing the exchange of information and evidence among financial crime and cybercrime experts.</p> <p>Moderator: Robert Golobinek, Ministry of Justice Slovenia</p> <p>Rapporteur: Goran Jankoski, National Bank of the Republic of North Macedonia</p> <p>Secretariat: Daniel Cuciurianu, Programme Manager, Council of Europe / iPROCEEDS-2 team</p> <p>▶ Introduction and objective of the workshop [5 min]</p> <ul style="list-style-type: none"> – Moderator’s notes – Secretariat <p>▶ Online Criminal Money Flow and Money Laundering Typologies [20 min]</p> <ul style="list-style-type: none"> – Camelia Lopez, Attorney Advisor, Global ICHIP, Dark Web and Cryptocurrency, US DOJ – Max Braun, Director, Prosecutor General’s Office, FIU Luxembourg

	<ul style="list-style-type: none"> ▶ Cooperation in the search, seizure and confiscation of online crime proceeds [15 min] <ul style="list-style-type: none"> – Max Braun, Director, Prosecutor General’s Office, FIU Luxembourg – Camelia Lopez, Attorney Advisor, Global ICHIP, Dark Web and Cryptocurrency, US DOJ ▶ New tools and techniques for financial investigation in cybercrime cases [35 min] <ul style="list-style-type: none"> – Kārlis Pūce, Leading Analyst, FIU Latvia – Horacio J. Azzolin, Prosecutor, Cybercrime Specialised Unit UFECI, Argentina ▶ Q&A [10 min] ▶ Conclusions by the rapporteur [5 min] <ul style="list-style-type: none"> – Goran Jankoski, National Bank of the Republic of North Macedonia
<p>[13 Dec, 16h30-18h00]</p>	<p>Workshop 6 - Generative artificial intelligence: threats and benefits in criminal justice</p> <p>Languages: EN/FR/ES</p> <p>Purpose: Artificial Intelligence (AI) in the criminal justice sector can both represent a serious threat, and enhance the fight against cybercrime. Generative AI may provide effective ways to detect crime or provide investigative assistance by analysing vast amount of data but may also be misused for criminal purposes. Falsified data (such as deep fakes) can even be presented as evidence in court. The aim of this workshop is to examine (a) the criminal threats that generative AI may pose for the criminal justice sector, (b) its role in countering cybercrime, and (c) the key issues that need to be taken into account in assessing electronic evidence generated by AI.</p> <p>Moderator/s: Patrick Penninckx, Head of Information Society Department, Council of Europe</p> <p>Rapporteur: Hon. Hania El Helweh, Judge, President of the First Instance Court, North of Lebanon</p> <p>Secretariat: CyberSouth and T-CY Secretariat</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [5 min] <ul style="list-style-type: none"> – Patrick Penninckx, Head of Information Society Department, Council of Europe ▶ Cybercrime and generative AI: threats and opportunities [40 min] <ul style="list-style-type: none"> – Emmanuel Kessler, Head of Team - Prevention/Outreach, EUROPOL – Antonio Farelo, Officer, Responsible AI Lab (IRAIL), INTERPOL Innovation Centre – Discussion ▶ Addressing generative AI e-evidence: key issues, threats and benefits [35 min]

	<ul style="list-style-type: none"> – Prof. Sabine Gless, CDPC rapporteur on AI and Criminal Law, Professor of criminal law and criminal procedure law, University of Basel, Switzerland – Krešimir Kamber, Adviser to the President and the Registrar, European Court of Human Rights – Mario Lara Orellana, Director of the Department of Institutional Development within the Administrative branch of the Judiciary of Chile – Discussion <p>▶ Conclusions [10 min]</p>
--	---

THU, 14 DECEMBER

<p>9h30-15h30</p> <p>Coffee break <i>11h00-11h30</i></p> <p>Lunch break <i>13h00-14h30</i></p>	<p>Project event: From CyberEast to CyberEast+</p> <p>Languages: EN</p> <p>Purpose: This event serves as the closing conference of the CyberEast project and pave the way to the follow up project CyberEast+. It will follow the project themes of legislation and policies, capacity building, and co-operation; it will tell the CyberEast story from the perspectives of the national partners demonstrating the impact and relevance of the project to improve their capacities regarding cybercrime and electronic evidence. The European Commission and the Council of Europe will formally assess and complete the project and launch a new regional action on cybercrime and electronic evidence in the region through the new CyberEast+ project. The workshop will also discuss in view of adoption a new Declaration on Strategic Priorities for the Eastern Partnership region with key project partners, serving as inspiration for policies and capacity building in the region's countries.</p> <p>Moderator/s: Giorgi Jokhadze / CyberEast team</p> <p>Rapporteur: CyberEast team</p> <p>Secretariat: Giorgi Jokhadze / CyberEast team</p> <p>▶ Opening session [20 min]</p> <ul style="list-style-type: none"> – Representative of the European Commission – Representative of the Council of Europe – Introduction of project country teams – Lead-in: agenda of the meeting (Cybercrime Programme Office) <p>▶ Closing of the CyberEast Project [70 min]</p> <ul style="list-style-type: none"> – Country priorities and achievements in terms of legislation and policies (project country representative) – Capacity building: needs and impact (project country representative) – Co-operation: putting standards into practice (project country representative) <p>Coffee break [30 min]</p> <p>▶ Discussion of the CyberEast+ Project [90 min]</p> <ul style="list-style-type: none"> – New priorities and directions of action (European Commission) – Country teams (Cybercrime Programme Office)
--	---

	<ul style="list-style-type: none"> – Plan of activities (Cybercrime Programme Office) <p>Lunch break [90 min]</p> <p>▶ Meeting of Policy Makers on Cybercrime Policies in the Eastern Partnership region [120 min]</p> <ul style="list-style-type: none"> – Presentation and comparative analysis of the old Declaration (2013) (invited expert) – Declaration of Strategic Priorities for the Eastern Partnership 2023 (Secretariat) – Intervention and assessment by the European Commission – Interventions and assessments from each of the Eastern Partnership countries – Wrap-up and adoption of the 2023 Declaration of Strategic Priorities
<p>9h30-16h30</p> <p><i>Coffee break 11h00-11h30</i></p>	<p>Project event: From iPROCEEDS-2 to CyberSEE</p> <p>Languages: EN</p> <p>Purpose: This closing conference of the iPROCEEDS-2 project will assess the project's main objectives, including legislation and strategic approaches, mechanisms for reporting, capacity enhancement in cybercrime, training for the judiciary and fostering collaboration between public and private sectors, as well as international cooperation. The focus will be on national partners presenting what difference the project has made to improve their agencies' competence in handling cybercrime and electronic evidence. The event will mark the formal evaluation and closing of the project. It will also prepare the ground for new regional action targeting cybercrime and electronic evidence in South-east Europe and Turkey: the new initiative "CyberSEE" will be jointly undertaken by the European Commission and the Council of Europe from 2024 to 2027.</p> <p>Moderator: Daniel Cuciurianu / iPROCEEDS-2 team</p> <p>Rapporteur: Daniel Cuciurianu / iPROCEEDS-2 team</p> <p>Secretariat: Daniel Cuciurianu / iPROCEEDS-2 team</p> <p>▶ Opening session [20 min]</p> <ul style="list-style-type: none"> – Representative of the European Commission – Representative of the Council of Europe – Introduction of the objective and the agenda of the meeting – Introduction of the project country teams <p>▶ Closing event of the iPROCEEDS-2 Project [70 min]</p> <ul style="list-style-type: none"> – Countries/area achievements in terms of legislation, policies and strategies – Countries/area capacities on cybercrime investigation, search, seize and confiscate online crime proceeds and securing electronic evidence – Judicial training results: most prominent objective of the project – Progress made in public-private and international co-operation <p>Coffee break [30 min]</p> <p>▶ Towards CyberSEE Project: regional meeting [90 min]</p>

<p>Lunch break 13h00-14h30</p>	<ul style="list-style-type: none"> - Strategic priorities and new directions of action (European Commission) - Plan of activities (Cybercrime Programme Office) - Current needs, domestic and regional priorities (Country teams) <p>Lunch break [90 min]</p> <p>▶ Essentials of the new project [120 min]</p> <ul style="list-style-type: none"> - Sustainable cybercrime and electronic evidence training within the Justice Academies, Police Academies and other training institutions - Stronger focus on threats of ransomware attacks and OCSEA - Cooperation between cybercrime and cybersecurity institutions - Complementarity of domestic and regional activities
<p>9h30-18h00</p> <p>Review of GLACY+ achievements</p> <p>9h00 – 13h00</p> <p>Coffee break 11h00-11h30</p> <p>Outlook to the future: GLACY-e prospects</p> <p>14h30 – 18h00</p> <p>Coffee break</p>	<p>Project event: From GLACY+ to GLACY-e</p> <p>Languages: EN/FR/ES/ PT (passive)</p> <p>Purpose: This session serves as the closing event of the GLACY+ project. It will provide an opportunity to review the impact of the GLACY+ project, and to share lessons learned. Building on the positive results of GLACY+, a continuation, consolidation and expansion is now commencing with the “Global Action on Cybercrime Enhanced” (GLACY-e), a new EU-CoE joint project. GLACY-e will extend the experience of the GLACY+ project by supporting new selected countries in Africa, Asia-Pacific and Latin America. It will reinforce the leading role of the 8 hub countries in the capacity building agenda in their respective regions.</p> <p>Moderator/s: Catalina Stroe, Programme Manager of GLACY+/-e projects</p> <p>Secretariat: GLACY+ project</p> <p>▶ Opening session [30 min]</p> <ul style="list-style-type: none"> - European Union - INTERPOL - Council of Europe <p>▶ GLACY+ overview and impact [30 min]</p> <ul style="list-style-type: none"> - Catalina Stroe, Council of Europe and Dong Uk Kim, INTERPOL – Introductory presentation <p>▶ Lessons learned from GLACY+ [150 min]</p> <ul style="list-style-type: none"> - Country coordinators, Country achievements, impact at national level and less successful stories [5 min each] <p>▶ What can we expect next? [30 min]</p> <ul style="list-style-type: none"> - Presentation of the GLACY-e project, Catalina Stroe <p>▶ Introduction of the selected countries [60 min]</p> <ul style="list-style-type: none"> - Country representatives, Introduction of the selected countries [7 min each]

<p>16h00-16h30</p>	<ul style="list-style-type: none"> ▶ GLACY-e workplan for Q1 2024 [30 min] <ul style="list-style-type: none"> - Catalina Stroe and Dong Uk Kim, Presentation of the workplan and open debates ▶ Sustainability by design and by default – strategic priorities for hub countries [45 min] <ul style="list-style-type: none"> - Introduction of the regional priorities and agendas by hub countries ▶ Closing remarks [10 min] <ul style="list-style-type: none"> - European Union - INTERPOL - Council of Europe
<p>14h30-18h00</p> <p>Coffee break 15h30-16h00</p>	<p>Project event: From CyberSouth to CyberSouth+</p> <p>Languages: EN/FR/ES</p> <p>Purpose: The objective of the final conference is to jointly review and validate the progresses in the fight against cybercrime in the MENA region during the period 2018 – 2023; assess the impact of the CyberSouth project in five main areas related to the project’s results (legislation, work of police, work of judiciary, international co-operation, national strategies) and evaluate together what worked well (best practices) and what can be improved in the next phase.</p> <p>Moderator/s: Denise Mazzolani, Programme Manager, Council of Europe</p> <p>Secretariat: CyberSouth team</p> <ul style="list-style-type: none"> ▶ Opening session (10 min) <ul style="list-style-type: none"> - Denise Mazzolani, CyberSouth Programme Manager, Council of Europe ▶ CyberSouth assessment: assessment of the five project results (50 min) <ul style="list-style-type: none"> - Summary of the final assessment report - Inputs from priority countries - Discussion ▶ Best practises and review of project implementation’s modalities (60 min) <ul style="list-style-type: none"> - Presentation by CyberSouth project team - Inputs from priority countries - Discussion ▶ Priorities of the MENA region in the cooperation on cybercrime 2024-2026 (50 min) <ul style="list-style-type: none"> - Presentation by priority countries - European Neighbourhood Policy: priorities for the MENA region - Introduction to the CyberSouth+ project: main components and inception phase ▶ Closing remarks (10 min)
<p>16h00-18h00</p>	<p>Lightning talks (livestream)</p>

	<p>Languages: EN/FR/ES/RO</p> <p>Purpose: For the third time, the Council of Europe will be featuring Lightning Talks sessions, during which speakers will briefly present innovative ideas in the field of cybercrime. A lightning talk is a very short presentation lasting only a few minutes. Several lightning talks will usually be delivered by different speakers in a single session.</p> <p>We invite you to submit your proposal for a major innovative idea that you are willing to share with over 500 participants from around the world, who will reunite at the Octopus Conference in Bucharest. 10 proposals will be selected based on the diversity of topics and presenters.</p> <p>Moderator: Jacqueline Fick, CEO, VizStrat Solutions</p> <p>Secretariat: Octopus Project team</p> <p>► Introduction and objective of the session</p> <p>► Lightning talks</p> <ul style="list-style-type: none"> - Abdullah Al Noman, Lawyer, Supreme Court of Bangladesh - Adriana Freitas, Research Project Manager, APWG.EU, Spain - Antonio Piña, Magistrate, General Council of the Judiciary, Spain - Cherie Adhiambo Oyier, Programme Officer - Women's Digital Rights, Kenya ICT Action Network (KICTANet) and Association for Progressive Communications (APC), Kenya - Contanza Mateuzzi, Lawyer, cyberlaw, Women4Cyber, Italy - Daniela Rodriguez, IT Officer, Ministry of Justice, Luxembourg - Ekaterina Dorodnych, Evaluation Specialist, UN Women, Italy - Ilvana Dedja, Researcher, Sense Cyber Research Center, Albania - Ioana Lekea, Assistant Professor, Hellenic Air Force Academy - Department of Aeronautical Sciences - War Games Laboratory, Greece - Matteo Lucchetti, Director, CYBER 4.0, Italy - Pavlos Topalnakos, Supreme Court Attorney, Hellenic Air Force Academy War Games Laboratory, Greece - Roberto Contreras (online), Lawyer, Chilean Public Prosecutor's Office - Ryan Lim Yi Hern, Deputy Attorney General, Attorney General's Chambers, Singapore - Tuomas Tammilehto, R&D Specialist, Laurea University of Applied Sciences, Finland - Yi Hon, Director, Attorney General's Chambers, Singapore - Yuko Yokoyama, Programme Manager, ICANN <p>► Conclusions</p>
FRIDAY, 15 DECEMBER	
9h30-11h00	<p>Workshop 7 - Regional workshop for Asia: Data protection as a facilitator for investigating and adjudicating cybercrime and electronic evidence-based cases</p> <p>Languages: EN</p> <p>Purpose: With the growing reliance on information-driven technology and the exponential growth in the amount of data created and exchanged every day by users and organizations, the right of personal data protection faces major</p>

	<p>challenges. This is also true for criminal justice authorities who need to reconcile effective measures to obtain, access, process, and/ or share personal data in support of criminal investigations and court proceedings with personal data protection rules. Where these requirements are met, they facilitate the sharing of personal data also across borders, with service providers and other private sector entities. This is why Article 14 on the protection of personal data was included in the Second Protocol to the Budapest Convention.</p> <p>The aim of this workshop is to share experiences and discuss challenges across Asia with respect to data protection and relevant legal frameworks in order to develop more effective criminal justice responses to cybercrime.</p> <p>Moderator/s: Peter Kimpian, Programme Manager, Data Protection Unit of the Council of Europe</p> <p>Rapporteur: Keongmin Yoon, Counsel, World Bank</p> <p>Secretariat: GLACY+ project</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [5 min] <ul style="list-style-type: none"> – Peter Kimpian, Programme Manager, Data Protection Unit of the Council of Europe ▶ Data protection safeguards in the Second Additional Protocol – why we needed them? [10 min] <ul style="list-style-type: none"> – Ethel Mercado-Gutay, Executive Judge, Regional Trial Court of Makati, Supreme Court of the Philippines ▶ Data protection as cornerstone of international police cooperation [10 min] <ul style="list-style-type: none"> – Marko Juric, Associate Professor, Department of Law, University of Zagreb, Croatia – Caroline Goemans-Dorny, Data Protection Officer, INTERPOL ▶ Addressing data protection – testimonials from countries [10 min] <ul style="list-style-type: none"> – Dilan Ratnayake, Senior Deputy Attorney General, Attorney General's Department, Sri Lanka ▶ The state’s obligation to protect against crimes and the right to privacy: how to find the right balance? [50 min] <ul style="list-style-type: none"> – Discussion moderated by Jayantha Fernando, Director, Data Protection Authority & Board Director, Sri Lanka CERT ▶ Conclusions [5 min] by the rapporteur
9h30-11h00	<p>Workshop 8 – Regional workshop for Pacific: Challenges in implementing cybercrime laws in small jurisdictions</p> <p>Languages: EN</p>

	<p>Purpose: Robust legal frameworks on cybercrime and electronic evidence are the cornerstone for successful investigations and criminal proceedings. International standards, such as the Budapest Convention, provide a framework for consistent definitions and criminalisation, standardised procedural powers and mechanisms for international cooperation. The absence of transposing such measures into national laws undermines a country’s ability to investigate, prosecute and adjudicate cases involving electronic evidence and to engage in the global efforts to effectively respond to the emerging challenges presented by cybercrime.</p> <p>Small jurisdictions, such as the Pacific Island States, may encounter additional challenges to adopting and adapting appropriate laws, considering their specific legal, administrative, and technical contexts. The workshop is aimed at mapping those challenges and possible solutions based on successful practices in the region.</p> <p>Moderator: Linda Folaumoetu’i, Attorney General of Tonga and Chair of the PILON Cybercrime Working Group</p> <p>Rapporteur: Jamie Crawford, Senior Crown Counsel, Crown Law Office of the Cook Islands, in representation of PILON</p> <p>Secretariat: GLACY+ project</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [10 min] <ul style="list-style-type: none"> – Linda Folaumoetu’i, Attorney General of Tonga and Chair of the PILON Cybercrime Working Group ▶ What makes for an effective cybercrime legal framework, adapted to the needs of Pacific Island States and what challenges do they meet when working on their legislative reform? [35 min] <ul style="list-style-type: none"> – Glenys Andrews, Legal Principal & Officer (Drafting), Office of the Attorney General, Fiji – Andrew Ega Kelesi, Director of Public Prosecutions, Office of the Director of Public Prosecutions, Solomon Islands – Moderated discussions by Noumea Loretta Afamasaga-Teueli, Head of Legislative Drafting, Department for Justice and Border Control, Nauru ▶ Pacific outlook on implementation: what are the key ingredients for effective enforcement? [40 min] <ul style="list-style-type: none"> – Domingo Kabunare, Digital Transformation Office, Ministry of Information, Communications and Transport, Kiribati – John Graham Jack, CIO Office of the Government, Prime Minister's Office Vanuatu – Moderated discussions by Matthew Blackwood, ICHIP, US Department of Justice ▶ Conclusions by the rapporteur, Jamie Crawford, Senior Crown Counsel, Crown Law Office of the Cook Islands, in representation of PILON
9h30-11h00	<p>Workshop 9 – Regional workshop for Africa: The Convention on Cybercrime and the Second Protocol – key to international cooperation on electronic evidence</p> <p>Languages: EN/FR/ES/PT (passive)</p>

Purpose: While electronic evidence is of increasing significance to criminal investigations and proceedings also in Africa, procedures to obtain such evidence from other jurisdictions are often lengthy and not effective. The Second Protocol to the Budapest Convention (opened for signature in 2022) provides tools for enhanced co-operation and disclosure of electronic evidence – such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations, whilst ensuring a strong system of human rights and rule of law safeguards, especially when it comes to protecting personal data. Almost a quarter of African countries are either Parties or have been invited to accede to the Budapest Convention. Making use of the tools of the Second Protocol is thus an option for Africa. Cabo Verde, Ghana, Mauritius and Morocco are among the signatories so far. The workshop is aimed at showcasing the relevance and expediency of the tools for cooperation provided for in the Protocol, as well as at discussing possible challenges to their implementation in the African region.

Moderator/s: Rabiyatou Bah, Programme Manager, OCWAR-C project
Hein Dries, Key expert on cybercrime, OCWAR-C project

Rapporteur: Abdul-Hakeem Ajijola, Chair of the African Union Cyber Security Expert Group

Secretariat: GLACY+ project

► **Introduction and objective of the workshop – why should African countries consider Convention on Cybercrime and its Protocols? [15 min]**

- Erica O’Neil, Assistant Deputy Chief, Computer Crime and Intellectual Property Section, United States Department of Justice
- Dr. Albert Antwi-Boasiako, Director-General, Cyber Security Authority Director, Ghana
- Alassane Ndiaye, Magistrate, Deputy Director of the Criminal Affairs and Pardons Directorate Senegal

► **Enhanced tools for international co-operation – what changes does the Second Additional Protocol bring? [25 min]**

- Daniel Monteiro, Senior Prosecutor, Ministry of Justice, Cape Verde [5 min]
- Rajeshsharma Ramloll, Attorney General, Attorney General's Chambers, Mauritius [5 min]
- Moderated discussions [15 min]

► **Putting theory into practice: ways towards a more effective international co-operation – good stories and challenges in the region [45 min]**

- Jamila Akaaga Ade, Assistant Director, Head, Cyber Crime Unit, Department of Public Prosecutions, Federal Ministry of Justice Nigeria
- Jacqueline De Lange, Section Commander: Commercial, Financial and Cybercrime, INTERPOL NCB Pretoria, South Africa
- Moderated discussions

► **Conclusions [5 min]**

9h30-11h00

Workshop 10 - Regional workshop for Latin America and the Caribbean: Inter-agency cooperation on digital forensics

Languages: EN/ES/RO

Purpose: Many countries in LAC have undertaken efforts in recent years to establish specialized cybercrime units at the level of police and prosecutorial services, as well as units responsible for digital forensics. However, the organizational setup and functions of such units keep evolving and are not always based on international good practices. Furthermore, interagency cooperation between specialized cybercrime units and other services to ensure that electronic evidence is admissible in courts, remains a challenge.

The workshop is aimed at identifying good practices of setting up forensic units in police or prosecutors' office, how to ensure inter-agency co-operation and how to avoid conflicting competencies in the area of digital forensics.

Moderator/s: Fabio Bruno, Assistant Director, pro tempore, Applied Innovation, INTERPOL

Rapporteur: Michael Stawasz, Deputy Chief of Computer Crime, US Department of Justice

Secretariat: GLACY+ team, INTERPOL

► **Introduction and objective of the workshop [10 min]**

- Fabio Bruno, Assistant Director, pro tempore, Applied Innovation, INTERPOL

► **Digital forensic units: what are the current investigative practices and organizational capabilities and what are the limitations? [35 min]**

- Luciano Kuppens, Federal National Justice Council, Brazil
- Mauricio Fernandez Montalban, Specialized Unit on Cybercrime and Money Laundering, Public Ministry, Office
- Armando Jose Diaz, Head of the Cybersecurity Department & Member of the 24/7 Point of Contact Unit, Dominican Republic
- Open debates

► **Avenues for inter-agency cooperation on digital forensics [40 min]**

- Moderated discussions, by Fabio Bruno, Assistant Director, pro tempore, Applied Innovation, INTERPOL

► **Conclusions [5 min]**

11h30-13h00

Workshop 11 - Capacity building as a game changer: what makes a difference? (livestream)

Languages: EN/FR/ES/RO

Purpose: The aim of the workshop is to jointly identify examples of capacity building efforts that made a difference in terms of introducing sustainable changes in criminal justice systems and increased effectiveness in the fight against cybercrime. Over the past decade, governments, international organizations, private sector as well as civil society organizations have been implementing

	<p>numerous projects to address cybercrime at national, regional and international level. Some actions were more successful than others. It is important to capitalize on those experiences that had an impact and helped criminal justice authorities and societies to address cybercrime more effectively.</p> <p>Moderator/s: Jayanta Fernando, Data Protection Authority & Board Director, Sri Lanka</p> <p>Rapporteur: Daniela Andrović, Regulatory Authority for Electronic Communications and Postal Services, Serbia</p> <p>Secretariat: CyberSouth team</p> <p>► Introduction and objective of the workshop [5 min]</p> <p>► Panel discussion: what worked well and what less</p> <p>Examples of national and international capacity building efforts resulting in systematic changes, as well as of actions that did not produce the expected results. The moderator will address questions to panel members and open the floor for interventions on the shared practices and cases:</p> <p>The national experience (40 min)</p> <ul style="list-style-type: none"> - Chile (Mauricio Fernandez Montalban, Director, Specialized Unit on Cybercrime and Money Laundering, Public Ministry, Office) - Ghana (Albert Antwi-Boasiako, Director-General, Cyber Security Authority) - South Korea (Sunhwa Lee, prosecutor and Seonhyeon Kim, investigator) - Morocco (Ahmed Tahiri Alaoui, Head, Cybercrime Unit, Public Prosecution Office) - Sri-Lanka (Wasantha Perera, Secretary, Ministry of Justice) <p>The international experience (40 min)</p> <ul style="list-style-type: none"> - GFCE (Vouter Wenstra, Manager Global Outreach & Partnerships, Global Forum on Cyber Expertise - GFCE) - INTERPOL (Dong Uk Kim, Cybercrime Specialised Officer) - ICHIP (Anand Ramaswamy, International Computer Hacking and Intellectual Property, Addis Ababa, USDOJ) - OAS (Michael Stawasz, USDOJ) - OSCE (Martha Stickings, Deputy Head and Cybercrime Adviser, Strategic Police Matters Unit) - UNODC (Mustafa Erten, Regional Centre for Cybercrime) - World Bank (Keongmin Yoon, Counsel) - Council of Europe (Denise Mazzolani, CyberSouth Project Manager) <p>► Q&A</p> <p>► Conclusions (10 minutes)</p>
11h30-13h00	<p>Workshop 12 – Online xenophobia and racism v. freedom of expression</p> <p>Languages: EN/FR/ES/RO</p>

	<p>Purpose: With online hate speech – including racism and xenophobia – on the rise, societies are struggling with an effective response that also respects the fundamental right of the freedom of expression. A broad range of measures may be taken to address hate speech online (see the Council of Europe Recommendation on Hate Speech adopted in 2022). In this spectrum of measures, criminal law is an important last resort. In 2003, the first Protocol to the Convention on Cybercrime was opened for signature, addressing the “criminalisation of acts of a racist and xenophobic nature committed through computer systems” (ETS No. 189). In connection with the twentieth anniversary of this Protocol, a good practice study was undertaken on the experience of this treaty.</p> <p>The workshop aims to present findings of this study, to provide further guidance and to discuss challenges in addressing xenophobia and racism committed online while respecting the right to freedom of expression.</p> <p>Moderator: Jamila Akaaga Ade, Assistant Director Head, Cyber Crime Unit Department of Public Prosecutions Federal Ministry of Justice, Nigeria</p> <p>Rapporteur: Marko Juric, Associate Professor, Law Department, University of Zagreb, Croatia</p> <p>Secretariat: Octopus Project and T-CY Secretariat</p> <p>► Introduction and objective of the workshop</p> <ul style="list-style-type: none"> – Jamila Akaaga Ade, Assistant Director Head, Cyber Crime Unit Department of Public Prosecutions Federal Ministry of Justice, Nigeria <p>► Findings of the Good Practice Study</p> <ul style="list-style-type: none"> – Jan Kralik, Cybercrime Division, Council of Europe <p>► Challenges Facing in Addressing Xenophobia and Racism online</p> <ul style="list-style-type: none"> – Fernanda Teixeira Souza Domingos, Federal Circuit Prosecutor in Brasilia, Coordinator of the Advisory Group on Cybercrime at the Federal Prosecution Service, Brazil – Antonio Piña, Magistrate, General Council of the Judiciary, Spain <p>► Determining boundaries between hate speech and freedom of expression</p> <ul style="list-style-type: none"> – Steven Gatembu Kairu, Judge of Appeal, Court of Appeal. Judiciary, Kenya – Esther Agelan, Board Member, International Association of Women Judges, Kenya <p>► Conclusions</p>
11h30-13h00	<p>Workshop 13 – Strengthening 24/7 points of contact</p> <p>Languages: EN/FR/ES</p> <p>Purpose: The aim of the workshop is to further explore modalities for reinforcing the functioning of 24/7 Network of contact points under the Budapest Convention:</p>

	<p>sharing good practices for the efficient processing of requests received; identifying additional ways to increase the operability of the Network; understanding the roles and responsibilities of the Network with regard to the new tools of the Second Protocol to the Budapest Convention.</p> <p>Moderator: Virgil Spiridon, Deputy Head of the Romanian National Police</p> <p>Rapporteur: Catalin Zetu, Head of the Cybercrime Unit of the Romanian National Police</p> <p>Secretariat: Daniel Cuciurianu / iPROCEEDS-2 team</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [5 min] <ul style="list-style-type: none"> – Moderator’s notes – Secretariat ▶ Examples of international cooperation facilitated by the Network [25 min] <ul style="list-style-type: none"> – Erica O’Neil, Assistant Deputy Chief, Computer Crime and Intellectual Property Section, United States Department of Justice – Nenad Bogunović, Service for Combating Cyber Crime, Serbia ▶ Domestic implementation of the new responsibilities of the 24/7 Points of Contact [15 min] <ul style="list-style-type: none"> – Antonio Segovia Arancibia, Transnational criminal law professor, UAI University, Chile ▶ Promoting the network at domestic and international level [20 min] <ul style="list-style-type: none"> – Daniela Matei, Cybercrime Unit of the Romanian National Police, 24/7 PoC – Theophilus Botchway, Cyber Security Authority, 24/7 PoC of Ghana ▶ Q&A [15 min] ▶ Conclusions by the rapporteur [10 min] <ul style="list-style-type: none"> – Catalin Zetu, Head of the Cybercrime Unit of the Romanian National Police
11h30-13h00	<p>Workshop 14 – Interplay between cybersecurity and cybercrime</p> <p>Languages: EN/FR/ES/RO</p> <p>Purpose: This workshop explores the links between cybersecurity and the prevention and control of cybercrime. It will consider in particular the cooperation between criminal justice authorities and Computer Security Incident Response Teams (CSIRTs). The purpose of this session is to identify ways in which cooperation between criminal justice authorities and cybersecurity actors could improve, including through joint action against common threats, protection of critical infrastructure, and capacity building.</p> <p>Moderator/s: Matteo Lucchetti, Director, Cyber 4.0, Italy</p> <p>Rapporteur: Cecilia Popa, EU CyberNet</p>

	<p>Secretariat: Giorgi Jokhadze / Andrei Enachi</p> <ul style="list-style-type: none"> ▶ Introduction and objective of the workshop [5 min] <ul style="list-style-type: none"> – Moderator’s notes – Secretariat ▶ Common risks and threats: understanding the landscape for cooperation [15 min] <ul style="list-style-type: none"> – Private sector perspective: Aisling Kelly, Microsoft – Discussion ▶ Protection of critical infrastructure: joint responsibility [30 min] <ul style="list-style-type: none"> – Ukraine: Anatasia Ponarina, State Security Service – South Africa: Jacqueline Fick, CEO, VizStrat Solutions – Discussion ▶ Capacity building for improved security and resilience [20 min] <ul style="list-style-type: none"> – César Moliné Rodríguez, EU CyberNet LAC4, Latin America and Caribbean Cyber Competence Centre ▶ Options for improved cooperation between law enforcement and CSIRTs [15 min] <ul style="list-style-type: none"> – Discussion: operational examples and suggestions by participating countries and organisations ▶ Conclusions [5 min]
14h30-17h00	<p>Closing plenary and conclusions</p> <p>Languages: EN/FR/ES</p> <ul style="list-style-type: none"> ▶ Key takeaways from workshops [14h45-15h15] <ul style="list-style-type: none"> – Summary of each workshop ▶ Lessons from 10 years of Cybercrime Programme Office of the Council of Europe (C-PROC) [15h15-16h15] <ul style="list-style-type: none"> – Moderator: Virgil Spiridon, Deputy Head of the Romanian National Police ▶ Keynotes: <ul style="list-style-type: none"> – Bjørn Berge, Deputy Secretary General, Council of Europe – Traian Hristea, State Secretary, Ministry of Foreign Affairs, Romania – Sabin Pop, H.E. Ambassador, Permanent Representative of Romania to the Council of Europe (1995-2001)

- Gheorghe Magheru, H.E. Ambassador, Permanent Representative of Romania to the Council of Europe (2001-2006)
- Stelian Stoian, H.E. Ambassador, Permanent Representative of Romania to the Council of Europe (2006-2013)

▶ **Treaty event**

▶ **Panel of C-PROC project managers on the impact of C-PROC to date – the way ahead – takeaways from side-events:**

- Catalina Stroe, Project Manager GLACY
- Giorgi Jokhadze, Project Manager CyberEast
- Nina Lichtner, Project Manager Octopus Project
- Dan Cuciurianu, Project Manager iPROCEEDS-2
- Denise Mazzolani, Project Manager CyberSouth

▶ **Outlook 2024 and conclusions [16h15-17h00]**

- Concluding panel
- Key messages of the Octopus Conference