Octopus Conference 2023

13-15 December 2023 – Bucharest, Romania

Conference Programme - Overview

Version 9 Oct 2023

WED, 13 DECEMBER 2023			
8h30-9h30	*Welcome coffee and registration*		
9h30-11h00	**Opening plenary session** EN/FR/ES ► Opening ► Setting the scene: challenges		
11h00-11h30	*Coffee-break*		
11h30-13h00	**Plenary session** [continued] EN/FR/ES ► Setting the scene: solutions		
13h00-14h30	*Group photo and Lunch break*		
14h30-16h00	**Workshop 1** EN/FR/ES/RO ► Global state of cybercrime legislation	**Workshop 2** EN/FR/ES/RO ► Spontaneous information sharing	**Workshop 3** EN/FR/ES ► Automatic detection of child sexual exploitation and abuse materials
16h00-16h30	*Coffee-break*		
16h30-18h00	**Workshop 4** EN/FR/ES/RO ► Synergies between the Budapest, Lanzarote, Istanbul and Trafficking Conventions	**Workshop 5** EN/FR/ES/RO ► The interplay of cybercrime and financial investigations	**Workshop 6** EN/FR/ES ► Generative artificial intelligence: threats and benefits in criminal justice
18h00-20h00	*Social event*		

THU, 14 DECEMBER			
9h30-13h00 *[coffee-break 11h00-11h30]*	**Project event:** EN ► From CyberEAST to CyberEast+	**Project event:** EN ► From iPROCEEDS-2 to CyberSEET	**Project event:** EN/FR/ES ► From GLACY+ to GLACY-e
13h00-14h30 Lunch break			
14h30-18h00		**Project event:** EN/FR ► From CyberSouth to CyberSouth+	
15h30-16h00	*Coffee-break*		
16h30-18h00	**Lightning talks** EN/FR/ES/RO		

FRIDAY, 15 DECEMBER				
9h30-11h00	**Workshop 7**: EN ► Regional Workshop for Asia	**Workshop 8:** EN ► Regional Workshop for Pacific	**Workshop 9:** EN/FR ► Regional Workshop for Africa	**Workshop 10** EN/ES ► Regional Workshop for Latin America and the Caribbean
11h00-11h30	*Coffee-break*			
11h30-13h00	**Workshop 11** EN/FR/ES/RO ► Capacity building as a game changer: what makes a difference?	**Workshop 12**: EN/FR/ES/RO ► Online xenophobia and racism v. freedom of expression	**Workshop 13** - EN/FR/ES ► Strengthening 24/7 points of contact	**Workshop 14**: EN/FR/ES/RO ► The interplay between cybersecurity and cybercrime
13h00-14h30	► **Special event: Romania/Council of Europe cooperation on cybercrime** ► **Treaty ceremony** *Lunch break*			
14h30-16h30	**Closing plenary and conclusions** EN/FR/ES ► Key takeaways from workshops ► Outlook for 2024 ► Conclusions of the conference			
16h30-17h00	*Networking coffee*			
18h00	*End of conference*			

Detailed Programme

WED, 13 DECEMBER 2023	
9h30-13h00 Coffee break *11h00-11h30*	**Opening plenary session** Languages: EN/FR/ES Purpose: This plenary session is designed to set the scene for subsequent conference sessions and exchanges between participants. Each of the "challenges" and "solutions" will be introduced by one or two speakers and be followed by brief discussions. ► **Opening** ► **Setting the scene: challenges and solutions** – Ransomware and the Counter Ransomware Initiative – OSINT and e-evidence of war crimes: Lessons learned from the Russian aggression against Ukraine – Cybercrime v. freedom of expression – Legal frameworks: the Convention on Cybercrime and its Protocols – Capacity building: 10 years of Cybercrime Programme office of the Council of Europe (C-PROC)
14h30-16h00	**Workshop 1 - Global state of cybercrime legislation** Languages: EN/FR/ES 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. ► **Introduction and objective of the workshop** ► **From 2013 to 2023: Ten years of progress in legislation on cybercrime and electronic evidence** ► **Examples of recent reforms** ► **Challenges and risks** ► **Conclusions**
14h30-16h00	**Workshop 2 - Spontaneous information sharing** Languages: EN/FR/ES Purpose: Criminal justice authorities often possess valuable information that it believes 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. ► **Introduction and objective of the workshop** ► **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** ► **Panel discussion on the use of Article 26 of the Convention by Parties providing information: what are the procedures and conditions?** ► **Panel discussion on receiving spontaneous information: How can it be used as evidence?** ► **Conclusions**
14h30-16h00	**Workshop 3 – Automatic detection of child sexual exploitation and abuse materials** Languages: EN/FR/ES 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. ► **Introduction and objective of the workshop**

	► **Advancements in automated detection and report optimization** ► **Enhancing obligations and overcoming challenges** ► **Collaborative solutions & policy implementation** ► **Conclusions**
[13 Dec, 16h30-18h00]	**Workshop 4 - Synergies between Budapest, Lanzarote, Istanbul and Trafficking Conventions for safer cyberspace** Languages: EN/FR/ES/RO 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. The aim of this workshop is to further enhance synergies between four different – but interconnected – Conventions: - 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) ► **Introduction and objective of the workshop** ► **Criminal justice action: need to address the gaps before pursuing the synergies** ► **Work on prevention and protection: a different perspective** ► **Countering cyberviolence: potential for synergies** ► **Conclusions**
[13 Dec, 16h30-18h00]	**Workshop 5 – The interplay of cybercrime and financial investigations** Languages: EN 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. ► **Introduction and objective of the workshop** ► **Online Criminal Money Flow and Money Laundering Typologies** ► **Cooperation in the search, seizure and confiscation of online crime proceeds** ► **New tools and techniques for financial investigation in cybercrime cases** ► **Conclusions**
[13 Dec, 16h30-18h00]	**Workshop 6 - Generative artificial intelligence: threats and benefits in criminal justice** Languages: EN/FR/ES Purpose: Artificial Intelligence in the criminal justice sector can both represent a serious threat or 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. ► **Introduction and objective of the workshop** ► **Cybercrime and generative AI: threats and opportunities** ► **Addressing generative AI e-evidence: key issues, threats and benefits** ► **Conclusions**
THU, 14 DECEMBER	
9h30-16h30 Coffee break *11h00-11h30* *Lunch break* *13h00-14h30*	**Project event: From CyberEAST to CyberEast+** Languages: EN 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. ► **Opening session** ► **Closing of the CyberEast Project** ► **Discussion of the CyberEast+ Project** ► **Meeting of Policy Makers on Cybercrime Policies in the Eastern Partnership region**
9h30-16h30 *Coffee break 11h00-11h30* *Lunch break 13h00-14h30*	**Project event: From iPROCEEDS-2 to CyberSEE** Languages: EN 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. ► **Opening session** ► **Closing event of the iPROCEEDS-2 Project** ► **Towards CyberSEE Project: regional meeting** ► **Essentials of the new project**
9h30-18h00 Coffee break *11h00-11h30* *Lunch break 13h00-14h30* Coffee break *15h30-16h00*	**Project event: From GLACY+ to GLACY-e** Languages: EN/FR/PT/ES 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. ► **Opening session** ► **Lessons learned from GLACY+**

	► **What can we expect next?** ► **Adoption of the declaration of principles for hub countries** ► **Closing remarks**
14h30-18h00 Coffee break *15h30-16h00*	**Project event: From CyberSouth to CyberSouth+** Languages: EN/FR 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. ► **Opening session** ► **CyberSouth assessment: assessment of the five project results** ► **Best practises and review of project implementation's modalities** ► **Priorities of the MENA region in the cooperation on cybercrime 2024-2026** ► **Closing remarks**
16h30-18h00	**Lightning talks** Languages: EN/FR/ES/RO 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. 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. We strive to ensure an appropriate balance of regions, professions, and relevance of subjects for discussion. Speakers using the format will be kept to a strict five-minute time limit, with four minutes for questions. You will be informed whether your proposal was selected mid November. ► **Introduction and objective of the session** ► **Lightning talks** ► **Conclusions**

FRIDAY, 15 DECEMBER	
9h30-11h00	**Workshop 7 - Regional workshop for Asia: Data protection as a facilitator for investigation and adjudication of cybercrime and cases involving electronic evidence** Languages: EN 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 to the protection of personal data faces major challenges. This is also true for criminal justice authorities who need to reconcile effective measures to obtain, process and share personal data that are needed in criminal investigations and proceedings with data protection requirements. Where these requirements are met, they facilitate the sharing of personal data also across borders and 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. The aim of this workshop is share experience – and discuss challenges – for countries of Asia on the setting up of data protection frameworks in order to permit a more effective criminal justice response to cybercrime. ► **Introduction and objective of the workshop** ► **Data protection safeguards in the Second Additional Protocol – why we needed them?** ► **Data protection as cornerstone of international police cooperation** ► **Addressing data protection – testimonials from countries** ► **The state's obligation to protect against crimes and the right to privacy: how to find the right balance?** ► **Conclusions**
9h30-11h00	**Workshop 8 – Regional workshop for Pacific: Challenges in implementing cybercrime laws in small jurisdictions in the Pacific** Languages: EN 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. 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. ► **Introduction and objective of the workshop** ► **What makes for an effective cybercrime legal framework, adapted to the needs of Pacific Island States?** ► **Making laws relevant: what challenges do Pacific Island States meet when working on their legislative reform?** ► **Conclusions**
9h30-11h00	**Workshop 9 – Regional workshop for Africa: The Convention on Cybercrime and the Second Protocol – key to international cooperation on electronic evidence** Languages: EN/FR 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. ► **Introduction and objective of the workshop – why should African countries consider Convention on Cybercrime and its Protocols?** ► **Enhanced tools for international co-operation – what changes does the Second Additional Protocol bring?** ► **Putting theory into practice: ways towards a more effective international co-operation – good stories and challenges in the region** ► **Conclusions**
9h30-11h00	**Workshop 10 - Regional workshop for Latin America and the Caribbean: Inter-agency cooperation on electronic evidence** Languages: EN/ES 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 aims 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. ► **Introduction and objective of the workshop** ► **Digital forensic units: what are the current investigative practices and organizational capabilities and what are the limitations?** ► **Avenues for inter-agency cooperation** ► **Conclusions**
11h30-13h00	**Workshop 11 – Capacity building as a game changer: what makes a difference?** Languages: EN/FR/ES Purpose: The aim of the workshop is to identify examples of capacity building efforts that have made a real difference in terms of enabling sustainable changes in criminal justice systems and of increased effectiveness of tools against cybercrime. Over the past decade, governments, international organizations, private sector as well as civil society organizations have been implementing 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. ► **Introduction and objective of the workshop** ► **Panel discussion: what worked well and what less** ► **Conclusions**
11h30-13h00	**Workshop 12 – Online xenophobia and racism v. freedom of expression** Languages: EN/FR/ES/RO 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. 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. ► **Introduction and objective of the workshop** ► **Findings of the Good Practice Study** ► **Challenges Facing in Addressing Xenophobia and Racism online** ► **Determining boundaries between hate speech and freedom of expression** ► **Conclusions**
11h30-13h00	**Workshop 13 – Strengthening 24/7 points of contact** Languages: EN/FR/ES Purpose: The workshop is to further explore modalities for reinforcing the functioning of 24/7 Network of contact points under the Budapest Convention: 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. ► **Introduction and objective of the workshop** ► **Examples of international cooperation facilitated by the Network** ► **Domestic implementation of the new responsibilities of the 24/7 Points of Contact** ► **Promoting the network at domestic and international level** ► **Conclusions**
11h30-13h00	**Workshop 14 – Interplay between cybersecurity and cybercrime** Languages: EN/FR/ES/RO 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. ► **Introduction and objective of the workshop** ► **Common risks and threats: understanding the landscape for cooperation**

	► **Protection of critical infrastructure: joint responsibility** ► **Capacity building for improved security and resilience** ► **Options for improved cooperation between law enforcement and CSIRTs** ► **Conclusions**
13h00 – 14h00	**Special event: Romania / Council of Europe cooperation on cybercrime** Languages: EN/RO Purpose: This special event is to reflect on the long-standing partnership of Romania and the Council of Europe in fostering global cooperation on cybercrime. Thirty years ago, in October 1993, Romania joined the Council of Europe. For some twenty years, Romania has been a strong partner of the Council of Europe in matters related to cybercrime, as a Party to the Budapest Convention (since 2004), by providing experts, and by contributing to and chairing the Cybercrime Convention Committee (T-CY). Ten years ago, in 2013, this cooperation was elevated to yet another level: in October 2013, the Government of Romania and the Council of Europe concluded a memorandum of understanding on the establishment of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest. C-PROC has supported more than 100 countries through more than 2000 capacity building activities since it became operational in April 2014.
14h00 – 14h30	**Treaty ceremony** ► **Signatures, ratifications or accessions to the Budapest Convention and its Protocols**
14h30-17h00	**Closing plenary and conclusions** Languages: EN/FR/ES ► **Key takeaways from workshops** ► **Outlook for 2024** ► **Conclusions**