

CYBERCRIME@COE UPDATE

April – June 2025

Highlights April – June 2025

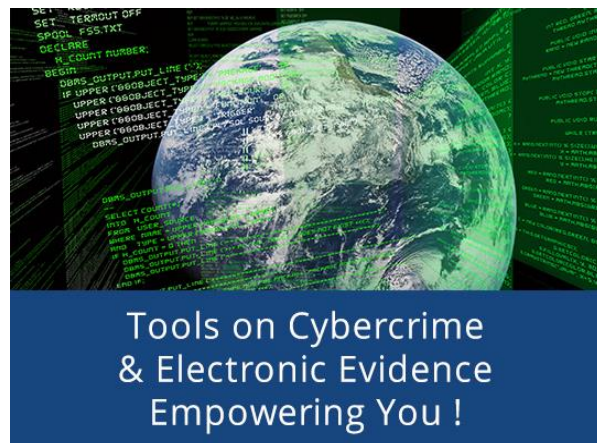
- [C-PROC: Over 500 professionals from 100 countries attended the Octopus Conference 2025](#)
- [4 States are taking important steps, Sao Tome and Principe and Vanuatu join the Convention on Cybercrime, Malta ratifies the First Protocol and Fiji signs the Second Protocol](#)
- [CyberSEE, CyberEast+, CyberSouth+, GLACY-e and Octopus Projects: The Cyber Games 2025 – Where practitioners come together to sharpen their skills for fighting against cybercrime](#)
- [CyberSEE project supports Serbia's efforts to develop a new Cybercrime Strategy](#)
- [CYBERKOP Action - Octopus Project: Strengthening Capacities on International Judicial Cooperation](#)
- [C-PROC: Regional Cybercrime Cooperation Training Exercise](#)



Follow us



The [Cybercrime Programme Office of the Council of Europe \(C-PROC\)](#) is on LinkedIn. Join our community of professionals!



Tools on Cybercrime
& Electronic Evidence
Empowering You !

CYBOX

Designed as a multi-tenancy solution leveraging the widely recognised Moodle Workplace platform, [CYBOX](#) introduces a new approach for C-PROC to capacity-building and training.



ONLINE
TRAINING
PLATFORM

Visit our Octopus Platform

The [Octopus Platform](#) aims to provide information on cybercrime and electronic evidence. Through the platform, you can access country wiki profiles on cybercrime legislation and policies, as well as training materials.

Save the date!

- 04–05 August 2025: Regional exercise on 24/7 POC Network, Fiji
- 01–04 September 2025: Underground Economy 2024, France
- 29–30 September 2025: Eurojust-Council of Europe Workshop, The Netherlands
- September–November 2025: Cyber-skills Sharing Programme, Global
- 01 October 2025: Annual meeting of the 24/7 POC Network, The Netherlands
- 02–03 October 2025: EUROPOL Conference, The Netherlands

UPDATE: Convention on Cybercrime and Cybercrime Convention Committee (T-CY)

Convention on Cybercrime

Opened for signature: 23 November 2001

Parties as of 30 June 2025: 80

Signatories and States invited to accede as of 30 June 2025: 15

T-CY

Members as of 30 June 2025: 80 States Parties

Observer States as of 30 June 2025: 15

Observer Organisations as of 31 March 2025: 11

STRASBOURG, FRANCE, 04 & 05 June 2025

4 States are taking important steps, Sao Tome and Principe and Vanuatu join the Convention on Cybercrime, Malta ratifies the First Protocol and Fiji signs the Second Protocol



On Wednesday, 04 June 2025, the Minister of Justice of Malta, Mr Johnathan Attard, deposited the instrument of ratification of the [First Additional Protocol](#) to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). [\[READ MORE\]](#)

STRASBOURG, FRANCE, 18 June 2025

Seychelles invited to accede to the Convention on Cybercrime



On 18 June 2025, Seychelles has been invited to accede to the [Convention on Cybercrime](#) (Budapest Convention). The invitation to accede is valid for five years from its adoption. This is also a result of capacity building activities through the projects of the [Cybercrime Programme Office](#) of the Council of Europe (C-PROC). [\[READ MORE\]](#)

STRASBOURG, FRANCE, 25 June 2025

The T-CY adopts a new Guidance Note on “Spontaneous Information”



The criminal justice authorities of one country may possess information that can assist the authorities of another country – who may not even be aware that this information exists – in their criminal investigations. Such information may be shared “spontaneously” – and without a prior request between authorities of different countries according to Article 26 of the [Convention on Cybercrime](#) (Budapest Convention). [\[READ MORE\]](#)

- ▶ THE CONVENTION PROVIDES A LEGAL FRAMEWORK FOR INTERNATIONAL COOPERATION ON CYBERCRIME AND ELECTRONIC EVIDENCE SUBJECT TO RULE OF LAW SAFEGUARDS (ARTICLE 15)
- ▶ PARTIES ARE MEMBERS OF THE CYBERCRIME CONVENTION COMMITTEE (T-CY) AND SHARE INFORMATION AND EXPERIENCE, ASSESS IMPLEMENTATION OF THE CONVENTION, AND INTERPRET THE CONVENTION THROUGH GUIDANCE NOTES
- ▶ PARTICIPATION IN THE NEGOTIATION OF FUTURE INSTRUMENTS AND THE FURTHER EVOLUTION OF THE BUDAPEST CONVENTION
- ▶ IMPROVED PARTNERSHIPS AND COOPERATION ALSO WITH THE PRIVATE SECTOR
- ▶ STATES REQUESTING ACCESSION OR HAVING ACCEDED MAY BECOME PRIORITY COUNTRIES FOR CAPACITY BUILDING PROGRAMMES

ARTICLE 37 BUDAPEST CONVENTION: PROCEDURE FOR ACCESSION

STEPS TOWARDS ACCESSION

- ▶ PREPARATION OF DOMESTIC LEGISLATION TO TRANSPOSE SUBSTANTIVE AND PROCEDURAL POWERS OF THE BUDAPEST CONVENTION
- ▶ LETTER BY GOVERNMENT TO THE SECRETARY GENERAL OF THE COUNCIL OF EUROPE EXPRESSING INTEREST IN ACCEDING TO THE BUDAPEST CONVENTION
- ▶ CONSULTATION OF THE PARTIES TO THE CONVENTION BY THE SECRETARIAT
- ▶ UPON CONSENSUS BY THE PARTIES: THE REQUESTING STATE IS INVITED TO ACCEDE
- ▶ COMPLETION OF INTERNAL PROCEDURES WITHIN REQUESTING STATE (SIMILAR TO RATIFICATION OF ANY INTERNATIONAL TREATY)
- ▶ DEPOSITING THE INSTRUMENT OF ACCESSION AT THE COUNCIL OF EUROPE



FOR MORE INFORMATION CONTACT:
CYBERCRIME@COE.INT

UPDATE: Joint Project Initiatives

GLACY-e, CyberEast+, CyberSEE, CyberSouth+, CyberSPEX, CyberUA and Octopus

BUCHAREST, ROMANIA, 07–11 April 2025

In person | C-PROC: Regional Cybercrime Cooperation Training Exercise



Based on a fictitious scenario, participants, under the guidance of the Council of Europe consultants and experts of the Romanian National Cyber Security Directorate, handled simulated attacks on electoral infrastructure and investigated links to criminal groups interfering with elections through information operations. Real-life skills for forensic analysis and online investigations to identify potential perpetrators and collect intelligence and evidence were tested during the training exercise. [\[READ MORE\]](#)

STRASBOURG, FRANCE, 12–14 May 2025

In person | CyberEast+, CyberSEE & Octopus Project – CYBERKOP Action: Stakeholders from the justice sector, law enforcement, and civil society exchanged views on internet regulations and innovations during EuroDIG 2025

Around 34 stakeholders supported by [CyberEast+](#) and [CyberSEE](#), joint projects of the Council of Europe and of the European Union, and by the CYBERKOP Action of the Octopus Project, exchanged views on public policy issues related to internet governance. [...] Through their active participation, the delegates strengthened their capacities to align national legal and policy frameworks with European and international standards. [\[READ MORE\]](#)



KUALA LUMPUR, MALAYSIA, 20–23 May 2025

In person | CyberSEE, CyberEast+, CyberSouth+, GLACY-e and Octopus Projects: The Cyber Games 2025 – Where practitioners come together to sharpen their skills for fighting against cybercrime



This inaugural edition marked a milestone in simulation-based exercises where top cybercrime investigators, digital forensics specialists and cybersecurity experts participate in team competitions to practice and share their skills to address real-life challenges in investigating ransomware attacks, including open source-based attribution, incident response, forensic imaging and tracing cryptocurrencies. [\[READ MORE\]](#)

PRAGUE, CZECHIA, 03–05 June 2025

In person | Regional participation in ISS World Europe 2025 to strengthening cybercrime investigation capacities supported by CyberSEE and CyberKOP



The event offered a variety of seminars and training sessions compiled into eight thematic tracks, covering tools, methodologies and equipment to enable law enforcement and intelligence communities to better tackle the challenges posed by the emerging challenges in cybercrime, cryptocurrencies, cyber money laundering, drug and human trafficking, artificial intelligence, darknet and other criminal activities conducted over telecommunications networks, the internet and social media. [\[READ MORE\]](#)

STRASBOURG, FRANCE, 04-06 June 2025

In person | C-PROC: Over 500 professionals from 100 countries attended the Octopus Conference 2025



Between 4-6 June 2025, the 15th edition of the [Octopus Conference](#) took place, in Strasbourg, France. Organised by the Cybercrime Programme Office of the Council of Europe ([C-PROC](#)), the event brought over 500 professionals from around 100 countries to exchange on electronic evidence, artificial intelligence crime, cyberviolence, cyber interference with democracy, crypto-investigations, pig-butchering, cybercrime as war crime, as well as youth and cybercrime.

The Conference was opened by Alain Berset (Secretary General of the Council of Europe), Jonathan Attard (Minister of Justice, on behalf of the Presidency of Malta of the Committee of Ministers) and Samuel Nartey George (Minister for Communication, Digital Technology and Innovations of Ghana).

Key messages emerged from each session and workshop, as well as from the overall conference, with a renewed invitation to make use of the tools provided by the framework of the [Convention on Cybercrime](#) (Budapest Convention) and related standards for continuing the international cooperation against cybercrime.

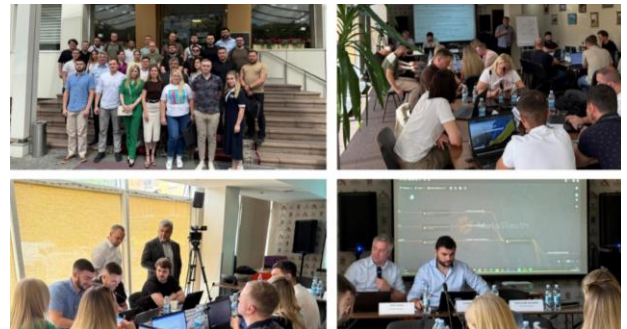
Participants (public sector, private sector, civil society, academia) also welcomed that [São Tomé and Príncipe as well as Vanuatu deposited instruments of accession to the Convention on Cybercrime, that Fiji signed the Second Protocol on electronic evidence to this treaty, and that Malta joined the First Protocol on xenophobia and racism](#) during the Conference. [\[READ MORE\]](#)

CHERNIVTSI, UKRAINE, 17-19 June 2025

In person | CYBERUA AND CYBEREAST+: Law enforcement, prosecutors and members of the cybersecurity community of Ukraine strengthen their response to cyberattacks in times of war

This activity was conducted within the framework of the [CyberUA project](#): Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine, which is part of the Council of Europe's Action Plan for Ukraine, "Resilience, Recovery, and Reconstruction" for 2023-2026, in collaboration with [CyberEast+](#), a joint project of the European Union and of the Council of Europe. Project counterparts engaged in real-time identification of online offenders and discussed good practices for the collection, securing and admissibility of electronic evidence essential for criminal prosecution.

Project counterparts engaged in real-time identification of online offenders and discussed good practices for the collection, securing and admissibility of electronic evidence essential for criminal prosecution. These practical, incident-based scenarios were designed to replicate real-world threats against critical infrastructure in Ukraine. Participants were guided through investigative procedures that adhere to both national legislation and international standards according to the [Convention on Cybercrime](#) (Budapest Convention) and its Second Additional Protocol, ensuring a comprehensive and compliant response.



A key component of the exercise included exploring operational implications of Ukraine's anticipated ratification of the [Second Additional Protocol](#) (2AP) to the Budapest Convention. Participants used direct cooperation channels with service providers, including issuing preservation requests and orders in emergency, and leveraging on tools such as the 24/7 Contact Network, SIENA (EUROPOL), and others. [\[READ MORE\]](#)

UPDATE: Octopus Project

Octopus project basics

Duration: January 2021 – December 2027

Budget: EUR 10 million

Funding: Voluntary contributions by Canada, France, Hungary, Iceland, Italy, Japan, Netherlands, United Kingdom, USA

Participating countries/regions: Global

RIGA, LATVIA, 07–08 April 2025

In person | Octopus Project: United Kingdom makes a further voluntary contribution to the Octopus Project



A delegation of domestic judicial and law enforcement institutions of Kosovo* visited Latvia, with the support of the [CYBERKOP Action](#) of the [Octopus Project](#) in view of, exchanging good practices and enhancing cross-border cooperation in key areas of justice reform and anti-corruption. Through in-depth discussions with Latvia's Ministry of Justice, Prosecutor General's Office, Court Administration, State Police, and the Corruption Prevention and Combating Bureau (KNAB), the delegation gained practical input on effective prosecutorial practices, digitalisation of the judiciary, and institutional approaches to preventing and investigating corruption. [\[READ MORE\]](#)

PRISTINA, KOSOVO*, April 2025

In person | Octopus Project - CYBERKOP Action: Kosovo* Police strengthens cybercrime response by updating the training program for first responders



The revised programme will equip officers with the practical tools and knowledge for identifying and classifying cyber offences, conducting initial investigations, handling of electronic evidence, and coordinating across institutions – thus ensuring first responders are well-prepared to act from the outset of a case. [\[READ MORE\]](#)

ISTOG, KOSOVO*, 12–13 June 2025

Online | Octopus project: Third webinar in the series on the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) – practical implications for prosecutors

A group of 24 judges, prosecutors, and legal professionals from across Kosovo* gathered in Istog on 12–13 June 2025 for an Introductory Training Course on Cybercrime and Electronic Evidence, organised under the [CYBERKOP Action](#) of the [Octopus Project](#), in cooperation with the Academy of Justice of Kosovo*. [\[READ MORE\]](#)



PRISTINA, KOSOVO*, 19–20 June 2025

In person | Octopus project - CYBERKOP Action: Finalization of the Draft Law on Personal Data Protection by Law Enforcement Institutions in Kosovo*

On 19–20 June 2025, the Information and Privacy Agency (IPA), with the support of the [CYBERKOP Action](#) of the [Octopus Project](#), held the second and final workshop dedicated to finalizing the draft Law on Personal Data Protection by Law Enforcement Institutions in Pristina, marking the successful conclusion of a year-long process. [\[READ MORE\]](#)



* This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

STRASBOURG, FRANCE, 30 June 2025

In person | Canada support to the Octopus Project for capacity building on cybercrime



The Government of Canada has made a voluntary contribution of CAD 975,000 to the [Octopus Project](#) of the Council of Europe in order to promote a global criminal justice response to cybercrime that is both effective and in line with human rights and rule of law requirements.

This new funding will provide much-needed support for enhanced action on cybercrime and electronic evidence in Southeast Asia - a region facing rapidly evolving cyber threats. It will focus on strengthening domestic legislation and criminal justice capacities on cybercrime and electronic evidence in line with the [Convention on Cybercrime](#), its [Second Additional Protocol](#), and related standards.

Canada remains a strong partner of the Council of Europe in international cooperation on cybercrime. Canada was among the first to sign the Convention on Cybercrime in 2001. It ratified it in 2015, being one of 80 countries worldwide to have joined this treaty thus far. It has also signed both of its additional protocols.

The Council of Europe welcomes this timely contribution of Canada to the Octopus Project, in particular, at a time when trusted partnerships are needed more than ever. [\[READ MORE\]](#)

CYBOX - Online platform for exchange, training, and resource sharing on cybercrime and electronic evidence

Designed as a multi-tenancy solution leveraging the widely recognised Moodle Workplace platform, [CYBOX](#) introduces a new approach for C-PROC to capacity-building and training.

CYBOX functions as a virtual hub for training on cybercrime and electronic evidence, offering tools to deliver both live and self-paced training activities. Institutions can create their own courses, manage enrolment, and organize virtual classrooms, making the platform a flexible solution for training and capacity building.

Beyond this, CYBOX acts as a central repository of cybercrime-related reference and training materials. Over time, this shared knowledge base will grow and serve as a valuable resource for trainers and practitioners around the world.



For countries or institutions interested to have their own tenant on the platform, it would be possible to:

- create a branded space for your institution;
- enrich your on- and offline trainings with a central platform for information exchange;
- facilitate training deliveries with virtual classrooms, tutorials, forums, assessments, evaluations, etc. and much more;
- build spaces for working groups and communities;
- configure custom automated reports for your activities.

Ultimately, CYBOX is designed to serve two main purposes: a repository of key materials, and a learning management system for [C-PROC](#) and partner countries.

UPDATE: Global Action on Cybercrime Enhanced (GLACY-e)

GLACY-e basics

Duration: August 2023 - 31 January 2026

Budget: EUR 5,556,000

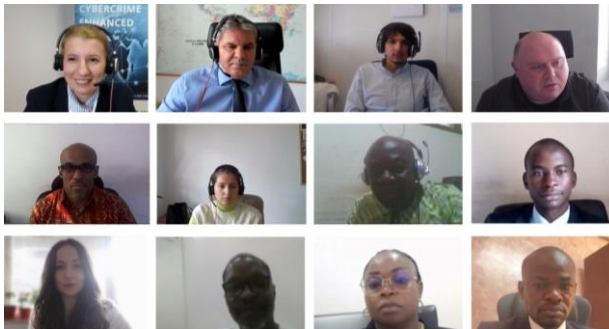
Funding: Joint project of the European Union and the Council of Europe

Participating countries: Global

Implementation: Cybercrime Programme Office (C-PROC) of the Council of Europe and INTERPOL

GLOBAL, 07 April 2025

Online | GLACY-e: Stakeholder workshop on the role and responsibilities of 24/7 Point of Contact



The workshop focused on the roles and responsibilities of the Contact Points, as outlined in Article 35 of the Convention, which facilitates expedited international cooperation on cybercrime and electronic evidence. Participants gained valuable insights from best practices shared by France and Luxembourg, leading to allocating the necessary resources and developing the capacities for processing international cooperation requests through this dedicated channel. [\[READ MORE\]](#)

SANTO DOMINGO, DOMINICAN REPUBLIC, 07-08 April 2025

In person | GLACY-e: Awareness raising workshops for legislators and service providers on the Second Additional Protocol to the Convention on Cybercrime



The workshop was an opportunity for legislators to strengthen their understanding of the [Protocol's](#) practical implications for cross-border access to electronic evidence in criminal investigations, direct cooperation with service providers and entities in other Parties, and tools for a speed up international cooperation between criminal justice authorities. [\[READ MORE\]](#)

FREETOWN, SIERRA LEONE, 29-30 April 2025

In person | Consultation and validation workshop of the Standard Operation Procedures on electronic evidence in Sierra Leone

As part of the ongoing cooperation between the authorities of Sierra Leone and the [GLACY-e](#) joint project of the European Commission and the Council of Europe on the drafting the Standard Operating Procedures (SOPs) on electronic evidence for law enforcement and prosecutors, a two-day consultation and validation workshop was organised by the national working group.

The session offered the opportunity to present for consultation and validation the final draft version to key stakeholders such as Sierra Leone Police, Judiciary, Central Intelligence and Security Agency (CISA), Office of the Public Prosecutions and the Anti-Corruption Commission.



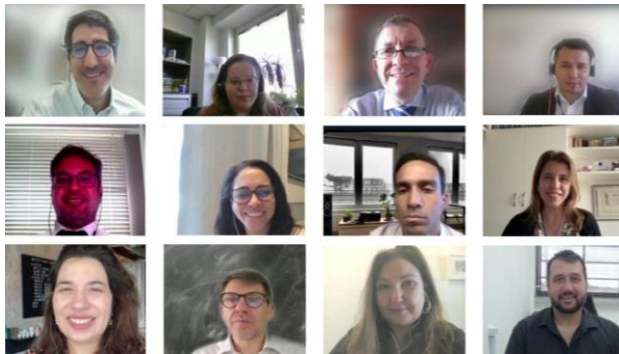
It is expected that the SOPs will enhance national legislation by formalizing the investigative powers into comprehensive rules and practices for the collection and analysis of electronic evidence. Additionally, they will augment the existing legal framework by addressing the technical aspects, thereby establishing uniform standards for the collection, preservation, and admissibility of electronic evidence.

Through this activity, the GLACY-e project will continue to provide strategic and technical support to Sierra Leone's authorities in strengthening national capacities to address cybercrime and handle electronic evidence effectively. [\[READ MORE\]](#)

BRAZIL, 19–30 May 2025**Online | Brazilian federal trainers start rolling out cybercrime training at state level**

Between 19–30 May 2025, two federal prosecutors trained previously under the [GLACY-e](#) joint project of the European Union and the Council of Europe coached a group of 25 state prosecutors in a second iteration of the Train of Trainers Programme facilitated by the same project. As underlined during the training, prosecutors are facing several challenges stemming not only from different understanding of concepts but also from the extraterritorial nature of the electronic evidence.

Giving the scale and complexity of cyber-attacks and exploitation of computer systems in Brazil, as well as the criminal cases involving electronic evidence, the ability of criminal justice authorities to conduct effective investigations and cooperate at international level is paramount. [\[READ MORE\]](#)

**STRASBOURG, FRANCE and ONLINE, 06 June 2025****In person | 3rd GLACY-e Steering Committee assesses mid-year progress and sets priorities for 2025**

On 6 June 2025, the [GLACY-e](#) joint project of the European Union and the Council of Europe organised its 3rd Steering Committee Meeting, in Strasbourg and online.



The meeting brought together national coordinators from hub and selected project countries, alongside representatives of the European Commission, INTERPOL, and the Council of Europe's Cybercrime Programme Office ([C-PROC](#)).

During the opening session, the representatives from the European Commission, INTERPOL and the Council of Europe reaffirmed their joint commitment to strengthening global capacities to combat cybercrime and improve access to electronic evidence through the GLACY-e project. [\[READ MORE\]](#)

UPDATE: Enhanced action on cybercrime for cyber resilience in Eastern Partnership States (CyberEast+)

CyberEast+ basics

Duration: 1 March 2024 – 28 February 2027

Budget: EUR 3.9 million (EU 90%, COE 10%)

Funding: European Union and the Council of Europe

Participating countries: Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine

Implementation: Cybercrime Programme Office (C-PROC) of the Council of Europe

KYIV, UKRAINE, 14–16 April 2025

In person | CyberEast+: Ukrainian law enforcement representatives benefited from the Specialised Course on Network and Malware Investigations



The National Security and Defence Council of Ukraine, in partnership with [CyberEast+](#), a joint endeavour of the European Union and of the Council of Europe, organised a Specialised Course on Network and Malware Investigations between 14 and 16 April 2025 in Kyiv, Ukraine. [\[READ MORE\]](#)

CHISINAU, MOLDOVA, 24–25 April 2025

In person | CyberEast+: Eastern Partnership counterparts increased their knowledge on judicial training programmes and resources developed by the Council of Europe



Some 25 project stakeholders, representing law enforcement and judicial training institutions/academies from Armenia, Azerbaijan, the Republic of Moldova and Ukraine, with the support of the Council of Europe, mapped the existing domestic training strategies on cybercrime and electronic evidence and assessed existing needs and gaps. [\[READ MORE\]](#)

YEREVAN, ARMENIA, 29–30 April 2025

In person | CyberEast+: Project partners from the Republic of Armenia analyse the benefits of common tools for incident/evidence handling and digital forensics



Representatives of law enforcement agencies and the cybersecurity community of the Republic of Armenia, engaged in a training on the use of common tools for incident/evidence handling and digital forensics, organised in the framework of [CyberEast+](#), a joint project of the European Union and of the Council of Europe. [\[READ MORE\]](#)

KYIV, UKRAINE, 05–07 May 2025

In person | CyberEast+: Ukrainian law enforcement representatives enhanced their skills on cybercrime investigations and computer forensics during Intermediate-Level Training



Over 28 law enforcement officials, alongside trainers and staff of the Academy, some of whom had attended the First Responder Training in February 2025, engaged in a series of practical exercises designed to enhance their competences in handling cybercrime cases and collection of electronic evidence. [\[READ MORE\]](#)

CHISINAU, REPUBLIC OF MOLDOVA, 20–22 May 2025

In person | CyberEast+: Defence attorneys from the Republic of Moldova engage in HELP Training Course on cybercrime and electronic evidence



The training was based on the [Council of Europe HELP online Course on Cybercrime and Electronic Evidence](#), which comprises [seven modules](#). The course focuses on legal tools and good practices for effectively addressing cybercrime and handling electronic evidence, in compliance with human rights standards. [\[READ MORE\]](#)

CHERNIVTSI, UKRAINE, 29–30 May 2025

In person | CyberEast+: Key stakeholders from Ukraine analyse the benefits of common tools for cybersecurity incident/evidence handling and digital forensics



On 29 and 30 May 2025, participants in the training examined the Standard Operating Procedures for cooperation between computer security incident response teams (CSIRTs) and Law enforcement in Ukraine that were developed under the [CyberEast project](#).

A set of amendments were proposed, considering current cybercrime threats and trends, further exacerbated by the ongoing armed aggression of the Russian Federation against Ukraine. Discussions revolved around compatible cyber-incident/cybercrime reporting platforms, as well as tools for gathering, processing and analysing electronic evidence. The delegates provided examples from their domestic legislation of effective cooperation mechanisms and exchanged views on incident response policies. [\[READ MORE\]](#)

YYEREVAN, ARMENIA, 10–11 June 2025

In person | CyberEast+: Armenian project stakeholders take stock of reporting mechanisms and discuss action plan on addressing cyberviolence

On this occasion, two Council of Europe consultants introduced the standards and good practices on cyberviolence and the tools available under the [Budapest](#), [Lanzarote](#) and [Istanbul](#) Conventions of the Council of Europe, as well as the [First Additional Protocol to the Convention on Cybercrime on Xenophobia and Racism](#) and the [Cyberviolence platform](#).



Project stakeholders exchanged views on initiatives meant to prevent and combat cyberviolence, through criminal justice tools (cybercrime) as well as alternative responses, such as awareness raising campaigns, support to victims and the possibility of anonymous reporting. [\[READ MORE\]](#)

BAKU, AZERBAIJAN, 18–19 June 2025

In person | CyberEast+: Azerbaijani partners gain knowledge on cooperation mechanisms under the Convention on Cybercrime and its Second Protocol

Around 20 participants from the State Service of Special Communication and Information Security, the Ministry of Justice, the Prosecutor General's Office, the Ministry of Digital Development and Transport, the State Security Service and the Ministry of Internal Affairs examined the tools, opportunities and requirements for sending and processing requests for international cooperation in criminal cases concerning electronic evidence, in line with the [Convention on Cybercrime](#). [\[READ MORE\]](#)



UPDATE: Enhanced cooperation on cybercrime and electronic evidence in the Southern Neighbourhood Region (CyberSouth+)

CyberSouth+ basics

Duration: January 2024 – December 2026

Budget: EUR 3.890 million

Funding: Joint project of the European Union and the Council of Europe

Participating countries: Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, Palestine* and Tunisia

Implementation: Cybercrime Programme Office (C-PROC) of the Council of Europe

** This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Council of Europe and European Union member States on this issue.*

RAMALLAH, PALESTINE*, 08-09 April 2025

Online | Workshop on investigating the illegal use of virtual assets for criminal justice professionals in Palestine*

The [CyberSouth+](#) project organised an online workshop on investigating the illegal use of virtual assets for prosecutors and law enforcement representatives.



Real-world case studies were used to ensure the Palestinian criminal justice professionals gain a solid understanding of types of virtual assets, how they work, how transactions can be traced and what data and e-evidence should be obtained in the event of an investigation. [\[READ MORE\]](#)

REGIONAL, 15 April 2025

Online | Regional workshop on the introduction of the First Protocol on Xenophobia and Racism

The [CyberSouth+](#) project organised an online regional workshop introducing the [First Additional Protocol to the Convention on Cybercrime](#) which focuses on the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

The participating criminal justice representatives showed notable interest in discussing the relevance and impact of the First Additional Protocol and topics such as accessing e-evidence through international cooperation and freedom of expression. [\[READ MORE\]](#)

TUNIS, TUNISIA, 15-16 April 2025

In person | Regional training for first responders to cybercrime and electronic evidence for law enforcement representatives

The [CyberSouth+](#) project organised a training session for first responders to cybercrime and other criminal investigations involving electronic evidence.

Given the increasing use of technology, e-evidence has become a crucial element in virtually all types of criminal investigations as such, the criminal justice authorities must keep up with the latest investigative techniques, technological advancements, and domestic legal frameworks. [\[READ MORE\]](#)



KOLEA, ALGERIA, 12-15 May 2025

In person | Advanced judicial training on cybercrime and electronic evidence for magistrates in Algeria

The [CyberSouth+](#) project supported the High School for Magistrates and the Algerian Ministry of Justice in the organisation of an advanced judicial training on cybercrime and electronic evidence for magistrates.

The interactive sessions enabled the 25 participating magistrates to deepen their knowledge on the provisions of the [Convention on Cybercrime \(Budapest Convention\)](#), as well as on technical subjects, including electronic evidence and cryptocurrencies. The participants were immersed in a mock trial exercise that afforded them an opportunity to apply the acquired knowledge and enhance their practical skills. [\[READ MORE\]](#)

AMMAN, JORDAN, 19–22 May 2024***In person* | Advanced judicial training on cybercrime and electronic evidence for magistrates**

The [CyberSouth+](#) project, in cooperation with the Jordanian Judicial Institute, organised an advanced judicial training on cybercrime and electronic evidence in Amman.



An interactive methodology and a mock trial were used to enable the participants deepened their expertise on key cybercrime topics such as virtual currencies, electronic evidence, and the [Convention on Cybercrime \(Budapest Convention\)](#) and its Protocols. [\[READ MORE\]](#)

CAIRO, EGYPT, 27–28 May 2025***In person* | Training on investigating OCSEA for law enforcement and the judiciary**

The [CyberSouth+](#) project supported the Egyptian Ministry of Justice in the organisation of a training on investigating online child sexual exploitation and abuse (OCSEA) .



The participants were engaged in a practical case scenario that allowed them to discuss life-like aspects of investigating OCSEA cases. The training topics included reporting OCSEA cases, measures to be taken by the first responders, international legal standards, cooperation with national and international service providers, investigation techniques and requirements for conducting victims' interviews, etc. The [CyberSouth+](#) project will continue to support the enhancement of capacities within the judicial and law enforcement sectors in Egypt carrying out capacity building activities. [\[READ MORE\]](#)

STRASBOURG, FRANCE, 03 June 2025***In person* | Second Steering Committee meeting of the project**

The [CyberSouth+](#) joint initiative of the European Union and the Council of Europe held its second Steering Committee meeting to review the implementation of activities and progress made during the first half of 2025.



On this occasion, the [CyberSouth+](#) project partners have outlined their priorities for the upcoming period and emphasized the need to strengthen the capacities of the judiciary, prosecution services, and law enforcement to effectively address emerging forms of cybercrime. [\[READ MORE\]](#)

TUNIS, TUNISIA, 24–25 June 2025***In person* | Regional Conference: Crisis management in the event of cyber-attacks**

The Council of Europe and DCAF (Centre for Security Sector Governance) coorganised the Regional conference: Crisis management in the event of cyber-attacks bringing together public officials and cybersecurity experts from the Southern Neighbourhood and the broader Mediterranean region to explore effective strategies for responding to cyber crises at both national and regional levels.



The discussions held covered a wide range of topics, including the typology of cyber threats, governance frameworks in times of crisis, the balance between emergency powers and legal safeguards, the role of national CERTs/CSIRTs, cross-border cooperation, strategic crisis communication, and public-private partnerships. [\[READ MORE\]](#)

UPDATE: Enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye (CyberSEE)

CyberSEE basics

Duration: January 2024 – June 2027

Budget: EUR 5.550 million

Funding: Joint project of the European Union (DG NEAR) and the Council of Europe

Participating countries: Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, Serbia, Türkiye and Kosovo*

** This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.*

SARAJEVO, BOSNIA AND HERZEGOVINA, 01–04 April 2025

In person | CyberSEE: Another step forward towards enhancing the skills in handling cybercrime and electronic evidence of judicial authorities in South-East Europe and Türkiye



The activity aligned with the [CyberSEE](#) project's objective to support sustainable judicial training in South-East Europe and Türkiye by developing cohesive pools of national trainers. This systematic approach was launched with the [Regional workshop](#) in October 2024, aimed at identifying training needs and it has continued with the assessment of development priorities and the identification of potential experts. [\[READ MORE\]](#)

SKOPJE, NORTH MACEDONIA, 03 April 2025

In person | CyberSEE: North Macedonia advances preparations for the ratification of the Second Additional Protocol to the Convention on Cybercrime

On 3 April 2025, the European Union–Council of Europe joint project [CyberSEE](#) supported the criminal justice authorities of North Macedonia in the organisation of a high-level domestic workshop in Skopje in view of implementation and further ratification of the Second Additional Protocol to the [Convention on Cybercrime](#) (Budapest Convention). [\[READ MORE\]](#)



WARSAW, POLAND, 08–09 April 2025

In person | CyberSEE: Enhanced regional capacity to tackle cybercrime in the digital finance era through a workshop on cryptocurrencies, electronic evidence and cooperation with service providers

Held at the National Prosecutor's Office of Poland under the auspices of the Polish Presidency of the Council of the European Union, the event brought together over 40 cybercrime investigators, prosecutors, judges, and representatives from Financial Intelligence Units (FIUs) from across South-East Europe to strengthen their practical skills and legal understanding in tackling cybercrime involving virtual currencies and digital evidence. [\[READ MORE\]](#)



ANKARA, TÜRKİYE, 09–10 April 2025

In person | CyberSEE: Türkiye advances legal and institutional measures to strengthen cybercrime response

Additional recommendations were made for amending the Türkiye's Criminal Procedure Law No. 5271/2004 and Cybersecurity Law No. 7545/2025 in view of full alignment with the international standards.

Both meetings contributed to a deeper understanding of the standards of the [Budapest Convention](#) and highlighted areas where national laws and training frameworks could be further strengthened. Participants identified key priorities for aligning domestic practices with international norms and discussed ways to enhance the national response to cybercrime through legal reforms and targeted capacity-building initiatives. [\[READ MORE\]](#)

SARAJEVO, BOSNIA AND HERZEGOVINA, 06 May 2025

***In person* | CyberSEE: Bosnia and Herzegovina continues its efforts towards the signature and implementation of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)**

On 6 May 2025, the European Union-Council of Europe joint project [CyberSEE](#), in cooperation with the criminal justice authorities of Bosnia and Herzegovina, organised a Domestic Expert Workshop on the Provisions of the [Second Additional Protocol](#) to the [Convention on Cybercrime](#) in Sarajevo to support the country's progress towards its signature and implementation.



The event brought together legal drafters, prosecutors, judges, and other key actors from state and entity levels, alongside representatives from the European Union Delegation to Bosnia and Herzegovina, the Council of Europe Office in Sarajevo, and experts from the Council of Europe's [Cybercrime Programme Office](#) (C-PROC).

[\[READ MORE\]](#)

VRDNIK, SERBIA, 15-16 May 2025

***In person* | CyberSEE project supports Serbia's efforts to develop a new Cybercrime Strategy**

On 15-16 May 2025, a domestic workshop to support the development of the Cybercrime Strategy in Serbia (2025–2030) was organised by the joint European Union and the Council of Europe [CyberSEE project](#), in cooperation with the Ministry of Internal Affairs in Vrdnik.



The workshop was aimed at supporting the national authorities in the process of the development of a comprehensive strategy and action plan to address cybercrime and electronic evidence, based on the emergency threats and the necessary capacities. [\[READ MORE\]](#)

BELGRADE, SERBIA, 27 May 2025

***In person* | CyberSEE supports Serbia's efforts to implement the Second Additional Protocol to the Convention on Cybercrime**

The event was organised in cooperation with the criminal justice authorities of Serbia, and gathered representatives from the Ministry of Justice, Supreme Public Prosecution Office, Ministry of Interior, Ministry of Telecommunication, Data Protection Authority, National Police and the [Delegation of the European Union to Serbia](#), alongside experts from the Council of Europe's [Cybercrime Programme Office \(C-PROC\)](#). Participants examined legal, institutional, and operational aspects of the [Second Additional Protocol's](#) implementation in the Serbian context.

Discussions focused on Serbia's ratification law, the guidance offered in the Explanatory Report to the Protocol, and the implications of EU Council Decision 2023/436, particularly the required reservations, declarations, and communications relevant to EU Member States and candidate countries. The meeting also explored the legal and procedural steps Serbia must undertake to effectively apply the Protocol's enhanced cooperation tools, such as direct cooperation with service providers, expedited disclosure of data, and joint investigations.



The workshop contributed to strengthening national understanding of the Protocol's requirements and helped clarify the roles and responsibilities of institutions involved in its implementation. It also served as an opportunity to consider the establishment of a national working group to guide future legislative reform in alignment with the Protocol's provisions. [\[READ MORE\]](#)

TIRANA, ALBANIA, 27–28 May 2025***In person* | CyberSEE continues to support Albania in aligning its legislation with the Second Additional Protocol to the Convention on Cybercrime**

The workshop convened representatives of the Ministry of Justice, members of the national working group responsible for steering the legislative reform process, and other institutional stakeholders. In a collaborative setting, legal practitioners, policy-makers and representatives from key public authorities engaged in advancing the national dialogue on reforming the domestic legislation for the implementation of the [Second Additional Protocol](#). The discussions were guided by Council of Europe consultants and legal experts, building on the Assessment Report previously prepared and shared with Albanian authorities.



The workshop also addressed drafting Albania's ratification law and related declarations and reservations under EU Council Decision 2023/436, emphasizing the need for legal coherence with existing domestic legislation and alignment with European human rights and data protection standards.

The activity facilitated consensus among stakeholders on legislative options and marked tangible progress in drafting the required legal amendments. It also provided a platform to agree on the next steps of the reform roadmap, further reinforcing national coordination and institutional readiness for the effective implementation of the Protocol. [\[READ MORE\]](#)

STRASBOURG, FRANCE, 06 June 2025***In person* | CyberSEE - Third meeting of the Project Steering Committee**

The [CyberSEE](#) joint project of the European Union and the Council of Europe held its third Steering Committee Meeting on 6 June 2025, at the Council of Europe premises in Strasbourg, France.



The meeting brought together representatives of the European Commission, the Council of Europe and officials from Public Prosecution Offices, Ministries of Justice, Police Cybercrime Units of all project countries.

The session was opened by the European Commission, which highlighted the growing cybercrime challenges in the region driven by emerging technologies such as Artificial Intelligence, online fraud, and online child exploitation. The importance of strengthening cooperation between the project and other European Union-funded initiatives in the region, such as the Regional Cooperation Council and Western Balkans Cyber Capacity Center, was underlined.

The meeting reviewed the project's progress over the past six months, including the support on implementation of legislative and institutional reforms, national cybercrime strategies and other capacity-building activities. [\[READ MORE\]](#)

UPDATE: Enhanced co-operation on e-evidence by EU Member States through the Second Protocol to the Budapest Convention (CyberSPEX)

CyberSPEX basics

Duration: 1 March 2024 – 28 February 2026

Budget: EUR 2.23 million

Funding: European Union (90%), Council of Europe (10%)

Participating countries: European Union Member States

BUCHAREST, ROMANIA, 14–15 April 2025

In person | CyberSPEX: Online Workshop on the implementation of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)



The [CyberSPEX project](#) organised the third meeting of its regional series on the implementation of the [Second Additional Protocol](#) to the [Convention on Cybercrime](#) (Budapest Convention). The meeting was held in cooperation with the Romanian Ministry of Justice and took place in Bucharest on 14–15 April 2025 with Central and Eastern European countries.

This successful event allowed representatives of Ministries of Justice, advisors, judicial authorities representatives and practitioners from Bulgaria, Croatia, the Czech Republic, Hungary, the Slovak Republic, Slovenia and Romania to meet and share common perspectives within the neighboring countries on the international cooperation in cybercrime and electronic evidence.

They exchanged practical views and challenges related to the implementation of the mechanisms and tools offered by the Second Additional Protocol - in particular related to public-private cooperation.

The similarities and common requirements of the Protocol and the [EU e-evidence regulation](#) were highlighted, with a view to enhance the cooperation and exchange of electronic evidence between the EU Member States and third Parties by implementing the two instruments in parallel. [\[READ MORE\]](#)

STRASBOURG, FRANCE, 02–06 June 2024

In person | CyberSPEX: Second Steering Committee, T-CY and Octopus Conference participation

The [CyberSPEX project](#) marked a significant month of activity in June 2025, reinforcing its role in supporting EU member states in the implementation of the [Second Additional Protocol](#) to the [Convention on Cybercrime](#).

On 2–3 June 2025, the project contributed to the [Cybercrime Convention Committee](#) (T-CY) by presenting the development of draft templates for Articles 6 to 8 of the Second Additional Protocol, marking a step forward in proposing common procedural instruments for cross-border access to electronic evidence under the Protocol.



Later that week, from 4 to 6 June, the CyberSPEX was instrumental in supporting the organization of the [Octopus Conference](#) 2025. In that context, CyberSPEX organized the [Main session 1-E-evidence: implementing the Second Protocol to the Convention on Cybercrime](#). The session gathered experts, policymakers, and practitioners to discuss both national and international approaches to putting the Protocol into effective practice as well as to highlight different approaches on the road to ratification.

To conclude a week of high-level engagement, CyberSPEX held its second Project Steering Committee meeting on 6 June in Strasbourg, France. Participants showed strong appreciation for the project's activities and technical resources, which are designed to aid national authorities in incorporating the Second Protocol into their domestic legislation. [\[READ MORE\]](#)

Inventory of activities (April – June 2025)

April 2025

CyberSPEX	Manual on the interaction between the Second Additional Protocol and corresponding instruments of the European Union, <i>desk research</i> , March–June 2025
Octopus Project - CYBERKOP Action	Kosovo* Police strengthens cybercrime response by updating the training program for first responders, <i>in person</i> , April 2025
CyberSEE	Regional judicial training on electronic evidence, Bosnia and Herzegovina, <i>in person</i> , 01–04 April 2025
CyberSEE	Domestic meeting with North Macedonian relevant institutions dedicated on the details of the 2AP and roadmap of the legislative reform process, North Macedonia, <i>in person</i> , 03 April 2025
GLACY-e	Stakeholder workshop on the role and responsibilities of 24/7 POC, Benin, Côte d'Ivoire, Cameroon, <i>online</i> , 07 April 2025
GLACY-e	Awareness workshop with the legislators on Second Additional Protocol, Dominican Republic, <i>in person</i> , 07 April 2025
GLACY-e	Awareness workshop with the service providers on Second Additional Protocol, Dominican Republic, <i>in person</i> , 08 April 2025
Octopus Project - CYBERKOP Action	Strengthening legal judicial cooperation through targeted study visit of domestic institutions of Kosovo* to Latvia, <i>in person</i> , 07–08 April 2025
C-PROC	Regional Cybercrime Cooperation Training Exercise on cybercrime/ security coordination, Romania, <i>in person</i> , 07–11 April 2025
CyberSouth+	Online workshop on investigating the illegal use of virtual assets for criminal justice professionals in Palestine*, <i>online</i> , 08–09 April 2025
CyberSEE, EUROJUST	Workshop on cryptocurrencies, e-evidence and cooperation with service providers, with EUROJUST, Poland, <i>in person</i> , 08–09 April 2025
CyberSEE	Domestic meeting on cybercrime training strategies at the Police Academy, Türkiye, <i>in person</i> , 09 April 2025
CyberSEE	Domestic meeting with Turkish Ministry of Justice and relevant institutions on legal reforms on cybercrime and electronic evidence, Türkiye, <i>in person</i> , 10 April 2025
CyberSPEX	Regional Meeting in support of the implementation of the Second Additional Protocol to the Budapest Convention, Central and Eastern-European countries, Romania, <i>in person</i> , 14–15 April 2025
CyberEast+	Training organised for Ukraine: Malware and Network Investigations, Ukraine, <i>in person</i> , 14–16 April 2025
CyberSEE, INTERPOL	41 st Operational Meeting of the INTERPOL Specialists Group on Crimes against Children, France, <i>in person</i> , 14–18 April 2025

CyberSouth+	Regional workshop on the introduction of the First Protocol on Xenophobia and Racism, <i>online</i> , 15 April 2025
GLACY-e	Support to drafting SOPs - debriefing session with the working group, Sierra Leone, <i>online</i> , 15 April 2025
GLACY-e	Support for data protection legislative reform - skeleton of the DP policy, Fiji, <i>desk study</i> , by 15 April 2025
CyberSouth+	Regional training for first responders to cybercrime and electronic evidence for law enforcement representatives, Tunisia, <i>in person</i> , 15–16 April 2025
GLACY-e, CyberEast+	Support for participation in the Cyber Crime Conference, with Cyber 4.0, Italy, <i>in person</i> , 16–17 April 2025
GLACY-e	Participation in EL PACCTO 2.0 Bi-regional LAC-EU Meeting, Belgium, <i>in person</i> , 23–25 April 2025
CyberEast+	Regional Meeting of Training Institutions on Cybercrime and Electronic Evidence, Republic of Moldova, <i>in person</i> , 24–25 April 2025
CyberSPEX	Contributions to the EJCN 18 th Plenary Meeting, The Netherlands, <i>in person</i> , 28–29 April 2025
GLACY-e	10 th Meeting of the Americas Working Group of Head of Units, Panama, <i>in person</i> , 28 April–02 May 2025
GLACY-e	Participation in the Launch of the Cyberlaw Study, Pacific, <i>online</i> , 29 April 2025
CyberEast+	Training on SOPs - Use of compatible tools for handling and forensics producing admissible evidence, Armenia, <i>in person</i> , 29–30 April 2025
GLACY-e	Support to drafting SOPs - consultation and validation session with key stakeholders, Sierra Leone, <i>in person</i> , 29–30 April 2025
GLACY-e	Support for 24/7 POC: Standard Operating Procedures, Fiji, <i>online</i> , 30 April 2025
Octopus Project	Good practice Study on addressing non-consensual dissemination of intimate images, <i>desk research</i> , April–June 2025
CyberSEE	Provide guidance to the North Macedonian national working group on the necessary amendments to existing national legal framework to implement 2AP provisions, North Macedonia, <i>online</i> , April–June 2025
CyberSEE	Assessment of the legislation of Bosnia and Herzegovina, benchmarked against 2AP provisions, <i>online</i> , April–August 2025
CyberSPEX	Further development of the Help Course, <i>desk research</i> , April–November 2025

May 2025

CyberSPEX	Manual on the interaction between the Second Additional Protocol and corresponding instruments of the European Union, <i>desk research</i> , March–June 2025
CyberEast+	Regular cybercrime training: ToT Cyber Police Ukraine - intermediate level, Ukraine, <i>in person</i> , 05–07 May 2025
GLACY-e	Africa Regional working group and operations, Cameroon, <i>in person</i> , 05–07 May 2025
CyberSEE	Expert workshop with BiH competent authorities on legal assessment and 2AP implementation, Bosnia and Herzegovina, <i>in person</i> , 06 May 2025
Octopus Project – CYBERKOP Action CyberEast+, CyberSEE,	Support participation in the European Dialogue on Internet Governance (EuroDIG) - 2025 Annual Conference, France, <i>in person</i> , 12–14 May 2025
CyberSouth+	Advanced judicial training on cybercrime and electronic evidence for magistrates in Algeria, <i>in person</i> , 12–15 May 2025
Octopus Project – CYBERKOP Action	Study visit of Kosovo* to the Council of Europe and European Court of Human Rights, France, <i>in person</i> , 12–15 May 2025
CyberSEE, EUROPOL	“Victim identification task force 16” with EUROPOL, AP Twins, The Netherlands, <i>in person</i> , 12–25 May 2025
GLACY-e	Support participation in Global Conference on Cyber Capacity, Switzerland, <i>in person</i> , 13–14 May 2025
GLACY-e	Awareness workshop on the Second Additional Protocol, Ecuador, <i>online</i> , 14 May 2025
CyberSEE	Domestic workshop to support the development of the Cybercrime Strategy (2025–2028), Serbia, <i>in person</i> , 15–16 May 2025
CyberSouth+	Advanced judicial training on cybercrime and electronic evidence for magistrates in Jordan, <i>in person</i> , 19–22 May 2025
CyberSPEX	Workshop about the provisions of the Second Protocol during the Cross-border Exchange of e-Evidence Course, in cooperation with CEPOL, Hungary, <i>in person</i> , 19–23 May 2025
GLACY-e	Training of Trainers Programme (ToT): Introductory Judicial Course (for prosecutors from state level), Brazil, <i>in person</i> , 19–30 May 2025
CyberEast+	HELP course for defence attorneys, Republic of Moldova, <i>in person</i> , 20–22 May 2025
C-PROC	The Cyber Games 2025 – Where practitioners come together to sharpen their skills for fighting against cybercrime, Malaysia, <i>in person</i> , 20–23 May 2025
GLACY-e	Support for data protection legislative reform - finalisation of the DP policy, Fiji, <i>online</i> , 21 May 2025
CyberSEE	Domestic meeting with Serbian relevant institutions dedicated on the details of the 2AP and roadmap of the legislative reform process, Serbia, <i>in person</i> , 27 May 2025

CyberSEE	Workshop with Albanian national key stakeholders to discuss the assessment and prepare the drafting process, Albania, <i>in person</i> , 27–28 May 2025
CyberSouth+	Training on investigating OCSEA for law enforcement and the judiciary, Egypt, <i>in person</i> , 27–28 May 2025
CyberEast+	Training on SOPs - Use of compatible tools for handling and forensics producing admissible evidence, Ukraine, <i>in person</i> , 29–30 May 2025

June 2025

CyberSPEX	Manual on the interaction between the Second Additional Protocol and corresponding instruments of the European Union, <i>desk research</i> , March–June 2025
T-CY, C-PROC	3 rd Meeting of the T-CY Working Group on Artificial Intelligence, France, <i>in person</i> , 01 June 2025
T-CY, C-PROC	32 nd Plenary Meeting of the Cybercrime Convention Committee (T-CY), France, <i>in person and online</i> , 02–03 June 2025
CyberEast+	Ukraine Workshop on Legislation and Coordination meeting, France, <i>in person</i> , 02–06 June 2025
CyberSouth+	2 nd Steering Committee meeting of the project, France, <i>in person</i> , 03 June 2025
CyberSEE, Octopus Project – CYBERKOP Action, ISS	Participation in the ISS World Europe 2025, Prague, <i>in person</i> , 03–05 June 2025
T-CY, C-PROC	15 th Octopus Conference on Cybercrime, France, <i>in person and online</i> , 04–06 June 2025
GLACY-e	3 rd Steering Committee Meeting, France, <i>in person and online</i> , 06 June 2025
CyberSEE	3 rd Steering Committee Meeting, France, <i>in person</i> , 06 June 2025
CyberSPEX	2 nd Steering Committee Meeting, France, <i>in person</i> , 06 June 2025
CyberEast+	National discussions on responsible reporting and cyberviolence: civil society, ISP and academia forum, Armenia, <i>in person</i> , 10–11 June 2025
GLACY-e	Handbook on implementation of cybercrime laws: First in person meeting of the Drafting Subcommittee, Tonga, <i>in person</i> , 10–12 June 2025
GLACY-e	Support for data protection legislative reform - briefing meeting with the Principal Secretary of the MoICT, Pacific, <i>online</i> , 11 June 2025
CyberSPEX	Contributions to the Annual SIRIUS SPoC Network Meeting in cooperation with the Cybercrime Department of the Polish National Prosecutors Office, Poland, <i>in person</i> , 11 June 2025
Octopus Project – CYBERKOP Action	Introductory Training Course for Judges and Prosecutors on Cybercrime and Electronic Evidence, Kosovo*, <i>in person</i> , 12–13 June 2025

CyberSPEX	Roundtable about the Second Additional Protocol during to the EuroISPA General Meeting, France, <i>in person</i> , 16–17 June 2025
GLACY-e	Participation in the First Annual Meeting of EL PACCTO 2.0, Peru, <i>in person</i> , 16–18 June 2025
CyberEast+	National exercise on investigation, forensics and interagency cooperation – in cooperation with CyberUA, Ukraine, <i>in person</i> , 17–19 June 2025
CyberEast+	Training on application of cooperation provisions of the Budapest Convention and its Second Protocol, Azerbaijan, <i>in person</i> , 18–19 June 2025
Octopus Project – CYBERKOP Action	Second workshop on drafting the Law on Personal Data Protection by Law Enforcement Institutions, Kosovo*, <i>in person</i> , 19–20 June 2025
CyberSouth+	Council of Europe - DCAF Regional Conference: Crisis management in the event of cyber-attacks, Tunisia, <i>in person</i> , 24–25 June 2025
GLACY-e	Participation in the national conference "Cybercrime - a global threat", Angola, <i>in person</i> , 26–27 June 2025

* Palestine: This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Council of Europe and European Union member States on this issue.

** Kosovo: This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

Coming next (July – September 2025)

July 2025

T-CY	Interpol Partners' Conference 2025 "Investing in a Safer World", France, <i>in person</i> , 02 July 2025
T-CY	Preventing the Cycle of Harm Briefing Event, France, <i>in person</i> , 03 July 2025
CyberSEE	High-Level Cybersecurity Conference, with the Regional Cooperation Council (RCC), European Commission (EC), and Western Balkans Cyber Capacity Center (WB3C), Montenegro, <i>in person</i> , 02–03 July 2025
CyberSEE, ICMEC, GLACY-e	Regional training on OCSEA investigations of peer-to-peer networks, with ICMEC, Romania, <i>in person</i> , 02–04 July 2025
Octopus Project – CYBERKOP Action	Support the Training on Investigation of Cybercrimes for First Responders, Kosovo*, <i>in person</i> , 03–04 July 2025
CyberSEE	Participation in the Final Session of the UN Working Group on Information Security, USA, <i>in person</i> , 07–11 July 2025
CyberSEE Project & Octopus Project – CYBERKOP Action	Regional Training on Money Laundering, Criminal Financing and Asset Recovery: New Tools and Technologies, Romania, <i>in person</i> , 07–11 July 2025
CyberSouth+	Training Workshop for multisectoral Committee members (child protection), Tunisia, <i>online</i> , 14–15 July 2025
T-CY	4 th Meeting of the T-CY Working Group on Artificial Intelligence, <i>online</i> , 15 July 2025
GLACY-e	Support to the legislative reform, Uruguay, <i>desk study</i> , by mid-July 2025
CyberSouth+	Training Workshop for the Delegate for Child Protection (DPE1), Sousse, Tunisia, <i>online</i> , 17–18 July 2025
CyberSouth+	Training Workshop for the Delegate for Child Protection (DPE2), Hammamet, Tunisia, <i>online</i> , 21–22 July 2025
GLACY-e	Support for the legislative process on data protection, Mozambique, <i>desk study</i> , July–September 2025
CyberSPEX	Prepare inventory of provider policies with respect to language of orders, WHOIS, notifications and confidentiality policies, <i>desk research</i> , July–September 2025
CyberSPEX	Mapping Study on the designation of authorities in EU m/s to be declared under art. 6.6, 7.5, 8.10, 14.7.c and 14.10.b in conjunction with authorities to be declared under the EU e-evidence package in cooperation with EJC (EUROJUST), <i>desk research</i> , July–September 2025
CyberSouth+	Adaptation of the judicial training materials on cybercrime and electronic evidence and national course delivery in Egypt, <i>online & in person</i> , July–November 2025

August 2025

CyberSPEX	Prepare inventory of provider policies with respect to language of orders, WHOIS, notifications and confidentiality policies, <i>desk research</i> , July–September 2025
CyberSPEX	Mapping Study on the designation of authorities in EU m/s to be declared under art. 6.6, 7.5, 8.10, 14.7.c and 14.10.b in conjunction with authorities to be declared under the EU e-evidence package in cooperation with EJCEN (EUROJUST), <i>desk research</i> , July–September 2025
GLACY-e	Regional exercise on 24/7 POC Network, Fiji, <i>in person</i> , 04–05 August 2025
GLACY-e	Participation in the ICT Senior Officials Meeting (PIF), Fiji, <i>in person</i> , 07–08 August 2025
GLACY-e	Train the trainers – introductory refresher course (new national trainers included), Dominican Republic, <i>in person</i> , 13–15 August 2025
GLACY-e	Train the trainers – adult trainer methodology course (new national trainers included), Dominican Republic, <i>in person/online</i> , August 2025
CyberSEE	Assessment of the North Macedonian national legislation, benchmarked against 2AP provisions, <i>online</i> , August 2025
CyberSPEX	Publication of the Manual on interaction between the Second Additional Protocol and corresponding instruments of the European Union (restricted), <i>desk research</i> , August 2025
GLACY-e	Regional training on cybercrime - design of the course, Papua New Guinea, <i>desk study</i> , by end-August 2025
GLACY-e	Support on legislation: Second Additional Protocol, Fiji, <i>desk study</i> , by end-August 2025
GLACY-e	Handbook on judicial training strategies for ASEAN countries, Philippines, <i>desk study</i> , by end-August 2025
Octopus Project, CYBERKOP Action	Update of the Guide on Seizing Cryptocurrencies, <i>online</i> , August–September 2025
CyberSouth+	Adaptation of the judicial training materials on cybercrime and electronic evidence and national course delivery in Egypt, <i>online & in person</i> , July–November 2025

September 2025

CyberSPEX	Prepare inventory of provider policies with respect to language of orders, WHOIS, notifications and confidentiality policies, <i>desk research</i> , July–September 2025
CyberSPEX	Mapping Study on the designation of authorities in EU m/s to be declared under art. 6.6, 7.5, 8.10, 14.7.c and 14.10.b in conjunction with authorities to be declared under the EU e-evidence package in cooperation with EJCEN (EUROJUST), <i>desk research</i> , July–September 2025
C-PROC	Underground Economy Conference, with Team CYMRU, France, <i>in person</i> , 01–04 September 2025
GLACY-e	Training of Trainers Programme (ToT): Advanced Judicial Course (for prosecutors from state level), Brazil, <i>in person</i> , 01–05 September 2025
GLACY-e	Training of Trainers Programme (ToT): Adult Training Methodology (for prosecutors from state level), Brazil, <i>online</i> , September 2025
CyberSPEX	Meeting with the draft working group on the implementation of the Second Additional Protocol to the Convention on Cybercrime, Finland, <i>in person</i> , 03 September 2025
Octopus Project – CYBERKOP Action	Study visit and bilateral meetings of Kosovo FIU delegation to Germany: Institutional approaches to cryptocurrency regulation, investigation, and supervision of VASPs/CASPs, <i>in person</i> , 03–04 September 2025
CyberSEE	Regional Judicial Training ToT, Albania, <i>in person</i> , 08–10 September 2025
CyberEast+	National discussions on responsible reporting and cyberviolence: civil society, ISP and academia forum, Azerbaijan, <i>in person</i> , 09–10 September 2025
Octopus Project – CYBERKOP Action	Domestic training for Investigators on Open-Source Intelligence (OSINT) and relevant tools, <i>in person</i> , 09–10 September 2025
CyberSEE	Europol AP Twins Annual Expert Meeting, The Netherlands, <i>in person</i> , 09–11 September 2025
CyberEast+	Meeting with Internet service providers, Azerbaijan, <i>in person</i> , 11 September 2025
CyberEast+	Advanced cybercrime training: OCSEA Investigations and OSINT, Armenia, <i>in person</i> , 15–17 September 2025
GLACY-e	Workshop on the handbook on judicial training strategies for ASEAN countries, Philippines, <i>in person</i> , 17–19 September 2025
CyberSEE Project & Octopus Project – CYBERKOP Action	Regional Training of Trainers (ToT) on delivery of the Specialised Judicial Training Course on Electronic Evidence, <i>in person</i> , 23–25 September 2025
CyberEast+	Regional Meeting/Showcase on use of AI in investigation and forensics, Poland, <i>in person</i> , 25–26 September 2025
C-PROC, Eurojust	CoE - Eurojust joint conference: Cooperation on the Second Additional Protocol to the Convention on Cybercrime, The Netherlands, <i>in person</i> , 29–30 September 2025

CyberSPEX	Participation in the EU e-Evidence workshop organised by EUROJUST, The Netherlands, <i>in person</i> , 30 September–01 October 2025
GLACY-e	IJTN: P2P workshop: Spontaneous information, Global, <i>online</i> , by end-September 2025
CyberSEE	Domestic meeting with Montenegrin relevant institutions dedicated on the details of the 2AP and roadmap of the legislative reform process, Montenegro, <i>in person</i> , September 2025 (TBD)
CyberSEE	High-level meeting with Serbian institutions on the necessary amendments to existing legal framework to implement 2AP provisions, Serbia, <i>in person</i> , September 2025 (TBD)
CyberSEE	Final workshop to support the development of the Cybercrime Strategy in Serbia (2025–2028), Serbia, <i>in person</i> , September 2025 (TBD)
CyberSEE	Study visit of Ministry of Security of BiH to CERT Türkiye (USOM), Türkiye, <i>in person</i> , September 2025 (TBD)
CyberSEE, INTERPOL	Regional law enforcement training and certification of trainers on cybercrime and electronic evidence, with INTERPOL (GLACY-e), Türkiye, <i>in person</i> , September 2025 (TBD)
GLACY-e	Support to the legislative reform: Awareness raising workshop for the members of the Congress, Panama, <i>in person</i> , September 2025
GLACY-e	IJTN: Adult training methodology course [French edition], Global, <i>online</i> , September 2025
GLACY-e	Awareness workshop with the legislators on Second Additional Protocol, Costa Rica, <i>in person</i> , September 2025
GLACY-e	Awareness workshop with the service providers on Second Additional Protocol, Costa Rica, <i>in person</i> , September 2025
GLACY-e	Support to the legislative reform - Awareness raising workshop for legislators, Uruguay, <i>in person</i> , September 2025
GLACY-e	Workshop on mainstreaming cybercrime and electronic evidence in the training curricula (prosecutors), Chile, <i>online</i> , September 2025
C-PROC	Organise the “Cyber-Skills Sharing Programme” 1 st Edition, global, <i>in person</i> , September–November 2025
CyberSouth+	Adaptation of the judicial training materials on cybercrime and electronic evidence and national course delivery in Egypt, <i>online & in person</i> , July–November 2025

* Palestine: This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Council of Europe and European Union member States on this issue.

** Kosovo: This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.

Inventory of capacity building projects

Octopus Project

Duration: January 2021 – December 2027

Geographical scope: Global

Budget: Up to EUR 10.000.000,00

Funding: Voluntary contributions by Canada, France Hungary, Iceland, Italy, Japan, Netherlands, United Kingdom, USA

CyberEast+

Duration: March 2024 – February 2027

Geographical scope: Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine

Budget: EUR 3.900.000,00

Funding: European Union and the Council of Europe

CyberSEE

Duration: January 2024 – June 2027

Geographical scope: South-eastern Europe and Türkiye

Budget: EUR: 5.500.000,00

Funding: Joint project of the European Union (DG NEAR) and the Council of Europe

CyberSPEX

Duration: March 2024 – February 2026

Geographical scope: European Union Member States

Budget: EUR 2.230.000,00

Funding: European Union and the Council of Europe

GLACY-e

Duration: August 2023 – January 2026

Geographical scope: Global

Budget: EUR 5.556.000,00

Funding: Joint project of the European Union (Neighbourhood, Development and International Cooperation instrument – NDICI – Global Europe) and the Council of Europe

CyberSouth+

Duration: January 2024 – December 2026

Geographical scope: Southern Neighbourhood Region

Budget: EUR 3.890.000,00

Funding: Joint project of the European Union (European Neighbourhood Instrument) and the Council of Europe

Octopus Project – CYBERKOP Action

Duration: September 2023 – March 2026

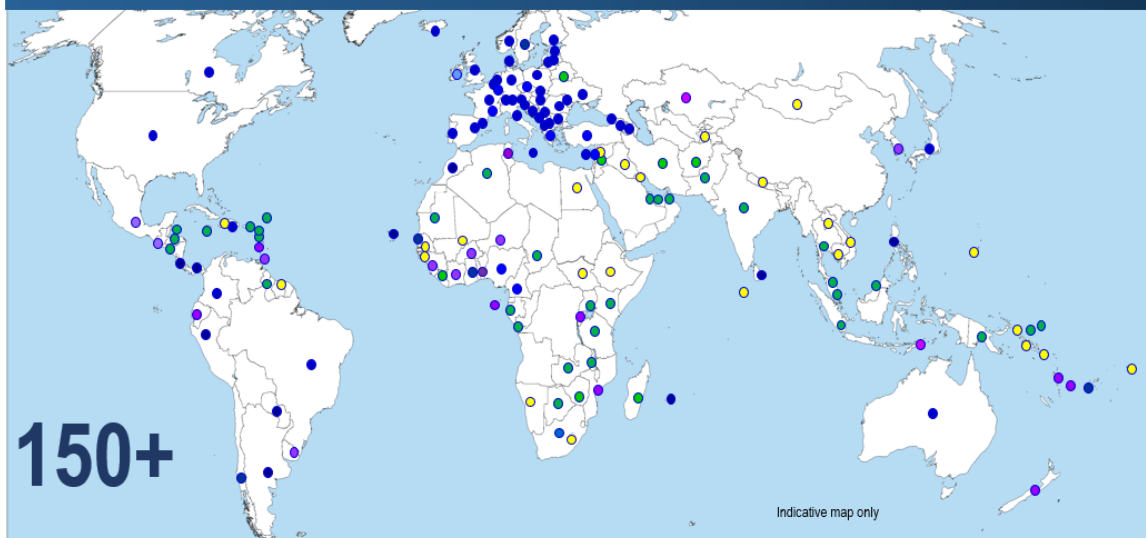
Geographical scope: Kosovo*

Budget: EUR 750.000,00

Funding: US State Department, International Narcotics and Law Enforcement Affairs

**This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo Declaration of Independence*

Reach of the Convention on Cybercrime



Parties:	80			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	40+	
Invited to accede:	15	Further States drawing on Budapest Convention for legislation:	20+	
=	97		=	60+

The Cybercrime@CoE Update does not necessarily reflect official positions of the Council of Europe, donors of capacity building projects or Parties to treaties referred to. For any additional information, contributions, subscriptions or removal from this distribution list, please contact: cybercrime@coe.int

www.coe.int/cybercrime

