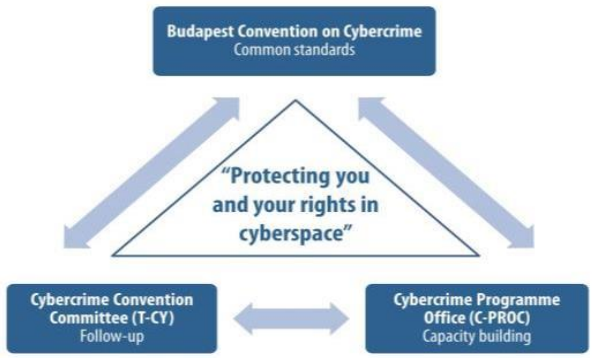
CYBERCRIME@COE UPDATE

April – June 2026

Highlights April – June 2026

- Creating, altering and distributing AI-generated child sexual abuse material is criminalised under Council of Europe conventions
- Costa Rica becomes the fourth state to ratify the Second Additional Protocol to the Convention on Cybercrime
- CyberSouth+ and GLACY-e: International conference on combating cybercrime brings together experts from 15 countries to Cairo
- CyberSEE, CyberSouth+, CyberSPEX, GLACY-e and Octopus Projects: The Cyber Games and Digital Security Challenge 2026 - The second edition takes the global fight against cybercrime to Africa
- T-CY adopts mapping study on virtual assets and endorses CyberSPEX templates for the implementation of the Second Additional Protocol
- 12 years of co-operation between Romania and the Council of Europe to strengthen capacities in the field of cybercrime
- GLACY-e supports international dialogue on cybercrime and scam centres at EU Crime Fighting Week 2026
- CyberSouth+ supported partner countries have participated with excellent results in MENA region's first large-scale cybercrime operation led by INTERPOL
- CyberEast+, CyberSouth+ and Octopus Project: Guidelines facilitating mutual legal assistance in cybercrime and electronic evidence were reinforced



Follow us

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

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.

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!

- 7-10 September 2026: Underground Economy Conference, France
- 12-13 October 2026: 35th T-CY Plenary meeting, France and online
- 14-16 October 2026: Octopus Conference, France and online

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

Convention on Cybercrime

Opened for signature: 23 November 2001

Parties as of 30 June 2026: 82

Signatories and States invited to accede as of 30 June 2026: 15

T-CY

Members as of 30 June 2026: 82 States Parties

Observer States as of 30 June 2026: 15

Observer Organisations as of 30 June 2026: 11

STRASBOURG, FRANCE, 3 June 2026

***In person* | Creating, altering and distributing AI-generated child sexual abuse material is criminalised under Council of Europe conventions**

The Council of Europe's Cybercrime Convention Committee (T-CY) and the Committee of the parties to the Convention on the protection of children against sexual exploitation and sexual abuse have issued a joint statement following a session held on 2 June 2026 in Strasbourg addressing the growing threats posed by AI-generated and altered child-sexual-exploitation and sexual-abuse material.

The joint statement underlines that the criminalisation provisions of the Convention on Cybercrime (Budapest Convention) and the Convention on the protection of children against sexual exploitation and sexual abuse (Lanzarote Convention) are technology-neutral and apply irrespective of the technologies used to create, alter or distribute such material, including through the use of artificial intelligence.

Continued cooperation among criminal-justice authorities, child-protection actors, international organisations, civil society and private-sector stakeholders is vital for addressing emerging technological developments related to online sexual offences against children. [READ MORE]

STRASBOURG, FRANCE, 4 June 2026

***In person* | T-CY adopts mapping study on virtual assets and endorses CyberSPEX templates for the implementation of the Second Additional Protocol**

The Cybercrime Convention Committee (T-CY) held its 34th Plenary meeting in Strasbourg on 3–4 June 2026, marking the Committee's 20th anniversary and welcoming Aisling Kelly as the new Head of the Cybercrime Division and Executive Secretary of the T-CY.

Among the key outcomes of the meeting, the T-CY adopted a mapping study on virtual assets and the relevance of the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol. Drawing on responses from Parties and observers representing 44 countries, the study provides an overview of how the Budapest Convention framework can be applied in the context of virtual assets and confirms its continued relevance in supporting investigations, international co-operation and access to electronic evidence. It also highlights the importance of co-operation with virtual asset service providers and other relevant stakeholders. [READ MORE]

UPDATE: Joint Project Initiatives

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

BUCHAREST, ROMANIA, 21 April 2026

***In person* | 12 years of co-operation between Romania and the Council of Europe to strengthen capacities in the field of cybercrime**

The Cybercrime Programme Office (C-PROC) of the Council of Europe, based in Bucharest, is celebrating its 12th anniversary this month. To mark the occasion, a meeting was held in Bucharest on 21 April 2026, with representatives of the diplomatic community, international organisations, and Romanian criminal justice authorities responsible for combating cybercrime. The event served as a platform for exchanging views on challenges and trends in the field of cybercrime and related issues. At the same time, the meeting provided a framework for analysing opportunities for co-operation and for encouraging collaboration with the diplomatic community, government agencies, and law enforcement to share resources, expertise, and best practices.

Among the topics discussed were capacity building in the field of cybercrime, enhanced co-operation and the disclosure of electronic evidence (Second Additional Protocol), disinformation and foreign interference in elections, and online violence – impact, accountability, and resilience in the digital age, some of the areas of interest for the work carried out by the Council of Europe's team in Bucharest.

The meeting facilitated an exchange of views on current challenges and possible solutions, outlining new avenues for co-operation between the Council of Europe (through C-PROC) and the Romanian authorities.

The Council of Europe is the largest human rights organisation on the continent. Since its founding in 1949, the organisation has created a common legal space, centered on the European Convention on Human Rights, across all 46 member states, for over 700 million people. The Convention on Cybercrime (Budapest Convention), signed in Budapest on 23 November 2001, currently has 97 states, 81 of which are Parties, 2 are signatories, and 14 have been invited to accede. [READ MORE]

BUCHAREST, ROMANIA, 27 April 2026

***In person* | C-PROC's Head of Office meets with Ambassador of Montenegro in Bucharest to discuss ongoing and prospective technical assistance on cybercrime and electronic evidence**

On 27 April, following the discussions during the Twelfth anniversary of the Cybercrime Programme Office of the Council of Europe (C-PROC) and meeting with the diplomatic community, His Excellency Mr Danilo Brajović, Ambassador of Montenegro in Bucharest, convened a meeting with the representatives of the C-PROC to discuss ongoing and prospective technical assistance on cybercrime and electronic evidence.

The C-PROC management presented its mandate, emphasizing the implementation of capacity building projects on cybercrime in accordance with the Convention on Cybercrime (Budapest Convention).

The discussions focused on supporting the Ministry of Justice of Montenegro on the implementation of the Second Additional Protocol to the Budapest Convention (2AP) and advising the law enforcement authorities on strengthening the specialised cybercrime unit, building on previous capacity building activities of the CyberSEE project for the benefit of the Montenegro Police Directorate and police training institutions.

Upcoming joint engagements were also explored, particularly co-operation with the Western Balkans Cyber Capacity Centre (WB3C) for the training on dark web investigations in April and the EU-funded projects coordination meeting in May, in Podgorica. Furthermore, activities scheduled to take place in June, in Montenegro were discussed, including the Regional exercise of the Western Balkans Working Group for Digital Asset Investigations and the Domestic expert workshop on the implementation of the 2AP. [READ MORE]

MARRAKECH, MOROCCO, 19-21 May 2026

***In person* | CyberSEE, CyberSouth+, CyberSPEX, GLACY-e and Octopus Projects: The Cyber Games and Digital Security Challenge 2026 - The second edition takes the global fight against cybercrime to Africa**

Organised in Marrakech from 19 to 21 May 2026 within the framework of the CyberSEE, CyberSouth+, CyberSPEX, GLACY-e and Octopus projects and in close partnership with INTERPOL and Morocco's General Directorate of National Security (DGSN) and General Directorate for Information Systems Security (DGSSI), the second edition of the Cyber Games and Digital Security Challenge brought together law enforcement representatives and cybersecurity specialists from 50 countries across the globe. Building on the success of the inaugural edition held in Malaysia in 2025, and reflecting Africa's growing capacity to combat cybercrime, this edition marked a historic milestone as the first time the event was hosted on the African continent.

During the opening session, Mr. Mohamed Dkhissi, Director of the Judicial Police of the General Directorate of National Security and INTERPOL Vice President for Africa, underlined Morocco's integrated strategy to combat cybercrime in line with its commitments under the Convention on Cybercrime (Budapest Convention) and its additional protocols.

From nearly 400 applicants, the 160 pre-selected top performers competed in mixed teams of police, forensics, and cybersecurity professionals, engaging in six investigative scenarios on ransomware, cryptocurrency tracing, Open-Source Intelligence (OSINT), digital forensics, asset seizure, and evidence-to-prosecution case building, using the Convention on Cybercrime and its Second Additional Protocol. The event also integrated the INTERPOL Digital Security Challenge, enabling further collaboration for a global response to cyber threats.

The Cyber Games boosted participants' skills in cybercrime investigations and digital forensics, while deepening understanding of international instruments and fostering cross-border cooperation and learning. [READ MORE]

BRUSSELS, BELGIUM, 26-27 May 2026

***In person* | Driving inclusive Digital Governance: CyberEast+ and CyberSEE foster multi-stakeholder collaboration at EuroDIG 2026 and beyond**

The 2026 session of the European Dialogue on Internet Governance (EuroDIG), supported by the European Commission and hosted by EURid on 26 and 27 May 2026 brought together 800 + participants, both online and onsite, from governments, international organisations, the private sector, civil society, and academia to address emerging internet governance challenges, ways to shape a resilient and inclusive European online space under the overarching theme of European Voices for the Future of the Internet – Celebrating 20 Years of .eu and the Beginning of a New Internet Governance Era.

Around 44 stakeholders supported by CyberSEE and CyberEast+ joint projects of the Council of Europe and of the European Union contributed by exchanging views on public policy issues related to deepfakes, generative AI, digital information ecosystems, the use of AI in public services and ways to tackle online violence and AI-driven discrimination.

The opening plenary on Democracy: Stifled or Revived by Digital Disruption of the Public Sphere? offered the opportunity for reflecting on tools designed to sustain democracy in the digital sphere, including ensuring media and social media pluralism, which is instrumental for guaranteeing fair elections and other democratic processes. One key topic that was highlighted was the current environment in which some countries are attempting to restrict online freedom and use power to bypass democratic rights. The only democratic answer is not to resist but to make digital transformation responsible, in line with democracy and the rule of law. [READ MORE]

STRASBOURG, FRANCE, April-June 2026

Online | CYBOX – platform improvements and further trainings conducted

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.

From plug-in updates, platform updates, enhanced user experience features allowing for a more robust and flexible design, the CYBOX space has been undergoing continuous transformations so as to better meet the needs of its users. Introductory trainings have been conducted, which helped attract more active users, linked through recommendations from institutions, participation in C-PROC activities or online searches. [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, Malta, Monaco, Netherlands, United Kingdom, USA

Participating countries/regions: Global

GENEVA, SWITZERLAND, 6-8 May 2026

In person | Geneva Cyber Week 2026

A three-hour interactive side event was hosted at Geneva Cyber Week 2026 with representatives from law enforcement, academia, private industry and internal CoE speakers. It showcased CoE legal frameworks and also use cases of AI in law enforcement work. The side event, organised by the Octopus Project and CyberEast+, provided a platform for global dialogue on the risks, opportunities and co-operation needs arising at the intersection of AI, cybercrime and electronic evidence. It considered how existing international legal frameworks, with a specific focus on the Convention on Cybercrime (Budapest Convention), the Second Additional Protocol and related instruments on co-operation and disclosure of electronic evidence can be applied to AI-related investigations. The discussion also took into account the wider Council of Europe framework on artificial intelligence, including the Framework Convention on Artificial Inteligence and the HUDEIRA methodology for assessing risks and impacts of AI systems on human rights, democracy and the rule of law. It further highlighted how capacity building and public-private co-operation can help states respond effectively. [READ MORE]

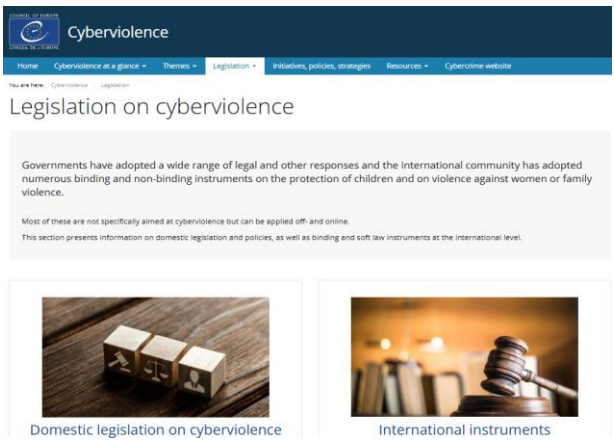
STRASBOURG, FRANCE, April-June 2026

Online | Cyberviolence Resource – domestic criminal legislation and policies made accessible

Initiated following the recommendations stemming from the T-CY Mapping Study on Cyberviolence (2018), the Cyberviolence Resource is one of the online tools led through the Octopus Project of the Council of Europe's Cybercrime Division, bringing together the work of colleagues from across sectors within the Organisation for the benefit of citizens and criminal justice authorities worldwide. Further to the 32nd T-CY Plenary, a questionnaire to collect information on domestic criminal legislation and policies in relation to cyberviolence was adopted, with a view to assisting current and future Parties to the Convention on Cybercrime intending to address offences related to cyberviolence in their domestic law, as well as updating the Council of Europe's online Cyberviolence Resource. The T-CY Secretariat and internal Working Group on cyberviolence has been analysing the information received so far and made a first part of it already accessible on the Cyberviolence Resource online platform.

Under the 'Legislation on cyberviolence' section, the 'Domestic legislation' component now features information from more than 44 countries on online xenophobia and racism, cyberviolence against children, cyberviolence against women, cyberviolence against journalists, online trafficking in human being and other forms of cyberviolence.

As next steps, the 'Case law' section section on the Cyberviolence Resource will be updated with information at domestic level as received through the questionnaire and further analytical will be made available. Additional contributions from Parties and Observers remain welcome. [READ MORE]



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

GLACY-e basics

Duration: 1 August 2023 – 15 December 2028

Budget: EUR 13,334,000

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

STRASBOURG, FRANCE, 15 April 2026

In person | Costa Rica becomes the fourth state to ratify the Second Additional Protocol to the Convention on Cybercrime

On 15 April 2026, Costa Rica ratified the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Costa Rica becomes the fourth country to ratify the Protocol, bringing it closer to its entry into force.

Opened for signature on 12 May 2022 in Strasbourg, the Second Additional Protocol, introduces innovative mechanisms. These include direct co-operation with service providers in other jurisdictions to access subscriber information, rapid collaboration in emergency situations, as well as the establishment of joint investigation teams and video conferencing paired with strong human rights and rule of law safeguards.

The Council of Europe, through its Cybercrime Programme Office (C-PROC) and the GLACY-e Project, continues to support countries in the process of implementation and ratification of the Second Additional Protocol through dedicated capacity building activities. [READ MORE]

LIMA, PERU, 21-24 April 2026

In person | GLACY-e: Peruvian judges and prosecutors trained on gender dimensions of cybercrime

Organized within the framework of the GLACY-e joint project of the European Union and the Council of Europe, the workshop was co-organized with the Peruvian Judiciary, notably the Superior Court of Justice of Lima, as host institution, and the Public Prosecutor's Office. The initiative contributed to enhancing participants' capacity to investigate, prosecute and adjudicate cybercrime cases while integrating gender-sensitive approaches throughout judicial processes. It also further consolidated the network of national trainers in gender and cybercrime, who are later expected to pass on their expertise to other justice professionals in Peru and replicate this learning experience.

Building on a similar training held in Arequipa in January this year, the course combined legal and practical components, addressing key issues such as the gendered nature of cybercrime, the impact on victims – particularly women and girls – and the challenges associated with reporting, evidence collection and prosecution. The course was jointly facilitated by an international expert of the Council of Europe alongside five national trainers previously trained under similar GLACY-e project. Particular attention was given to identifying forms of online violence that disproportionately affect women, as well as to preventing secondary victimization and strengthening access to justice. [READ MORE]

ONLINE, April – May 2026

In person | GLACY-e: Federal judges in Brazil completed the course on adult training methodologies

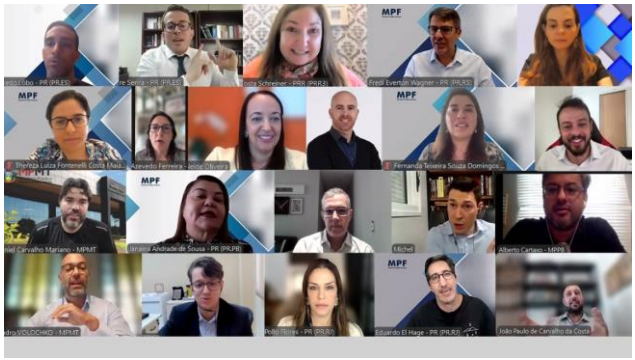
25 federal judges from Brazil enhanced their training knowledge through a successful completion of a two-day online "Training of Trainers: Adult Training Methodologies" course, organised under the GLACY-e project, an initiative of the European Union and the Council of Europe.

The course was designed to build judges' practical skills and competencies in adult education, with an emphasis on interactive learning and training delivery, fully aligned with the principles of adult education. [READ MORE]

ONLINE, 7–8 May 2026

In person | Brazil advances cybercrime justice with new training-of-trainers program

Brazil has taken a major step in its fight against cybercrime with the launch of a state-level judicial training-of-trainers program under the GLACY-e project, co-funded by the Council of Europe and the European Union. After completing the introductory judicial course on the CYBOX platform in May 2025, followed by the advanced course held in São Paulo from 29 September to 3 October 2025, some 25 state prosecutors were equipped with advanced knowledge in cybercrime, electronic evidence and international co-operation mechanisms.



This initiative shows the progress made by Brazil since its accession to the Budapest Convention and the successful initial training of federal prosecutors in 2024. State prosecutors completing the training programme, and subsequently conducting a training session themselves, will be certified as Council of Europe trainers. [READ MORE

Madrid, SPAIN, 21-22 May 2026

In person | GLACY-e and CyberSPEX: Strengthening trans-regional co-operation in the fight against cybercrime: regional roundtable advances implementation of the Second Additional Protocol

The GLACY-e and CyberSPEX joint projects of the European Union and the Council of Europe supported Argentina, Brazil, Cabo Verde, Chile, Colombia, Dominican Republic, Panama, Paraguay, Peru, Ecuador, Costa Rica, Portugal and Spain to advance in the implementation of the Second Additional Protocol (2AP) to the Convention on Cybercrime (Budapest Convention) through a two-day roundtable. The event was held in Madrid on 21-22 May 2026, and was hosted by the Ministry of the Presidency, Justice and Relations with the Parliament of Spain.

As cybercrime continues to evolve, accessing electronic evidence across multiple jurisdictions remains one of the most pressing challenges for criminal justice systems worldwide. The Second Additional Protocol aims to boost international co-operation and facilitate more efficient cross-border collaboration, while upholding human rights and the protection of personal data.

Participants, comprising focal points of the Ibero-American Network of Cybercrime Prosecutors (CiberRed), 24/7 points of contact (POCs), representatives from various national institutions and legislative experts, shared experiences and best practices regarding the Protocol's implementation and application. Discussions explored real-world case studies on cross-border co-operation with service providers and emergency response scenarios, enriching the collective knowledge base and fostering a culture of collaborative justice.

The Cybercrime Programme Office of the Council of Europe (C-PROC) remains committed to fostering co-operation, building capacities and supporting effective implementation of the Convention and its Protocols to make cyberspace safer and uphold the rule of law across continents. [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

CHISINAU, MOLDOVA, 7-9 April 2026

***In person* | CyberEast+, CyberSEE, CyberSouth+, GLACY-e: Enhancing knowledge of cybercrime experts through a regional cybercrime co-operation exercise**

From 7 to 9 April 2026, the Cybercrime Programme Office of the Council of Europe (C-PROC), through CyberEast+, Cyber SEE, CyberSouth+ and GLACY-e, joint projects of the European Union and of the Council of Europe, supported a regional technical co-operation exercise themed with incident handling and investigation of current cyberthreats. This event was organised under the Presidency of the Republic of Moldova of the Council of Europe Committee of Ministers, in partnership with the Estonian E-Governance Academy (eGA) and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ).

The three-day exercise, designed to enhance digital security across regions, brought together over 60 representatives of law enforcement, specialised prosecutors and cybersecurity experts responsible for the protection of critical information infrastructure from 20 countries. Key highlights included tackling infostealer infrastructure, handling ransomware and ultimately dismantling a criminal organisation that was disseminating child abuse material.

The Council of Europe, through its Cybercrime Programme Office, is committed to fostering a culture of information sharing and to improving digital forensics skills across borders, by developing cybercrime technical exercises requiring coordinated responses and interagency co-operation. [READ MORE]

UKRAINE, 15-17 April 2026

***In person* | CyberEast+, CyberUA: Ukrainian investigators increased their expertise on the use of Artificial Intelligence (AI)**

The Cybercrime Programme Office of the Council of Europe (C-PROC), through CyberEast+, a joint project of the European Union and of the Council of Europe and the CyberUA project, funded by voluntary contributions under the Action Plan of the Council of Europe, organised a three-day specialised training for practitioners from Ukrainian investigative and prosecutorial agencies on the use of Artificial Intelligence (AI) for Open Source Intelligence (OSINT), the investigation and forensics on war crimes and related offences. This exercise built on the achievements of the regional meeting on AI supported under CyberEast+ in 2025, which examined various AI tools used to facilitate cybercrime investigations and digital forensics.

The training was built around the Council of Europe Framework Convention on Artificial Intelligence and the Convention on Cybercrime (Budapest Convention), which are practical instruments that can be used not only for the prosecution and adjudication of cybercrime offences, but also to ensure that human rights, democracy and the rule of law are upheld in the process. The exercise was conducted via the CYBOX online platform developed under the Octopus Project. The event brought together 34 Ukrainian cybercrime investigators, detectives, forensic experts and prosecutors, specialising in the use of OSINT and of AI tools to facilitate investigations of war crimes and other related offences. [READ MORE]

YEREVAN, ARMENIA, 22 -23 April 2026

***In person* | CyberEast+, CyberSouth+ and Octopus Project: Guidelines facilitating mutual legal assistance in cybercrime and electronic evidence were reinforced**

Addressing well-known problems of efficiency and expedience of international co-operation on cybercrime and electronic evidence, Mutual Legal Assistance Guidelines were agreed by Eastern Partnership states back in 2021, under the joint CyberEast regional initiative of the European Union and the Council of Europe.

5 years later, international co-operation, judicial and law enforcement representatives from 10 countries were gathered in Yerevan, Armenia on 22 and 23 April 2026 to review and update these Guidelines in line with recent standards and improved practices. Two joint regional projects of the European Union and of the Council of Europe, CyberEast+ and CyberSouth+, in partnership with the Council of Europe Octopus Project, based on voluntary contributions, organised these cross-regional discussions.

Representatives from Armenia, Egypt, Jordan, Kazakhstan, Libya, Republic of Moldova, Morocco, Palestine, Tunisia, and Ukraine gathered to discuss and update on themes of legal basis and regulations for co-operation, as well as efficient management of the cooperation process and quality of outgoing requests, as part of these Guidelines.

The meeting produced updated 2026 MLA Guidelines, which will be further refined and circulated to all participants for comments and suggestions. The revised Guidelines will form a basis for dedicated training session and tabletop exercise, planned to be conducted at the end of October 2026.

These practice-oriented Guidelines, aligned with requirements of the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol, aim to walk the states through on both legal and practical methods to improve the speed and quality of mutual legal assistance. [READ MORE]

UKRAINE, 16-18 June 2026

***In person* | CyberEast+ and CyberUA: Ukrainian authorities and private sector actors enhanced their co-operation through joining a cybercrime exercise**

The ongoing aggression of the Russian Federation against Ukraine, reflected in increasing cyberattacks, including against critical infrastructure, remains one of the key challenges in the Eastern Partnership region.

In order to respond to this type of hybrid cyber war, and to improve the knowledge and practical skills of law enforcement officers, prosecutors, the cybersecurity community and private sector experts of Ukraine, CyberEast+, a joint project of the European Union and of the Council of Europe, in collaboration with the CyberUA project of the Council of Europe, organised the third cybercrime co-operation exercise with private sector entities, from 16 to 18 June 2026.

Thirty-six participants from the Prosecutor General's Office, the National Security and Defence Council, the State Bureau of Investigations, the State Service of Special Communications and Information Protection, the State Security Service, the National Health Service and various service providers/infrastructure entities from Ukraine actively engaged in the exercise.

Using professional skills and practical knowledge, the Ukrainian counterparts identified simulated cyber security incidents and responded with cybercrime investigations that followed necessary procedures to secure electronic evidence on the basis of standards of the Convention on Cybercrime (Budapest Convention). This exercise provided an opportunity to use an array of Open-Source Intelligence (OSINT) tools and to conduct digital forensics for the identification of potential perpetrators of the attack. [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.*

ONLINE, February - May 2026

Online | CyberSouth+ delivers dedicated training modules on cybercrime and digital investigations for public prosecutors in Palestine*

Building on previous training activities, the Palestinian Public Prosecution, in partnership with Birzeit University, have developed a national Diploma in Cybercrime and Digital Investigations. This initiative reflects a growing institutional commitment to embedding cybercrime expertise within the Palestinian criminal justice system. The CyberSouth+ joint project of the European Union and the Council of Europe is contributing to this nationally-owned effort through a series of weekly online modules delivered by international experts. [READ MORE]

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

CHISINAU, MOLDOVA, 7-9 April 2026

In person | Enhancing knowledge of cybercrime experts through a regional cybercrime co-operation exercise

The Cybercrime Programme Office of the Council of Europe, supported the organization of a three-day exercise designed to enhance digital security across regions. This event brought together over 60 representatives of law enforcement, prosecutors and cybersecurity experts responsible for the protection of critical information infrastructure from 20 countries. Key highlights included tackling infostealer infrastructure, handling ransomware and ultimately dismantling a criminal organization that was disseminating child abuse material. [READ MORE]

PRISTINA, KOSOVO*, 14-16 April 2026

In person | Strengthening regional co-operation and operational capacities to combat online child sexual exploitation and abuse

The CyberSouth+ joint project of the European Union and the Council of Europe supported the participation of its partner countries in the regional training on investigating OCSEA. This event brought together law enforcement authorities to share practical approaches in the handling of reports as developed by the National Center for Missing and Exploited Children. It also covered the use of open-source intelligence (OSINT) tools, analysing child sexual abuse material (CSAM) and identifying victims, conducting child-sensitive interviews, collecting electronic evidence, and addressing challenges related to financial flows in OCSEA cases. [READ MORE]

* *All references to Kosovo, whether to the territory, institutions, or population, in this text shall be understood in full compliance with United Nations' Security Council Resolution 1244 and without prejudice to the status of Kosovo.*

YEREVAN, ARMENIA, 22 -23 April 2026

In person | Guidelines facilitating mutual legal assistance in cybercrime and electronic evidence were reinforced

Representatives from a number of countries gathered to discuss and update the legal basis, regulations and efficient management of co-operation efforts. The resulting revised guidelines will stand as basis for dedicated training sessions and a tabletop exercise expected to be conducted at the end of October 2026. These practice-oriented guidelines, aligned to the Budapest Convention on Cybercrime and its Second Additional Protocol, aim to improve mutual legal assistance. [READ MORE]

MENA Region, 18 May 2026

***In person* | CyberSouth+ supported partner countries have participated with excellent results in MENA region's first large-scale cybercrime operation led by INTERPOL**

Operation Ramz, the first cybercrime operation of its scale coordinated by INTERPOL in the MENA region, concluded with over 200 arrests and more than 3800 victims identified across the 13 participating countries. Running from October 2025 to February 2026, the operation targeted phishing infrastructure, malware networks, and cyber-enabled fraud schemes, resulting in server seizures and the dissemination of nearly 8000 pieces of intelligence among national authorities.

The operation has received support from the Qatar Ministry of Interior and the CyberSouth+ project, a joint initiative of the European Union and the Council of Europe. The project has facilitated the participation of representatives from all its partner countries in INTERPOL's 15th MENA working group meeting on cybercrime for Heads of Units, where the joint operation was launched.

Operational highlights from CyberSouth+ partner countries include the dismantling of a «phishing-as-a-service» website in Algeria, the arrest of three individuals in Morocco following the seizure of phishing software and banking data, and investigative actions in Jordan that have uncovered a financial fraud scheme linked to a human trafficking network.

Operation Ramz is a concrete illustration of how CyberSouth+'s sustained capacity building activities contribute to equipping the national authorities with the skills, tools, and regional relationships needed to engage in complex cross-border investigations and ultimately achieve operational outcomes for enhanced criminal justice in cyberspace. [READ MORE]

CAIRO, EGYPT, 14-15 June 2026

***In person* | International conference on combating cybercrime brings together experts from 15 countries to Cairo**

The Ministry of Justice of the Arab Republic of Egypt, in partnership with the Faculty of Law of the British University in Egypt, the United Nations Office on Drugs and Crime, and the Cybercrime Programme Office of the Council of Europe, organised the international conference on "Combating cybercrime: evolving threats, electronic evidence, and the imperative of international co-operation". The conference brought together more than 100 participants for expert discussions on the evolving landscape of cybercrime and international co-operation. At the heart of the conference was the recently adopted UN Convention against Cybercrime (the Hanoi Convention), examined alongside the Council of Europe Convention on Cybercrime (the Budapest Convention). [READ MORE]

CAIRO, EGYPT, 16 June 2026

***In person* | CyberSouth+ Fourth Steering Committee**

The CyberSouth+ joint initiative of the European Union and the Council of Europe convened its fourth Steering Committee meeting to take stock of progress achieved and agree on activities for the next six months. Among the results highlighted for the first half of 2026 were: enhanced skills and knowledge in the area of OCSEA, progress in addressing technology-facilitated gender-based violence, and the delivery of regional and international practical training activities. [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.*

PODGORICA, MONTENEGRO, 27-30 April 2026

***In person* | CyberSEE: Strengthening Dark Web and Open-Source Intelligence (OSINT) investigative capacities across the Western Balkans**

Between 27 and 30 April 2026, the CyberSEE joint project of the European Union and the Council of Europe supported the Albanian State Police in organising their first activity as co-leaders of the Operational Action 6.2 under EMPACT policy cycle, in co-operation with the Western Balkans Cyber Capacity Centre (WB3C). The workshop on Dark Web Investigation in Podgorica, Montenegro brought together law enforcement representatives of Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, and Serbia,

Over four days, participants engaged in hands-on exercises, covering Operations Security (OPSEC), Open-Source Intelligence (OSINT) fundamentals, social media investigations, judicial reporting, dark web architecture, passive infiltration techniques, marketplace analysis, and cryptocurrency tracking basics, culminating in a cross-border tabletop case simulation.

This joint effort also enabled participants to strengthen regional co-operation, share field experiences, and reinforce professional trust for coordinated actions. The initiative fosters investigators' ability to translate digital traces and operational mistakes into actionable intelligence. Cryptocurrency investigations, ransomware-related cybercrime, and the utilisation of artificial intelligence were identified as priority areas for future training. [READ MORE]

NOVI SAD, NIŠ, ZLATIBOR, SERBIA, May 2026

***In person* | CyberSEE supports implementation of "Cyber Guard", Serbia's national platform for reporting high-tech crime**

The CyberSEE joint project of the European Union and the Council of Europe supported the implementation of the "Cyber Guard", the newly established national platform for reporting high-tech crime, through three dedicated workshops.. Held in Novi Sad (7 May), Niš (13 May), and Zlatibor (20 May 2026), the workshops marked a significant step in rolling out the platform at national level and strengthening the country's criminal justice response to cybercrime.

The workshops brought together delegates from 27 local police directorates across Serbia, primarily officers from criminal investigation units specialising in economic and financial crime and investigations related to crimes against children, those most likely to receive and process cybercrime reports at the local level.

The platform was presented as a centralised national mechanism for receiving, processing, and analysing cybercrime reports submitted by both citizens and legal entities. A defining feature is its citizen-oriented approach: for the first time in Serbia, citizens can report various forms of high-tech crime quickly and securely through a single national entry point, without the need to visit a police station. Built on European best practices and adapted to national requirements, the platform also supports structured information exchange between local police units and the central Service for Combating High-Tech Crime, coordination with prosecution authorities, case triage, and electronic evidence management. [READ MORE]

BRUSSELS, BELGIUM, 28 May 2026

***In person* | CyberSEE's 5th Steering Committee advances regional co-operation**

On 28 May, the 5th Steering Committee Meeting of the CyberSEE project brought together around 37 representatives from the European Commission, DG ENEST, EU Delegations, EU4LEA, Council of Europe, and project teams from South-East Europe and Türkiye, joining online and onsite, to review achievements from January to June 2026, including progress on legal frameworks, capacity building for criminal justice authorities, and enhanced co-operation with cybersecurity institutions. The meeting also addressed regional trends, legislative updates, and co-operation initiatives such as the Western Balkans Digital Asset Investigations Working Group and EMPACT. The Steering Committee endorsed the future workplan, confirmed the ongoing stakeholder engagement, and identified priorities for further project support. [READ MORE]

PRAGUE, CZECHIA, 2-4 June 2026

***In person* | CyberSEE supports strengthening of the cybercrime investigation capacities in the region**

The CyberSEE joint project of the European Union and the Council of Europe supported the enhancement of criminal justice capacities to fight against cybercrime through the participation of 16 law enforcement, intelligence and financial crime investigators from the countries in the South-East Europe and Türkiye in the ISS World Europe 2026, which took place in Prague, Czechia, from 2 to 4 June 2026.

The forum delivered technical training across eight thematic tracks, enabling the delegates from the criminal justice authorities to update their knowledge on emerging crimes over telecommunications networks and social media. The participants attended seminars and training sessions addressing online and internet investigations, lawful interception of 2G/3G/4G/5G and 6G networks, generative and agentic AI use cases for law enforcement and intelligence agencies, and the use of metadata, Exchangeable Image Format (EXIF) data and push tokens in criminal investigations. Further tracks focused on social network monitoring and AI-driven analytics, threat intelligence gathering and cyber security, investigating blockchain transactions, mobile signal interception, electronic surveillance, tracking and forensics. [READ MORE]

THE HAGUE, THE NETHERLANDS, 9-11 June 2026

***In person* | CyberSEE reinforces regional capacities to combat online child sexual exploitation at AP Twins annual expert meeting 2026**

The CyberSEE joint project of the European Union and the Council of Europe supported the reinforcement of capacities to fight against online child sexual abuse, through the participation of 13 investigators and team leaders from South-East Europe and Türkiye in the AP Twins annual expert meeting 2026, held at Europol's Headquarters in The Hague, Netherlands, from 9 to 11 June 2026.

Organised by the AP Twins team within the European Cybercrime Centre (EC3) at Europol, the meeting brought together law enforcement investigators, prosecutors, investigative judges, and partners from across Europe and beyond, united by a shared commitment to combating child sexual exploitation and abuse (CSEA), both online and offline. Over two and a half days, participants shared tactics, methods, and trends in investigating CSEA, including recent developments in investigative techniques and cross-border co-operation, and the use of virtual currencies and gaming platforms in the exploitation of children. In-depth case studies, including Operation Alice, provided practical insights into complex investigations. Dedicated sessions also explored Europol's analytical capabilities, victim identification processes, officer well-being, the legal evolution and its impact on judicial procedures. [READ MORE]

DÜRRES, ALBANIA, 9-11 June 2026

***In person* | From evidence acquisition to analysis: CyberSEE workshop strengthens regional digital forensics capacities**

Between 9 and 11 June 2026, the CyberSEE joint project of the European Union and the Council of Europe organised the Regional workshop on basic digital forensics – from evidence acquisition to analysis and reporting, in Dürres, Albania. The event brought together 24 practitioners from law enforcement and forensic departments across South-East Europe and Türkiye, offering a platform to exchange good practices and enhance operational skills through hands-on exercises and open discussions, with a joint focus on understanding and applying forensic methodologies for secure laboratory management, legal identification, collection, and preservation of digital evidence, as well as the practical analysis of digital artefacts and forensic imaging.

On the first day, the activity covered the fundamentals of digital forensics – lab infrastructure, evidence identification and acquisition, forensic imaging, hashing, and chain of custody – through hands-on exercises using open-source tools. Attendees practised media sanitisation, encrypted disk detection, live RAM acquisition, and artefact examination, and received introductory sessions on mobile, Linux, and network forensics, including browser history, email headers, and wireless forensics.

The second day delved into anti-forensics methods, with practical exercises on steganography, metadata manipulation, anonymity techniques, and data recovery. A session on reporting good practices followed, and participants applied their accumulated knowledge in a scenario-based investigation, receiving feedback and working collaboratively. Operational challenges and cases from participants' investigative experience were highlighted, discussed, and analysed collectively.

The final day concluded the investigation scenarios and open discussions based on the cases and challenges presented by the participants, allowing them to reflect on lessons learned and consider how to integrate new skills into their daily work. [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 – 31 December 2026

Budget: EUR 2.23 million

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

Participating countries: European Union Member States

BUCHAREST, ROMANIA, 21 April 2026

***In person* | CyberSPEX: Roundtable for 2AP draft working group and national authorities**

The roundtable on the implementation of the Second Additional Protocol (2AP) to the Budapest Convention, organized by the CyberSPEX project in Romania, brought together 28 representatives from key Romanian institutions to discuss the international co-operation procedures established under Articles 6–10 of the Protocol. Experts from the Cybercrime Division, C-PROC and the CyberSPEX project of the Council of Europe highlighted the Protocol's complex nature and emphasized the essential role of competent authorities and service providers in facilitating effective cross-border co-operation.

Discussions focused on practical and legal challenges related to obtaining subscriber information, co-operating with service providers and adapting to changes in the policy framework governing voluntary data disclosure. Participants stressed the need for stronger legal mechanisms to ensure clearer and more reliable procedures for accessing and sharing data.

Particular attention was given to the implementation of Articles 6–10, covering formal orders for subscriber information, cross-border co-operation, expedited enforcement procedures and emergency mechanisms through the 24/7 Network. [READ MORE]

BRUSSELS, BELGIUM, 13 May 2026

In person | CyberSPEX: EU CyberNet Stakeholder Community Day: "Advancing Europe's Cybersecurity Partnership: Made in Europe, Delivered Globally"

The meeting aimed at reflecting on how EU cybersecurity capacity building (CCB) missions can serve as a vehicle for European technology promotion, embedding EU regulatory frameworks and standards into critical infrastructure and learn from peer approaches developed by other actors. The Cybercrime Programme Office (C-PROC) of the Council of Europe with the support of the CyberSPEX project actively contributed to the meeting by showcasing good practices and positive examples in the implementation of cybercrime and electronic evidence capacity-building activities worldwide. The legal standards provided by the Budapest Convention on Cybercrime.and its Second Additional Protocol (2AP) on enhanced co-operation are considered international norms, whose implementation should be promoted and supported across countries. The importance of coordination, complementarity, and strong engagement with professional communities was highlighted as key to achieving tangible results. Supporting partner countries in developing strategic plans to strengthen criminal justice capacities is crucial for effectively fighting against cybercrime and contributing to global efforts in this field. The promotion of international standards and EU values in cyberspace was emphasised.

ONLINE, February - May 2026

***Online* | CyberSPEX Launches Advisory Meetings to Support EU Member States in Implementing the Second Additional Protocol to the Budapest Convention**

The CyberSPEX project is supporting EU Member States in implementing the Second Additional Protocol (2AP) to the Budapest Convention on Cybercrime, which is a multifaceted process requiring the harmonisation of various legislative instruments, including the EU e-Evidence Regulation, criminal procedural law, data protection law, and telecommunications law, while fully respecting safeguards and human rights.

In response to strong demand for deeper exchanges of experience among national authorities, CyberSPEX was organising a series of online advisory meetings running from February to May 2026. These regular meetings facilitated knowledge-sharing, identified legislative gaps, and promoted good practices in implementing the 2AP into domestic law. Topics covered the selection of competent authorities, the implemenation of Article 7 and Article 9 of the Second Protocol as well as a presentation of the Hungarian law implementing the Protocol.The meetings were open to representatives from all EU Member States, including legislative drafters, advisors, law enforcement, prosecutors, judges, and representatives from Ministries of Justice.

BUCHAREST, ROMANIA, 26 May 2026

***In person* | CyberSPEX: PoC Meeting of EU m/s on emergency procedures under the 2AP**

The workshop brought together 24/7 Network contact points, MLA authorities, and practitioners from EU Member States to examine practical, operational, and legislative challenges in implementing emergency co-operation under Articles 9 and 10 of the Second Additional Protocol (2AP) . Outcomes included the identification of key legal and procedural gaps, clarified national requirements for handling expedited requests, and promoted the exchange of good practices to enhance the effectiveness of cross-border cooperation through the 24/7 Network. [READ MORE]

STRASBOURG, FRANCE, 1 June 2026

***In person*| CyberSPEX: 4th Steering Committee Meeting**

The meeting aimed to update EU Member States on the latest developments of the CyberSPEX project, exchange experiences on the implementation and ratification of the Second Additional Protocol (2AP) to the Budapest Convention on Cybercrime, identify remaining support needs, and agree on the project workplan for June–December 2026. Discussions reviewed progress across the project's three main objectives: legislative alignment with the 2AP, progress towards ratification, and the capacity building of criminal justice practitioners. Finally, participants endorsed the programme of future activities, including targeted legislative support workshops, specialised training initiatives and the development of sustainable training materials to facilitate the effective implementation of the 2AP once it enters into force. [READ MORE]

MADRID, SPAIN, 21 May 2026

***In person* | CyberSPEX: Meeting with Spanish authorities on the implementation of the Second Additional Protocol**

The meeting, organised under the CyberSPEX project, brought together 20 Spanish stakeholders from the Ministry of Presidency, Justice and Relations with the Parliament, the General Prosecutor's Office, the judiciary and other relevant ministries to discuss the implementation of the Second Additional Protocol (2AP) to the Budapest Convention on Cybercrime.

Participants examined legislative and operational challenges related to aligning domestic legislation with both the Second Additional Protocol and the EU e-Evidence Package. Discussions focused on direct co-operation with service providers, access to subscriber information, and the practical adjustments required to implement new procedures. Key issues identified included the roles of competent authorities and operational preparedness.

The roundtable strengthened inter-institutional dialogue, identified priorities for legislative reform and reaffirmed the need for continued co-operation, capacity-building and technical support to ensure the effective implementation of the Protocol. [READ MORE]

STRASBOURG, FRANCE, 2 June 2026

***In person* | CyberSPEX: Third Consultation with civil society stakeholders, service providers and the industry (with T-CY)**

Following meetings held in December 2024 and November 2025, the Secretariat of the Cybercrime Convention Committee (T-CY), with the support of the CyberSPEX project, organised on 2 June 2026 the third consultation with civil society stakeholders and service providers on the implementation of the Second Protocol to the Convention on Cybercrime.

The consultation focused on civil society perspectives on conducting effective and efficient criminal investigations and proceedings in an international context, including the application of conditions and safeguards to ensure respect for human rights, the rule of law and data protection. More broadly, the event aimed at providing a venue for exchanging views and enhancing knowledge about the Second Additional Protocol and its impact on national legal frameworks and international co-operation in criminal investigations and proceedings.

Held in hybrid format at the Council of Europe's Palais de l'Europe in Strasbourg, the event brought together over 200 representatives of civil society, internet service providers, registries and other industry stakeholders, as well as members and observers of the T-CY, other representatives of Parties to the Convention on Cybercrime, the European Commission and relevant EU agencies and mechanisms including EUROPOL, EUROJUST and SIRIUS project.

Discussions highlighted the importance of necessity and proportionality, judicial oversight, transparency and effective remedies in cross-border judicial co-operation. Participants also considered the victim's rights perspective, including the need for trauma-informed and child-sensitive approaches in conducting international investigations and prosecutions, strict confidentiality of digital evidence and safeguards against secondary victimisation.

It was concluded that international and direct co-operation require equivalent levels of data protection safeguards and respect for human rights, in order to ensure that the flow of data necessary in criminal investigations and proceedings is both efficient and based on trust. [READ MORE]

BUDAPEST HUNGARY, 23 June 2026

***In person* | CyberSPEX: Dedicated one-day session during the CEPOL-EJTN "Cross border exchange of electronic evidence" - week**

CyberSPEX contributed to the CEPOL-EJTN "Cross border exchange of electronic evidence" – training, which is aimed to equip prosecutors and law enforcement officials with the knowledge and skills needed to effectively use and exchange electronic evidence in cross-border investigations and for the prosecution of cybercrime. Around 38 experts from 16 EU Member States - including Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, Greece, Hungary, Italy, Lithuania, Poland, Portugal, Romania, Spain, and Sweden - deepened their understanding of the Budapest Convention on Cybercrime., its 24/7 Point of Contact Network, and the provisions of the Second Additional Protocol (2AP). Discussions covered the operational challenges of cooperating with service providers, legal solutions offered by the Second Protocol, and the implications of necessary legislative changes for practitioners. Experts from the Romanian and Belgian Police contributed by presenting practical case studies, focusing on online fraud, international cooperation, and emergency procedures in cybercrime matters.

Inventory of activities (April – June 2026)

April 2026

CyberSEE, GLACY-e, CyberSouth+	Cyber-Skills Sharing Programme, 1st Edition, global, *in person,* January–June 2026
CyberSEE, CyberSouth+, GLACY-e	Regional Cybercrime Cooperation Exercise / Training with license handover, with CyberEast+, Chisinau, Republic of Moldova, *in person*, 6-10 April 2026
CyberSEE	Support participation in "Victim identification task force 18" with EUROPOL, The Hague, The Netherlands, *in person*, 13-24 April 2026
CyberSEE, Octopus Project, CyberSouth+, Octopus Project – CYBERKOP Action	Regional Training on investigating OCSEA starting from NCMEC reports, with CYBERKOP, Pristina, Kosovo*, *in person*, 14-15 April 2026
CyberEast+	Training on use of AI tools for OSINT, investigation and forensics on war crimes and related offences – with CyberUA project, Ukraine, *in person*, 15-17 April 2026
CyberSEE, Octopus Project, CyberSouth+, Octopus Project – CYBERKOP Action	Regional meeting with service providers on information sharing in cases of OCSEA, with CYBERKOP, Pristina, Kosovo*, *in person*, 16 April 2026
GLACY-e	Support on national legal reform - review of the final draft at the request of the Special Commission on National Security of the Congress, Guatemala, *desk study*, by 20 April 2026
CyberSPEX	Roundtable for 2AP draft working group and national authorities, Bucharest, Romania*, in person,* 21 April 2026
C-PROC, T-CY	12 years' anniversary of the Cybercrime Programme Office (C-PROC) of the Council of Europe, Bucharest, Romania, *hybrid*, 21 April 2026
GLACY-e	Gendered aspects of cybercrime - course, Lima, Peru, *in person*, 21-24 April 2026
CyberEast+, CyberSouth+, Octopus Project	Regional Conference on practical use of Second Protocol and development of Cross-Border Cooperation Guidelines, Yerevan, Armenia, *in person,* 22-23 April 2026
C-PROC	Meeting of C-PROC's Head of Office with Ambassador of Montenegro, Bucharest, Romania, *in person*, 27 April 2026
CyberSEE	Workshop on Dark Web Investigation, under EMPACT OA 6.2, with Albanian Police and WB3C, Podgorica, Montenegro, *in person*, 27-30 April 2026
GLACY-e	Train the trainers - Adult training methodology (federal judges), Brazil, *online*, April-May 2026
Octopus Project	Advisory mission on legislation for Trinidad and Tobago, *online*, April-June 2026
Octopus Project	Further development of the Cyberviolence Resource through analysis of responses received via the T-CY questionnaire, with focus on domestic legislation

Octopus Project	Further development of the CYBOX platform
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026
CyberSPEX	Advisory Meetings to Support EU Member States in Implementing the Second Additional Protocol to the Budapest Convention, online February – Mai 2026

May 2026

CyberSEE, GLACY-e, CyberSouth+	Cyber-Skills Sharing Programme, 1st Edition, global, *in person,* January–June 2026
CyberSEE	Coordination meeting of the EU funded projects on cybercrime and cybersecurity in the Western Balkans, Podgorica, Montenegro, *in person,* 4-5 May 2026
CyberEast+	HELP course on cybercrime/e-evidence for defence attorneys, Ukraine, *in person,* 4-6 May 2026
CyberSEE	Domestic training on cybercrime for first responders in Kosovo, with CYBERKOP (1 of 5 editions), Kosovo*, *in person,* 5-6 May 2026
CyberSEE	Support the workshops in Serbia for implementation of national platform for reporting high-tech crime, Novi Sad, Serbia, *in person,* 7 May 2026
CyberEast+, Octopus Project	Geneva Cyber Week - AI and Cybercrime Workshop, Geneva, Switzerland, *in person,* 8 May 2026
GLACY-e	INTERPOL Instructor Development Course (IDC) for Pacific and GLACY Course Designing Workshop, Tonga, *in person*, 11-19 May 2026
CyberSEE	Support the workshops in Serbia for implementation of national platform for reporting high-tech crime, Nis, Serbia, *in person,* 13 May 2026
CyberSPEX	EU CyberNet Stakeholder Community Day: "Advancing Europe's Cybersecurity Partnership: Made in Europe, Delivered Globally", Brussels, Belgium, *in person*, 13 May 2026
CyberSEE, CyberSouth+, Octopus Project, GLACY-e	Cyber Games 2026 with INTERPOL Marrakech, Morrocco, *in person,* 19-21 May 2026
CyberSEE	Support the workshops in Serbia for implementation of national platform for reporting high-tech crime, Zlatibor, Serbia, *in person,* 20 May 2026
CyberSPEX	Meeting with Spanish authorities on the implementation of the Second Additional Protocol, Madrid, Spain, *in person*, Madrid, Spain, 21 May 2026

GLACY-e, CyberSPEX	CiberRED and International conference on Second Additional Protocol (with CyberSPEX), Madrid, Spain, *in person*, 21-22 May 2026
CyberSPEX	PoC Meeting of EU m/s on emergency procedures under the 2AP, *in person*, Bucharest, Romania, 21 May 2026
GLACY-e	E-evidence training, Freetown, Sierra Leone, *in person*, 25-29 May 2026
GLACY-e	Train the Trainers - Advanced judicial training (federal judges), *in person*, 25-29 May 2026
CyberSEE, CyberEast+,	Support organisation of EuroDIG, Brussels, Belgium, *in person,* 26-27 May 2026
CyberSEE	CyberSEE 5th Steering Committee Meeting, Brussels, Belgium, *in person,* 28 May 2028
Octopus Project	Advisory mission on legislation for Trinidad and Tobago, April-June 2026, online
Octopus Project	Further development of the Cyberviolence Resource through analysis of responses received via the T-CY questionnaire, with focus on domestic legislation
Octopus Project	Further development of the CYBOX platform
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026

June 2026

CyberSEE, GLACY-e, CyberSouth+	Cyber-Skills Sharing Programme, 1st Edition, global, *in person,* January–June 2026
CyberSPEX	4th Steering Committee Meeting, *in person*, Strasbourg, France, 1 June 2026
CyberSPEX	Third Consultation with civil society stakeholders, service providers and the industry (with T-CY), *in person,* Strasbourg, France, 2 June 2026
CyberSEE, Octopus Project – CYBERKOP Action	ISS World workshops, Prague, Czechia, *in person,* 2-4 June 2026
C-PROC	The 34th Plenary of the T-CY, Strasbourg, France, *in person,* 3-4 June 2026
GLACY-e	5th Steering Committee Meeting, Strasbourg, France, *hybrid*, 5 June 2026
CyberEast+	Steering Committee Meeting and presentation of Revised Barometer Reports, Strasbourg, France, *in person*, 5 June 2026
GLACY-e	Handbook on implementation of cybercrime laws: Final in person meeting of the Drafting Subcommittee, Nadi, Fiji, *in person*, 8-10 June 2026
CyberSEE	Domestic Judicial training on cybercrime and electronic evidence in Kosovo, Pristina, Kosovo*, *in person,* 9-10 June 2026

CyberSEE	Workshop on Digital Forensics - from evidence acquisition to analysis and reporting, Durres, Albania, *in person*, 9-11 June 2026
CyberSEE	Support participation in AP Twins Meeting at Europol, The Hague, The Netherlands, *in person*, 9-11 June 2026
GLACY-e	INTERPOL Operation Sunset, Lima, Peru, *in person*, 9-11 June 2026
CyberSouth+, GLACY-e	International conference "Combating cybercrime: evolving threats, electronic evidence, and the imperative of international co-operation", Cairo, Egypt, *in person*, 14-15 June 2026
CyberSouth+	Fourth Steering Committee Meeting, Cairo, Egypt, *in person*, 16 June 2026
GLACY-e	Crime Fighting Week, Brussels, Belgium, *in person*, 16-18 June 2026
CyberEast+	Regional (Ukraine-wide) cyber cooperation exercise with private sector actors (critical infrastructure and service providers) with NSDC focusing on war crimes and GHRV - in cooperation with CyberUA project, Ukraine, *in person*, 16-18 June 2026
CyberSEE	Participation of Albanian Police in EUROJUST operational meeting on Ghost Call Operation, The Hague, The Netherlands, *in person*, 18-20 June 2026
CyberSPEX	Dedicated one-day session during the CEPOL-EJTN "Cross border exchange of electronic evidence" – week, Budapest, Hungary, *in person*, 23 June 2026
CyberSEE	Second Western Balkans Working Group on Digital Assets Investigation, with CEPOL, Budva, Montenegro, *in person,* 29 June - 3 July 2026
GLACY-e, CyberSouth+	INTERPOL Operation Serengeti III and ITU Regional Cyber Drills, Victoria Falls, Zimbabwe, *in person*, 30 June – 3 July 2026
Octopus Project	Advisory mission on legislation for Trinidad and Tobago, April-June 2026, online
Octopus Project	Launch of online tool on the Cyberviolence Resource further to analysis of responses received via the T-CY questionnaire, with focus on domestic legislation
Octopus Project	Further development of the CYBOX platform
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026

** 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 2026)

July 2026

GLACY-e, CyberSouth+	INTERPOL Operation Serengeti III and ITU Regional Cyber Drills, Victoria Falls, Zimbabwe, *in person*, 30 June – 3 July 2026
CyberSEE	Workshop with Montenegrin national working group on the necessary amendments to legal framework to implement SAP, Petrovac, Montenegro, *in person,* 1-2 July 2026
CyberSEE	Domestic workshops to assess progress in legislation, capacities and cooperation in Montenegro, Budva, Montenegro, *in person*, 1-2 July 2026
CyberSEE, Octopus Project – CYBERKOP Action	Domestic Training on Investigation of Cybercrime for First Responders, 7th training, *in person,* 7-8 July 2026
CyberSouth+	Regional training on Online Child Sexual Exploitation and Abuse (OCSEA) investigations: "From CyberTipline Reports to Case Resolution, Madrid, Spain, *in person,* 7 - 9 July 2026
CyberSPEX, CyberSEE	CyberSEA Conference, *in-person*, Mamaia, Romania, 28-30 July 2026
CyberSEE	Develop the Guide for investigation of cryptocurrencies, *online*
CyberSEE	Develop Judicial Training on cryptocurrencies, *online*
CyberSEE	Develop Standard Operating Procedures to seize crypto assets, *online*
Octopus Project	Further development of the Cyberviolence Resource through analysis of responses received via the T-CY questionnaire, with focus on domestic case law
Octopus Project	Further development of the CYBOX platform
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026

August 2026

GLACY-e, CyberSPEX	Meeting for Asian hubs and EU Member States, Bucharest, Romania, *in person*, 17-19 August 2026
GLACY-e	INTERPOL Instructor Development Course (IDC), Brazil, *in person*, 17-21 August 2026
CyberSPEX	Training for law enforcement on the 2AP (in co-operation with INTERPOL), Asuncion, Paraguay, *in-person*, 31 August – 04 September 2026
GLACY-e	INTERPOL Course Design Workshop, Brazil, *in person*, 24-26 August 2026
CyberSouth+	Joint Simulation exercice with EUROMED Police, Budapest, Hungary, *in person,* 24-28 Aug 2026
Octopus Project	Further development of the Cyberviolence Resource through analysis of responses received via the T-CY questionnaire, with focus on domestic case law
Octopus Project	Further development of the CYBOX platform
GLACY-e	Americas Working Group meeting for heads of unit & regional ops meeting, Paraguay, *in person*, 31 August – 4 September 2026
GLACY-e	Support on legislation: data protection - series of validation workshops (private & public sector) to finalise the Bill, Fiji, in person, week of 31st August or week of 7th September 2026 (TBC)
GLACY-e	Regional training on cybercrime - design of the course, Papua New Guinea, *online*, by end of August 2026
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026
CyberSPEX	Development of a Model Course for training competent authorities in support of the implementation of the Second Additional Protocol, *in person and online*, by August 2026

September 2026

GLACY-e	Americas Working Group meeting for heads of unit & regional ops meeting, Paraguay, *in person*, 31 August – 4 September 2026
GLACY-e	Support on legislation: data protection - series of validation workshops (private & public sector) to finalise the Bill, Fiji, in person, week of 31st August or week of 7th September 2026 (TBC)
CyberEast+	LEA/CSIRT SOP finalisation forum, Yerevan, Armenia, *in person,* 3-4 September 2026
GLACY-e	Regional exercise on 24/7 Network, LATAM, in person, 4 September 2026

CyberSEE, CyberSouth+, GLACY-e, CyberSPEX	Underground Economy Conference, Strasbourg, France, *in person,* 7-10 September 2026
CyberSPEX	Briefing of permanent representatives about 2AP, *in person*, Strasbourg, France, 8 September 2026
GLACY-e	Operation Nightshade, Argentina, *in person*, 8-10 September 2026
CyberSEE	International workshop track on major operations against cyberattacks, Strasbourg, France, *in person,* 9 September 2026
CyberEast+	LEA/CSIRT SOP finalisation forum, Baku, Azerbaijan, *in person,* 15-16 September 2026
CyberSPEX	Training and support for the establishment and training of authorities under 2AP, *in person*, Budapest, Hungary, 15-16 September 2016
CyberSEE, CyberSouth+	Europol Cybercrime Conference, The Hague, The Netherlands, *in person, 23*-24 September 2026
GLACY-e	Train the Trainers - Introductory judicial course for state judges, Rio de Janeiro, Brazil, *in person*, 23-25 September 2026
CyberSPEX	Workshop on admissibility of electronic evidence, The Hague, The Netherlands, in person, 24-25 September 2026 (in co-operation with ULTRA XL project)
CyberSPEX	EJCN Masterclass on the Provisions of the Second Additional Protocol, *in person,* 25 September 2026
CyberSEE	Regional workshop on strategies to combat disinformation, with WB3C, Podgorica, Montenegro, *in person,* 28 September – 2 October 2026
CyberSPEX	Training for Italian Prosecutors on 2AP, *in person*, Milan, Italy, 30 September – 02 October 2026 (in cooperation with the Italian School for the Judiciary)
CyberSEE	Workshop with relevant authorities of Kosovo on the amendments to the existing legislation, Pristina, Kosovo*, *in person,* September 2026 (TBD)
CyberSEE	Domestic workshops to assess progress in legislation, capacities and cooperation in Kosovo, Pristina, Kosovo*, *in person,* September 2026 (TBD)
Octopus Project	First responder training on cybercrime and e-evidence for Seychelles, date TBC
Octopus Project, GLACY-e	Development of the guide on investigation and prosecution of online scams
Octopus Project	Further development of the Cyberviolence Resource through analysis of responses received via the T-CY questionnaire, with focus on domestic case law
Octopus Project	Further development of the CYBOX platform
GLACY-e	Adaptation and development of a e-learning introductory course for Peru on CYBOX, Peru, *online*, by December 2026

GLACY-e	Support to the legislative reform on cybercrime and electronic evidence and awareness-raising workshops on the Second Additional Protocol, Colombia, *in person and online*, by December 2026
GLACY-e	Support to the legislative reform on cybercrime and electronic evidence - alignment with the provisions of the Second Additional Protocol, Chile, *in person and online*, by December 2026

** 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, Malta, Monaco, 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 – December 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 – December 2028

Geographical scope: Global

Budget: EUR 13.334.000,00

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

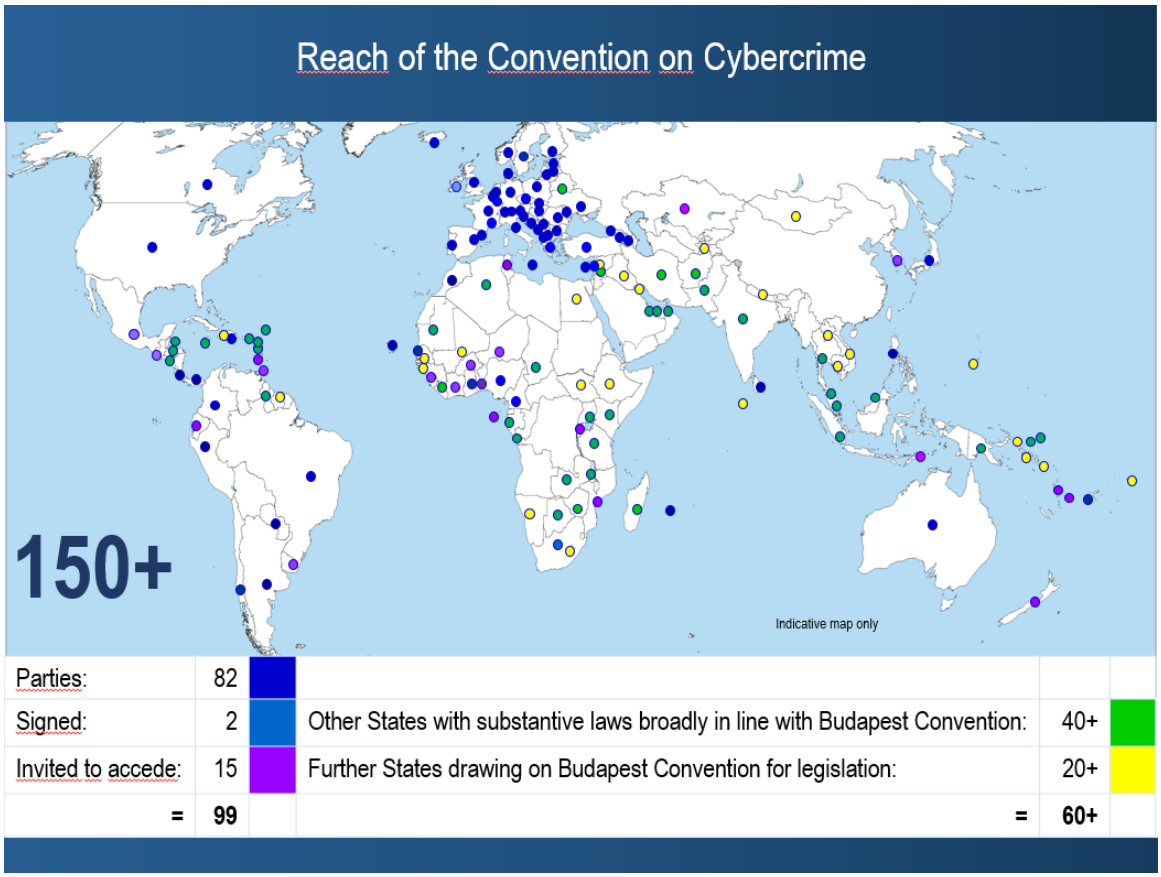
Duration: September 2023 – March 2026

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*



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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE