CYBERCRIME@COE UPDATE

October – December 2025

Highlights October – December 2025

- Bosnia and Herzegovina became the 52nd State to sign the Second Additional Protocol to Convention on Cybercrime
- 33rd T-CY Plenary adopts Workplan 2026–2027
- C-PROC: Third African Forum on Cybercrime and Electronic Evidence creates the platform to discuss and act on the continent's commitment to combat cybercrime
- CyberEast+: Countering election interference: cyber exercise and crisis communication in practice for Ukrainian election and cybersecurity professionals
- CyberSPEX: Second T-CY consultation with industry and service providers on the procedures for cooperation under the Second Additional Protocol to the Convention on Cybercrime
- CyberSEE, CyberSouth+, GLACY-e, CYBERKOP Action & Octopus Projects: The CyberVAW Conference - strengthening women's leadership against cyberviolence
- Ninth annual meeting of the Network of 24/7 points of contact

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!

- February–April 2026: Cyber-Skills Sharing Programme, 1st edition, global
- 19-21 May 2026: Cyber Games and Digital Security Challenge, Morocco
- 02 June 2026: T-CY meeting with stakeholders, France and online
- 02–04 June 2026: 34th 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 31 December 2025: 81

Signatories and States invited to accede as of 31 December 2025: 16

T-CY

Members as of 31 December 2025: 81 States Parties

Observer States as of 31 December 2025: 16

Observer Organisations as of 31 December 2025: 11

STRASBOURG, FRANCE, 14 November 2025

***In person* | Bosnia and Herzegovina became the 52nd State to sign the Second Additional Protocol to Convention on Cybercrime**

On 14 November, Ambassador Haris Bašić, Permanent Representative of Bosnia and Herzegovina, signed the Second Additional Protocol to the Convention on Cybercrime, on enhanced co-operation and disclosure of electronic evidence, in the presence of Mr. Bjørn Berge Deputy Secretary General of the Council of Europe.

The Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence was opened for signature on 12 May 2022, in Strasbourg and offers innovative tools, such as direct cooperation with service providers in other jurisdictions to obtain subscriber information, expeditious co-operation in emergency situations, joint investigation teams and joint investigations, with strong human rights and rule of law safeguards.

The event took place in the context of the 33rd Plenary of the Cybercrime Convention Committee (T-CY) on 13-14 November 2025, where the members of the Convention on Cybercrime (Budapest Convention) gathered to take stoke of the latest developments on cybercrime and electronic evidence and decide on the further directions for capacity building and other strategic matters. [READ MORE]

STRASBOURG, FRANCE, 14 November 2025

***In person* | 33rd T-CY Plenary adopts Workplan 2026–2027**

The 33rd Plenary of the Cybercrime Convention Committee (T-CY) took place in Strasbourg on 13–14 November 2025, with wide participation from Parties, Observer States, and international organisations. A key outcome of the meeting was the adoption of the T-CY Workplan for 2026–2027, which sets priorities for the next two years. A top priority is to support the signatures, ratifications, and entry into force of the Second Additional Protocol, helping Parties implement it effectively. Respect for human rights and the rule of law is essential for all States applying or acceding to the Convention on Cybercrime (Budapest Convention) and its Protocols. The T-CY remains committed to supporting Parties in applying the Budapest Convention and its Protocols, while maintaining strong safeguards for human rights and the rule of law. [READ MORE]

UPDATE: Joint Project Initiatives

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

THE HAGUE, THE NETHERLANDS, 01 October 2025

***In person & online* | Ninth annual meeting of the Network of 24/7 points of contact**

More than 100 participants from over 70 Parties and Observers to the Convention attended the event online and in presence and discussed about the ways for enhancing the cooperation through the Network. The role and responsibilities of the 24/7 PoC were addressed as well as the capacity building support provided by the Secretariat of the Network in cooperation with some of its members. The meeting offered a platform for sharing experiences and examples of successful cooperation through the Network. Furthermore, the new responsibilities for the Network to be introduced by the Second Additional Protocol were introduced and further discussed. [READ MORE]

ATHENS, GREECE, 10-11 October 2025

***In person* | CyberSEE and Octopus Project – CYBERKOP Action: Engaging in the South-Eastern European Dialogue on Internet Governance (SEEDIG) annual meeting**

The CyberSEE project and CYBERKOP Action of the Octopus project supported the SEEDIG 10, a leading regional initiative that brings together stakeholders from across South-East Europe for multistakeholder discussions on Internet governance and digital policy. Held under the theme "A Decade of Dialogue and Cooperation: What's Next?", the conference offers a platform to reflect on past achievements while fostering forward-looking dialogue on the future of digital governance and regional collaboration. [READ MORE]

BUDAPEST, HUNGARY, 13-17 October 2025

***In person* | CyberSEE, Octopus Project – CYBERKOP Action and CyberEast+: Regional police officers strengthen skills to investigate cybercrime**

Representatives from law enforcement agencies participated in an intensive international cybercrime training program. The event was jointly organised by the Australian Federal Police (AFP) and the Cybercrime Programme Office of the Council of Europe (C-PROC) through the CyberSEE project, CYBERKOP Action of the Octopus Project and the CyberEast+ project. Supported by the International Training Centre in Budapest, the initiative facilitated the enhancement of participants' technical expertise and promoted closer cooperation among agencies in addressing evolving cybercrime challenges. [READ MORE]

ANKARA, TÜRKIYE, 20-25 October 2025

***In person* | CyberSEE & GLACY-e joined forces for supporting the international training and certification of trainers on cybercrime and e-evidence**

The Council of Europe's Cybercrime Programme Office (C-PROC), in cooperation with INTERPOL, delivered the International Training and Certification of Trainers on Cybercrime and Electronic Evidence in Ankara, Türkiye.

Jointly organised under CyberSEE and GLACY-e projects, the workshop gathered law enforcement, Computer Emergency Response Teams (CERTs), Financial Intelligence Units (FIUs) and prosecutors from around 8 countries to learn how to best design, deliver and sustain high-quality, needs-based training at national and regional levels.

Across six days, participants completed INTERPOL's Instructor Development Course (IDC) and a Course Developer's Workshop (CDW), moving from foundations to practice: adult-learning principles, ADDIE-based lesson design, assessment, blended learning and ethical responsibilities. [READ MORE]

BUDVA, MONTENEGRO, 23-24 October 2025

***In person* | International Conference on Combating Cyberviolence Against Women (CYBERVAW)**

The CyberSEE joint project of the European Union and the Council of Europe in cooperation with the CyberSouth+, GLACY-e, Octopus projects and CyberKOP Action, with the support of criminal justice authorities from South-East Europe, organised the International Conference on Combating Cyberviolence Against Women (CYBERVAW), on 23-24 of October 2025, in Budva, Montenegro.

This South-East Europe initiative, turned into a broader event given the relevance of the topic and general interest of the criminal justice authorities in enhancing capacities and international cooperation on addressing cyberviolence. The event brought together 75 participants from over 25 countries, including prosecutors, judges, cybercrime investigators, policymakers, and civil society, to advance on gender-responsive approaches within criminal justice systems and sharing of good practices among jurisdictions.

The conference featured panels dedicated to key international legal frameworks, including the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol, the Istanbul Convention, the UN Convention against Cybercrime, the GREVIO General Recommendation No.1 on the digital dimension of violence against women, the draft Council of Europe Recommendation on accountability for technology-facilitated violence against women and girls, as well as the relevant EU instruments, the Directive on combating violence against women, the Digital Services Act and the AI Act.

The key outcome of this conference was a shared recognition of the importance of integrating cyberviolence provisions into broader criminal law reforms. Participants agreed that international standards and practical experiences can guide national efforts to strengthen legal frameworks, improve investigation and prosecution, and ultimately enhance protection for victims. The event thus laid the groundwork for concrete follow-up actions, cooperation and advancement of legislation and practice in this field. In addition, given the limited jurisprudence in this area, participants highlighted the value of establishing a Directory of case law on gender-based cyberviolence for use by practitioners. [READ MORE]

NAIROBI, KENYA, 25-27 November 2025

***In person & online* | C-PROC: Third African Forum on Cybercrime and Electronic Evidence creates the platform to discuss and act on the continent's commitment to combat cybercrime**

The third edition of the African Forum on Cybercrime and Electronic Evidence, organised jointly by the European Union and the Cybercrime Programme Office of the Council of Europe (C-PROC) and hosted by the Kenyan Government in Nairobi between 25-27 November, has brought together more than 350 high-level audience of policymakers, criminal justice professionals, and cybersecurity practitioners from across Africa. The Forum focuses on emerging cybercrime threats and more effective ways to address them through robust legal frameworks, capacity building efforts, and strengthened international cooperation.

African countries are increasingly aligning their legislation with international and regional standards. So far 13 African states are now Parties, and 4 more have been invited to accede to the Convention on Cybercrime (Budapest Convention), while engagement with the African Union's Malabo Convention continues to expand, signalling the continent's commitment to a global framework for combating digital crime.

Building on the success of the 2018 and 2021 editions, this year's Forum focuses on emerging cyber threats, such as AI-driven crimes, the tracing of illicit financial flows and virtual assets, data protection, online child protection against cyberviolence, and the use of electronic evidence in cross-border investigations, including showcasing practical tools to strengthen cooperation among African nations in combating cybercrime.

The Forum serves as a platform for open dialogue and knowledge-sharing among participating countries facilitating national and regional cooperation in line with best international and regional standards. Its impact extends beyond the event for ongoing collaboration and supports countries in enhancing their cybercrime and cybersecurity national legal frameworks. Key messages will be shared on the Forum's website after the event. [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

PRIZREN, KOSOVO*, 13-15 October 2025

***In person* | Octopus Project – CYBERKOP Action: Regional authorities discuss access to public documents through Initiative 2020 Conference**

The Information and Privacy Agency, together with counterpart authorities from Bosnia and Herzegovina, Croatia, North Macedonia, Montenegro, Albania, and Slovenia, concluded the Regional Conference on Access to Public Documents – Initiative 2020. During the 6th meeting of the Initiative, participants exchanged experiences and challenges related to the right of access to information, with particular focus on administrative procedures, administrative silence, and the need to strengthen proactive transparency, monitoring, enforcement mechanisms, and institutional capacities.

The authorities raised concerns over developments that may threaten institutional independence, stressing its importance for guaranteeing access to information. Discussions also addressed legislative harmonization with European and international standards, and the impact of digital transformation. The meeting was attended by the Albanian Commissioner in his role as Chair of the International Conference of Information Commissioners, who called for stronger regional cooperation.

**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.*

PRISTINA, KOSOVO*, 17 November 2025

***In person* | Octopus Project - CYBERKOP Action: Second Steering Committee meeting of the Action**

The second Steering Committee meeting of the CYBERKOP Action of the Octopus Project took place on 17 November 2025 in Pristina, co-chaired by the Council of Europe and the US Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL).

Participants reviewed the achievements and impact of the Action to date, reflecting on the progress made through the implementation of 51 capacity building activities since its launch. Discussions highlighted notable advancements in aligning the domestic legal framework with international standards, including the Convention on Cybercrime (Budapest Convention), strengthening the capacities of judicial and law enforcement authorities through targeted trainings, and fostering both interagency and international cooperation in the fight against cybercrime. Representatives of key domestic institutions – including the Ministry of Justice, the Appellate Prosecutor's Office, the Cybercrime Investigation Directorate, the Academy of Justice, the Financial Intelligence Unit, the National Cyber Security Unit (KOS-CERT), and the Information and Privacy Agency – actively contributed to the discussions, sharing updates on institutional developments and outlining priorities for the next implementation phase. [READ MORE]

PRISTINA, KOSOVO*, 17-19 November 2025

***In person* | Octopus Project – CYBERKOP Action: Strengthening cooperation at the European case handling workshop 2025**

Around 80 experts from 23 data protection authorities across the Europe met in Pristina for the European case handling workshop 2025, hosted by the Information and Privacy Agency of Kosovo*, with the support of the CYBERKOP Action of the Octopus Project.

As digital technologies reshape privacy and accountability, this workshop stands at the frontline of Europe's data protection cooperation. Organised under the Spring Conference of European Data Protection Authorities, it provided a dynamic platform for regulators and practitioners to share practical experience, explore cross-border enforcement strategies, and strengthen cooperation.

The two-day programme featured keynote sessions and interactive workshops led by various data protection authorities, focusing on AI and deepfakes, smart cameras and biometrics, data protection in cross-border collaboration, children's data on digital platforms, data scraping, and the processing of health data in the digitalisation era.

Each session dived into the real-world dilemmas emerging from the intersection of technology, privacy, and human rights, echoing the CYBERKOP Action's broader goal of building resilience against cybercrime and electronic evidence challenges.

The workshop marked a milestone for Kosovo*, highlighting its commitment to international standards and human rights, while fostering cross-border cooperation and policy dialogue on data protection across the Europe. [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.*

PUTRAJAYA, MALAYSIA, 17-19 November 2025

***In person* | Octopus Project: Stakeholder consultations on the Draft Cybercrime Bill of Malaysia**

Following the request of the Government of Malaysia to accede to the Budapest Convention, Malaysia has been invited to accede on 24 September 2025.

In view of prospective accession to and future implementation of the Convention on Cybercrime (Budapest Convention), a stakeholder consultations meeting was organised by the National Cyber Security Agency of Malaysia (NACSA) in cooperation with the Cybercrime Programme Office of the Council of Europe (C-PROC) through Octopus Project and GLACY-e, as well as ESIWA Project and the Delegation of the European Union to Malaysia. The event built on the previous work done together with Malaysia and facilitated stakeholder consultations and further support the national authorities in their efforts to strengthen the legislative framework and capacities on cybercrime and electronic evidence.

BUCHAREST, ROMANIA, 21 November 2025

***In person* | Octopus Project: Meeting with Delegation of the European Union to Barbados and the Eastern Caribbean States, the OECS and CARICOM/CARIFORUM**

On 21 November 2025, the Council of Europe's Cybercrime Programme Office (C-PROC) hosted a study visit of the Delegation of the European Union (EUD) to Barbados, the Eastern Caribbean States, the Organisation of Eastern Caribbean States (OECS) and CARICOM/CARIFORUM, the Foundation for the Internationalisation of Public Administration (FIAP) and representatives from the relevant institutions responsible for cybercrime and cybersecurity policies in Barbados, the Dominican Republic, Grenada, Guyana, Jamaica, Suriname, Trinidad and Tobago aimed at providing insights into effective responses to cybercrime. The meeting was an opportunity to introduce the participants to the Council of Europe global action of cybercrime, built on the framework of the Convention on Cybercrime (Budapest Convention), the Cybercrime Convention Committee (T-CY) and the capacity-building initiatives led by C-PROC. A particular emphasis was given to the capacity building support provided under the Octopus and the GLACY-e projects. [READ MORE]

BAMBERG, GERMANY, 25 November 2025

***In person* | Octopus Project - CYBERKOP Action: Study Visit in Germany Enhances Cooperation on Cybercrime Investigations**

A study visit was held at the Office of the Public Prosecutor General in Bamberg, bringing together representatives of the Cybercrime Directorate of the Kosovo* Police and German prosecutors and investigators specialized in cybercrime. The visit focused on how cybercrime cases are investigated, including the handling of digital evidence and the role of specialized units as key contact points for cyber incidents. The visit enabled in-depth knowledge exchange through operational discussions and case reviews, strengthening participants' understanding of investigative procedures and technological tools used in Germany. The activity enhanced investigative capacities, promoted the adoption of best practices, and reinforced professional networks, laying the groundwork for stronger future cooperation in cross-border cybercrime investigations.

PODUJEVA, KOSOVO*, 26-27 November 2025

***In person* | Octopus Project - CYBERKOP Action: Kosovo Police enhance their first-response capacities to cybercrime**

The CYBERKOP Action of the Octopus Project, in cooperation with the Kosovo* Police, have successfully concluded this year's training series for first responders, equipping 103 officers with practical competencies essential for investigating cybercrime offences from the first moment they are reported.

Developed earlier this year with the support of the CYBERKOP Action, the training programme was designed in line with international best practices and legal standards provided under the Convention on Cybercrime (Budapest Convention). As a result, participating officers are now better prepared to identify and classify cyber offences, conduct initial investigative steps, handle electronic evidence properly, and ensure effective inter-institutional coordination. These skills form the foundation of a consistent and effective first-response approach in cybercrime 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.*

ONLINE, 16-22 December 2025

***Online* | Octopus Project: Series of webinars on cyberviolence in Southeast Asia**

Cyberviolence - including non-consensual dissemination of intimate images (NCDII), online child sexual exploitation and abuse (OCSEA), and technology-facilitated trafficking in human beings - is an escalating threat globally, and in Southeast Asia in particular. Criminal justice authorities in the region confront increasingly complex cases involving: large volumes of harmful digital content, including deepfakes and extortion-related materials; livestreamed exploitation, grooming, and self-generated sexual content among children; online recruitment and exploitation linked to human beings trafficking networks, including scam compounds; cross-border data flows, jurisdictional fragmentation, and limited fast cooperation channels.

In order to address the challenges faced by the countries from the region and for enhancing their response to cyberviolence three webinars were organised by the Octopus Project.

Complementing this, the Cyberviolence Resource offers a collection of guidance, case studies, and practical tools to assist criminal justice authorities in tackling cyberviolence effectively.

The Council of Europe through the Octopus Project builds on these insights to assist countries worldwide in strengthening their national and regional responses, drawing on relevant international standards and good practices, including those developed under the Convention on Cybercrime (Budapest Convention) and its expedited tools for access to electronic evidence. Council of Europe in cooperation with Survivors & Tech Solving Image-Based Sexual Abuse (STISA).

Some 150 criminal justice authorities (especially from but not limited to) Southeast Asian countries joined the discussions online. The recordings and resources shared will be made available through the CYBOX online platform to criminal justice authorities worldwide. More webinars on the topic will be open to countries in 2026. [READ MORE]

Cyberviolence Resource – domestic criminal legislation and policies to be made accessible in 2026

Initiated following the recommendations stemming from the T-CY Mapping Study on Cyberviolence (2018), the Cyberviolence Resource is one of the online tools initiated 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 will analyse the information received so far and make it accessible on the Cyberviolence Resource online platform. Further to the 33rd T-CY Plenary, the T-CY Secretariat invites additional members and observers to submit their replies to the questionnaire, should they wish to do so.

Cyberviolence is often misunderstood and not taken as seriously as it should be. Yet, it is important to remember that cyberviolence may start online, but it often ends offline with devastating consequences for the victims and their families. Threats of violence, stalking, incitement to suicide, solicitation of children for sexual purposes… may all result in the victim self-harming or being physically attacked by the initial perpetrator. It is important to act in order to prevent cyberviolence from happening, and to protect and bring justice to the victims.

However, most countries are struggling to recognize the different facets of the problem and to address them in domestic law. Some types of cyberviolence are addressed fully or in part in international agreements, but many remain unaddressed.

The Council of Europe is working across sectors (through, for instance, the mechanisms related to the Budapest Convention, the Istanbul Convention and the Lanzarote Convention) to ensure human rights are upheld in cyberspace as well, for all. [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 – 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

SANTIAGO, CHILE, 01-03 October 2025

***In person* | GLACY-e: Strengthening responses to cybercrime in Chile: from AI challenges to international cooperation**

Between 1–3 October 2025, the joint European Union-Council of Europe GLACY-e project partnered with the Public Ministry and the Ministry of Foreign Affairs of Chile in view of strengthening cybercrime capacity through targeted workshops. The events focused on increasing awareness on the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) and on discussing content and methodological approaches of training modules addressing artificial intelligence and cybercrime.

Both activities benefited from meaningful contributions of international experts and representatives from Spain, Brazil, Peru, Costa Rica, and Argentina, who shared experiences and perspectives that enriched the discussions. Participants welcomed the support of the GLACY-e project, acknowledging that these exchanges provided a deeper knowledge on the Second Additional Protocol and the opportunity to discuss about training response to challenges and opportunities presented by AI in the fight against cybercrime. [READ MORE]

BUCHAREST, ROMANIA, 08 October 2025

***In person* | Strengthening cooperation with Kenya on cybercrime and the Budapest Convention, meeting with Hon. William Kabogo Gitau, Minister of ICT and Digital Economy of Kenya**

Representatives of the Council of Europe's Cybercrime Programme Office (C-PROC) held a productive exchange with Hon. William Kabogo Gitau, Minister of ICT and Digital Economy of Kenya, the Director of the National Computer and Cybercrimes Coordination Committee (NC4), and a representative of the Embassy of Romania in Kenya.

The meeting provided an opportunity to review ongoing collaboration between Kenya and the Council of Europe, particularly regarding the accession process of Kenya to the Convention on Cybercrime (Budapest Convention) and preparations for the Third African Forum on Cybercrime, scheduled to take place in Nairobi on 25–27 November 2025.

Discussions confirmed Kenya's strong commitment to advancing the accession process, following the country's official invitation to join the Budapest Convention. The Hon. Minister GITAU underlined his engagement with C-PROC through capacity-building activities under the GLACY-e project, on the areas of cybercrime policy and legislation and targeted trainings to Judicial, Prosecution and Law Enforcement Officials. [READ MORE]

ACCRA, GHANA, 27-29 October2025

***In person* | GLACY-e: Strengthening responses to cybercrime in Chile: from AI challenges to international cooperation**

The GLACY-e project partnered with the Cyber Security Authority of Ghana to organise the Introductory Training of Trainers course on cybercrime and electronic evidence for 30 prosecutors and law enforcement officers on 27-29 October in Accra, Ghana.

The training offered participants an introduction to the Convention on Cybercrime (Budapest Convention), highlighting its relevance to contemporary cybercrime challenges. Core topics covered during the sessions included cybercrime typologies, internet fundamentals, the handling of electronic evidence, applicable procedural powers, and mechanisms for international collaboration. Furthermore, the overview of the Second Additional Protocol, was given by providing insights into enhanced tools for international cooperation.

Over the three-day programme, participants also engaged in in-depth discussions on challenges faced by Ghana, including the securing of electronic evidence and inter-agency coordination. These exchanges provided the participants with an opportunity to share experiences and enhance their skills and knowledge.

This training represents a building block in establishing a pool of trained prosecutors and law enforcement officers at the national level, ensuring the sustainability of capacity-building efforts on cybercrime and electronic evidence. As a GLACY-e hub country, Ghana is well positioned to bolster national efforts and share its expertise on cybercrime and electronic evidence in the region. [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

BAKU, AZERBAIJAN, 14-16 October 2025

***In person* | CyberEast+: Azerbaijani investigators increase their knowledge on financial investigations, virtual currencies and Darknet**

Parallel financial investigations and identifying the online crime proceeds in cybercrime cases remain high priorities for the authorities of the Republic of Azerbaijan. In this context, CyberEast+, a joint project of the Council of Europe and of the European Union, organised a training on financial investigations, virtual currencies and Darknet, between 14 and 16 October 2025.

The Azerbaijani counterparts, including cybercrime and financial crime investigators, forensic experts, detectives, prosecutors and representatives of the Ministry of Finance, were introduced to key aspects regarding financial intelligence units (FIU) and money laundering offences, as well as social engineering, online fraud, virtual currencies, Darkweb, encryption and anonymity. Participants increased their knowledge on modus operandi of money laundering offences, red flag indicators, blockchain analysis and legal instruments for seizing cryptocurrencies, through both guidance from two Council of Europe consultants and by means of practical exercise/case studies.

The internationally recognised instruments and standards, including the Convention on Cybercrime (Budapest Convention), its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence, the Warsaw Convention and the EU Anti-Money Laundering Directives were instrumental for this activity. [READ MORE]

CHISINAU, MOLDOVA, 04-06 November 2025

***In person* | CyberEast+: Moldovan counterparts enhance their skills in conducting criminal investigations on online child sexual exploitation and abuse (OCSEA)**

Combating online child sexual exploitation and abuse (OCSEA) remains a priority for the Eastern Partnership countries and receives extensive support through CyberEast+, a joint initiative of the European Union and of the Council of Europe. Over the past years, through consolidated efforts of both the Children's Rights Division and the Cybercrime Programme Office of the Council of Europe (C-PROC), criminal justice authorities of the region's countries have enhanced their knowledge and capacities on the legal provisions and available tools for investigating, prosecuting and adjudicating OCSEA cases, in line with the Convention on Cybercrime (Budapest Convention) and the Lanzarote Convention.

These efforts were further examined during the training on the use of open-source intelligence (OSINT) in investigating OCSEA, organised by the CyberEast+ project between 4 and 6 November 2025 in Chisinau, the Republic of Moldova. Representatives of the Ministry of Internal Affairs, the National Institute of Justice, the Superior Council of Magistracy and the General Prosecutor's Office analysed a series of open-source intelligence (OSINT) tools used for the detection, investigation and prevention of OCSEA through dedicated practical exercises. The training also provided a forum for authorities from the Republic of Moldova to discuss ways to improve national practices, as well as to enhance cooperation in OCSEA investigations, on the basis of the Convention on Cybercrime and of the Lanzarote Convention. [READ MORE]

STRASBOURG, FRANCE, 12 November 2025

***In person* | CyberEast+: Eastern Partnership stakeholders discuss key outcomes during the Third Steering Committee meeting of the project**

The CyberEast+ project, a joint initiative of the European Union and of the Council of Europe, held its third Steering Committee meeting on 12 November 2025 in Strasbourg, France. On this occasion, two cybersecurity projects supported by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) and the e-Governance Academy, were invited to present their activities in Ukraine, Armenia, the Republic of Moldova and Azerbaijan, and discuss possible synergies with the CyberEast+ project.

Representatives of the project countries, present in person and online, assessed the effectiveness of the project strategy, took stock of the achievements made since the project's action in 2025 and agreed on further steps needed to address emerging cybercrime trends though capacity building in 2026 and beyond. Key stakeholders updated on the state of play in terms of legislation, policies, capacities and cooperation on cyber resilience in Armenia, Azerbaijan, the Republic of Moldova and Ukraine. All participants stressed the importance of aligning their domestic legislations with the provisions of the Convention on Cybercrime (Budapest Convention), its Second Additional Protocol, as well as with the European Union legislation, especially with the Directive 2022/2555 (NIS2). [READ MORE]

UKRAINE, December 2025

***In person* | CyberEast+: Countering election interference: cyber exercise and crisis communication in practice for Ukrainian election and cybersecurity professionals**

In December 2025, an exercise on "Cyber interference in elections: response, investigation, forensics and interagency cooperation" was held to strengthen the capacity of the Ukrainian national authorities concerned in countering cyber threats and disinformation in electoral processes. This activity, organised with the support of the Council of Europe in cooperation with the Central Election Commission of Ukraine, combined the exercise on detecting and investigating election-related cybercrime and cybersecurity incidents with a workshop on crisis communications focused on communication response to cyber interference and disinformation in elections.

The exercise gathered representatives of the Central Election Commission of Ukraine, along with officials from national authorities responsible for election security, cybersecurity, cybercrime investigations, and information security.

During the cyber exercise, the participants enhanced their knowledge and skills on handling election-related cybercrime and cybersecurity incidents, focusing on the analysis of e-evidence, digital forensics, detecting criminal activity, and relevant interagency coordination. The accompanying cybersecurity crisis communication workshop strengthened participants' knowledge and skills in strategies and tactics for preventing and mitigating the impact of disinformation, as well as in interagency coordination mechanisms to counter disinformation campaigns and tools for communication response to cyber threats and incidents that could undermine public trust in electoral processes. [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.*

THE HAGUE, THE NETHERLANDS, 01 October 2025

***In person & online* | Support to CyberSouth+ partners attending the Ninth annual meeting of the Network of 24/7 points of contact**

The Council of Europe, through the Cybercrime Programme Office, organized the ninth Annual Meeting of the 24/7 Points of Contact at the EUROPOL premises. According to Article 35 of the Convention on Cybercrime (Budapest Convention), the 24/7 Network facilitates immediate assistance with e-evidence collection and expedited data preservation - as a distinctive element - for cybercrime investigations carried out by the members of the Network. More than 100 participants from over 70 Parties and Observers to the Convention attended in an effort to further develop cooperation. [READ MORE]

BUDVA, MONTENEGRO, 23-24 October 2025

***In person* | CyberSouth+: CyberVAW Conference - strengthening women's leadership against cyberviolence**

The CyberSouth+ joint project of the European Union and the Council of Europe, in cooperation with CyberSEE, GLACY-e, Octopus and the CyberKOP Action projects, came together to advance gender-responsive approaches within the criminal justice systems and share on good practices. The event brought together 75 participants from over 25 countries and featured panels dedicated to key international legal frameworks. [READ MORE]

LISBON, PORTUGAL, 29 October 2025

***In person* | GLACY-e and CyberSouth+: Advancing AI and cybercrime capacity building: Insights from the Lisbon Forum**

CyberSouth+ and GLACY-e supported the workshop on "The role of capacity building in the era of artificial Intelligence and cybercrime", held as part of the Lisbon Forum on AI and Global Governance. The workshop highlighted the critical role of capacity building as the participants underlined the need for continuous trainings such as AI ethics, digital forensics, electronic evidence handling and procedural safeguards. [READ MORE]

TUNIS, TUNISIA, 20 November 2025

***In person* | CyberSouth+: Synergies between the Budapest and Hanoi Conventions on cybercrime explored during a workshop in Tunisia**

The CyberSouth+ project organised a national workshop in Tunis on international standards for cybercrime legislation, with a particular focus on exploring synergies between the Council of Europe Convention on Cybercrime (Budapest Convention) and the United Nations Convention against Cybercrime (Hanoi Convention).

The workshop was organised in cooperation with the Council of Europe Office in Tunis and the Ministry of Foreign Affairs, Migration and Tunisians Abroad. It brought together representatives from the Ministry of Justice, the Ministry of Interior, the Assembly of the Representatives of the People, and other relevant national institutions. [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, 03 October 2025

In person | CyberSEE: Montenegro advances legislative alignment for the ratification of the Second Additional Protocol to the Convention on Cybercrime

On 3 October 2025, the CyberSEE joint project of the European Union and the Council of Europe, in cooperation with the Ministry of Justice of Montenegro, organised in Podgorica a high level workshop to support the established national working group in harmonization of the national legislation in view of the ratification of the Second Additional Protocol (2AP) to the Convention on Cybercrime (Budapest Convention).

The workshop brought together representatives from the Ministry of Justice, members of the national working group, judicial authorities, alongside Council of Europe experts. Discussions centred on the identification of the national legislation to be amended for implementing the new tools for enhanced co-operation offered by the Protocol. [READ MORE]

BELGRADE, SERBIA, 04-05 November 2025

In person | CyberSEE strengthening capacities in digital forensics and electronic evidence

From 4 to 5 November 2025 the CyberSEE joint project of the European Union and the Council of Europe contributed to organising the Digital Forensics Conference 2025, in Belgrade, Serbia. The event gathered over 200 prosecutors, judges, cybercrime investigators, forensic specialists, and officials from the Ministries of Justice, alongside experts from the private sector, cybersecurity industry, and financial services across South-East Europe and Türkiye to exchange good practices and strengthen their technical and operational capacities in digital forensics, cross-border investigations, and the handling of electronic evidence.

During the first day, the attendees explored how cybercriminal networks operate across borders and how investigators and private companies can respond effectively. Participants also examined topics such as tracing online criminal networks, Open-Source Intelligence (OSINT)-based methods, and the evolving landscape of anti-money laundering and countering the financing of terrorism (AML/CFT) standards in the digital economy. The session "Challenges and Solutions in Cross-Border Cybercrime Investigations and Live Acquisition of Electronic Evidence" led by CyberSEE experts delved into live data forensics and encryption handling techniques, emphasizing through case studies, the practical challenges of evidence acquisition and analysis, while showcasing how live forensics differs from traditional approaches.

On the second day, the discussions underlined the importance of data integrity, governance, and cross-border cooperation in crypto investigations. A highlight was the Operation PATHFINDER session which showcased real-world police collaboration between the Czech Republic and Ukraine and illustrated how effective cross-border cooperation, data sharing, and forensic readiness can sustain investigations even under crisis conditions.

The event concluded with two hands-on workshops, one addressing the Suspicious Activity Reports (SAR) / Suspicious Transaction Reports (STR) on compliance reporting for U.S. and EU financial intelligence units, and one on ransomware investigation providing participants with practical skills for tackling emerging financial and cyber threats. [READ MORE]

ANTALYA, TÜRKIYE, 04-07 November 2025

***In person* | CyberSEE builds judicial capacities for enhancing the international cooperation on cybercrime and electronic evidence**

From 4 to 7 November 2025, the CyberSEE joint initiative of the European Union and the Council of Europe project organised a Specialised Judicial Training Course on International Cooperation on cybercrime and electronic evidence in Antalya, Türkiye.

The training brought together around 50 judges, prosecutors, representatives of the Ministry of Justice, the Justice Academy of Türkiye, and national trainers, to enhance their skills on international cooperation on cybercrime and electronic evidence. Participants deepened their understanding of the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol (2AP), focusing on provisions, tools and mechanisms, such as mutual legal assistance (MLA) and spontaneous information exchange. [READ MORE]

SKOPJE, NORTH MACEDONIA, 24-25 November 2025

***In person* | CyberSEE supports North Macedonia to advance legislative alignment with the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)**

On 24 November 2025, a domestic expert meeting on the provisions of the Second Additional Protocol (2AP) to the Convention on Cybercrime (Budapest Convention) organised by the CyberSEE project in cooperation with the Ministry of Justice took place in Skopje, North Macedonia.

Building on the foundations set during the high-level domestic workshop held on 3 April 2025, the meeting gathered representatives of key criminal justice authorities, including the Ministry of Justice, the Ministry of Interior, prosecutors, judges, draft legislators, as well as representatives of the Council of Europe's Office in Skopje.

Throughout the sessions, the experts presented and reviewed the draft Assessment Report benchmarking national legislation against the Second Additional Protocol discussed required legislative amendments, and examined Articles 6–14 of the Protocol, including key definitions and for their implementation. The event enabled national stakeholders to gain a clearer understanding of the legal reforms needed for the ratification and effective implementation of the Protocol, while identifying new legal concepts to be integrated and further areas where technical assistance would be beneficial. [READ MORE]

SARAJEVO, BOSNIA AND HERZEGOVINA, 09 December 2025

***In person* | CyberSEE: Fourth Steering Committee Meeting**

On 9 December 2025, the CyberSEE joint project of the European Union and the Council of Europe organised its fourth Steering Committee Meeting, gathering representatives of the European Commission, the European Union Delegation to Bosnia and Herzegovina, the Council of Europe, and officials from the criminal justice authorities of all project countries/areas. The meeting provided a complete overview of the project's achievements in 2025 and clear insights into how the delivered outcomes align with the scope of the action.

The meeting highlighted the support provided to the legal reforms in the project countries/areas through a mix of practical activities organised at domestic, regional, and international levels. These achievements followed tailor-made roadmaps for each country/areas and included high-level meetings with decision makers, assessments of existing national laws, and technical workshops with national working groups to draft the necessary amendments. The signature by Bosnia and Herzegovina of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention) and the development of Serbia's Cybercrime Strategy were acknowledged as key results. [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

LJUBLJANA, SLOVENIA, 07 October 2025

BRATISLAVA, SLOVAK REPUBLIC, 20 October 2025

WARSAW, POLAND, 04-05 November 2025

***In person* | CyberSPEX: CyberSPEX: National meetings on the implementation of the Second Additional Protocol**

In October and November 2025, the CyberSPEX joint project of the European Union and the Council of Europe held three in-country workshops in Slovenia, Slovakia and Poland to support national preparations for the implementation of the Second Additional Protocol (2AP) to the Convention on Cybercrime (Budapest Convention).

The workshop in **Ljubljana** (7 October), focused on domestic legislative changes in implementing Articles 6–10 of the Protocol, highlighted accompanying safeguards and the needs of both authorities and private-sector entities.

The meeting in **Bratislava** (20 October) enabled members of the national drafting working group and service providers to explore legislative reforms required to implement the Protocol and align it with the EU e-Evidence Package.

The meeting in **Warsaw** (4 November) was organized in co-operation with the National Prosecutor's Office and informed the relevant stakeholders from the public authorities about the provisions of the Protocol. [READ MORE]

STRASBOURG, FRANCE, 12 November 2025

***In person* | CyberSPEX: Second T-CY consultation with industry and service providers on the procedures for cooperation under the Second Additional Protocol to the Convention on Cybercrime**

The meeting focused on how to best implement the provisions of the Second Additional Protocol (2AP) in practice and create efficient and safe mechanisms for their operational application.

Through discussions structured around cross-border cooperation, verification and authentication of requests, secure data handling, and conditions for cooperation under the Protocol, participants examined practical mechanisms for implementing 2AP and shared challenges and good practices. [READ MORE]

BRUSSELS, BELGIUM, 20-21 November 2025

***In person* | CyberSPEX: CyberSPEX: Regional meeting in support of the implementation of the Second Additional Protocol to the Convention on Cybercrime – Western European countries**

The meeting brought together representatives from Belgium, France, Germany, Luxembourg and The Netherlands and provided an opportunity for legal drafters and authorities to deepen their understanding on the 2AP's mechanisms, share national experiences, and discuss proposals of ongoing legislative measures under the 2AP, designed to strengthen cross-border co-operation with service providers and other stakeholders. [READ MORE]

SARAJEVO, BOSNIA AND HERZEGOVINA, 09 December 2025

***In person* | CyberSPEX: Third Steering Committee meeting in support of the implementation of the Second Additional Protocol**

The event brought together representatives from EU member states, EU institutions and partner initiatives to review progress in the implementation of the Second Additional Protocol (2AP) to the Convention on Cybercrime (Budapest Convention) in the project countries.

Moreover, it highlighted the project's strong engagement through the Regional meetings and in-country events. Major events organised by CyberSPEX like the EUROJUST/CoE co-branded workshop and the 2nd T-CY consultation with service providers and the industry were marked as important venues for the exchange of knowledge and opinion.

Participants discussed achievements and challenges in aligning domestic legislation with the Protocol and shared updates on the national implementation efforts.

The Steering Committee also examined ongoing project activities and endorsed priorities for the December 2025 – June 2026 workplan, including tailored capacity-building support, development of guidance tools, and cooperation with EU-funded initiatives such as SIRIUS.

CyberSPEX will continue to support EU member states in strengthening cross-border cooperation on electronic evidence, while ensuring compliance with human rights, the rule of law and data protection safeguards. [READ MORE]

SARAJEVO, BOSNIA AND HERZEGOVINA, 10-11 December 2025

***In person* | CyberSEE and CyberSPEX: International workshop on the implementation of the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention)**

By gathering legislators, advisors, and practitioners from the judiciary and law enforcement from EU member states, South-East Europe and Türkiye, the workshop provided a technical platform to examine the requirements and challenges posed by the implementation of the Protocol. Experience in cooperation with service providers and in emergency situations were shared by Belgium, Bosnia and Herzegovina, Kosovo*, Latvia, Serbia and Türkiye by presenting concrete cases.

At the same time, the workshop addressed potential solutions for domestic challenges in implementing the instrument and its interaction with the EU e-Evidence package and other legal treaties. Participants enhanced their knowledge of the Second Protocol implementation processes, identified legislative requirements, exchanged good practices, and identified counterparts for further support, while reaffirming the need for strengthened interagency cooperation, enhanced peer exchange and sustained technical assistance.

The national progress made in the implementation of the Second Protocol by Albania, Bosnia and Herzegovina, Italy, Montenegro, North Macedonia and Slovenia generated active discussions on the use of definitions, the appointment of authorities, data protection requirements and the interaction with other EU instruments like EU e-Evidence package, NIS2 directive and EU GDPR. [READ MORE]

Inventory of activities (October – December 2025)

October 2025

C-PROC	Annual Meeting of 24/7 Contact Points, The Netherlands, *in person*, 01 October 2025
GLACY-e	Workshop Cybercrime and artificial intelligence, identification of training needs for judges and prosecutors, Chile, *in person*, 01 October 2025
CyberSPEX	Support procedures on emergency disclosure (art.9) and emergency mutual assistance (art. 10) - Annual 24/07 PoC meeting and EUROPOL Conference, The Netherlands, *in person*, 01–03 October 2025
GLACY-e	Awareness workshop with the legislators on Second Additional Protocol, Chile, *in person*, 02 October 2025
GLACY-e	Workshop on Budapest Convention, Pacific, *online*, 02 October 2025
C-PROC	EUROPOL Cybercrime Conference, The Netherlands, *in person*, 02–03 October 2025
GLACY-e	Awareness workshop with the service providers on Second Additional Protocol, Chile, *in person*, 03 October 2025
CyberSPEX	Domestic Meeting on the implementation of the Second Additional Protocol to the Convention on Cybercrime in Slovenia, *in person*, 07 October 2025
CyberEast+	Advanced cybercrime training: OCSEA Investigations and OSINT, Azerbaijan, *in person*, 07–09 October 2025
GLACY-e	Support to the legislative reform - debriefing session with the working group, Uruguay, *online*, 08 October 2025
CyberSEE, CYBERKOP	Support SEEDIG Annual Meeting, Greece, *in person*, 10–11 October 2025
CyberSEE, Octopus Project - CYBERKOP Action	Cybercrime investigations course in cooperation with Australian Federal Police, Hungary, *in person*, 13–17 October 2025
CyberEast+	Advanced cybercrime training: Virtual Currencies and Darknet, Azerbaijan, *in person*, 14–16 October 2025
Octopus Project	Participation in the expert meeting on cross-border cooperation on e-evidence for Kyrgyzstan, *online,* 16 October 2025
GLACY-e	National consultation on the new cybercrime bill, Nigeria, *in person*, 16–17 October 2025
CyberSPEX	Meeting on the implementation of the Second Additional Protocol to the Convention on Cybercrime in Slovakia, *in person*, 20 October 2025

CyberSEE, GLACY-e, INTERPOL	Regional law enforcement training and certification of trainers on cybercrime and electronic evidence (ToT), Türkiye, *in person*, 20–25 October 2025
CyberEast+	Advanced cybercrime training: Virtual Currencies and Darknet, Ukraine, *in person*, 21–23 October 2025
Octopus Project, GLACY-e	Support to the legislative reform - Stakeholder consultations on the cybercrime bill, Malaysia, *in person*, 22–23 October 2025
C-PROC	CYBERVAW Conference on Cyberviolence Against Women, Montenegro, *in person*, 23–24 October 2025
GLACY-e	Train the Trainers – introductory judicial course (prosecutors and LEA), Ghana, *in person*, 27–29 October 2025
CyberEast+	National discussions on responsible reporting and cyberviolence, Moldova, *in person,* 28–29 October 2025
GLACY-e	V Technical round table on security issues between the Government of Ecuador and the European Union, Ecuador, *online*, 28–29 October 2025
CyberSEE	Support participation in INTERPOL "International Child Sexual Exploitation (ICSE) database training", France, *in person*, 28–30 October 2025
GLACY-e, CyberSouth+	Workshop on the role of capacity building in the era of artificial intelligence and cybercrime, Portugal, *in person*, 29 October 2025
CyberSEE	Domestic meeting with Montenegrin relevant institutions dedicated on the details of the SAP and roadmap of the legislative reform process, Montenegro, *in person*, 30 October 2025
CyberSEE	Participation of Ministry of Security of BiH to Cybersecurity Summit, Serbia, *in person*, 30 October 2025
CyberEast+	Specialised course: Combating criminal disinformation through tools against cybercrime, Ukraine, *in person*, 30–31 October 2025
GLACY-e	Workshop on mainstreaming cybercrime and electronic evidence in the training curricula (prosecutors and LEAs), Ghana, *in person*, 30–31 October 2025
CyberSPEX	Further development of the Help Course, *desk research*, February–November 2025
GLACY–e	Support for the legislative process on data protection, Mozambique, *desk study, online and in person*, May–December 2025
CyberSouth+	Adaptation of the judicial training materials on cybercrime and electronic evidence and national course delivery in Egypt, *online & in person*, July–November 2025
Octopus Project	CYBOX onboarding users and further work on improvement, *online*, October–December 2025
Octopus Project	Ongoing work for the Cyberviolence Resource and the Octopus platform, *online*, October–December 2025

November 2025

CyberSPEX	Meeting on the implementation of the Second Additional Protocol to the Convention on Cybercrime in Poland, *in person*, 04 November 2025
CyberSEE	Support the Regional Digital Forensics Conference, Serbia, *in person,* 04–05 November 2025
CyberEast+	Advanced cybercrime training: OCSEA Investigations and OSINT, Moldova, *in person,* 04–06 November 2025
GLACY-e	Support for the legislative process on data protection – workshop, Mozambique, *in person*, 04–06 November 2025
CyberSEE	Domestic Judicial training on international cooperation in Türkiye, *in person*, 04–07 November 2025
CyberSPEX	Training with Polish cybercrime prosecutors on the direct co-operation provisions Art. 6 and Art. 7 of the Second Additional Protocol, Poland, *in person*, 05 November 2025
CyberSEE , Octopus Project - CYBERKOP Action	Third Training on Investigation of Cybercrimes for First Responders, Kosovo*, *in person*, 05-06 November 2025
Octopus Project	T-CY AI Working Group meeting, France, *in person and online*, 11 November 2025
CyberSEE	Support participation in the Europol Cybercrime Prevention Forum, under EMPACT OA 7.1, The Netherlands, *in person*, 11–12 November 2025
T-CY, C-PROC	Second meeting with industry and service providers on the procedures enhancing direct cooperation under the Second Additional Protocol to the Convention on Cybercrime, France, *in person and online*, 12 November 2025
CyberEast+	Third Steering Committee Meeting, France, *in person,* 12 November 2025
T-CY, C-PROC	33rd Plenary of the Cybercrime Convention Committee (T-CY), France, *in person,* 13–14 November 2025
GLACY-e, CyberSPEX	CiberRed Plenary and International Conference on Second Additional Protocol, Portugal, *in person*, 17–18 November 2025
CyberEast+	Contribution to the Lanzarote Committee event on Capacity Building and Plenary Session, Moldova, *in person*, 18–19 November 2025
CyberEast+	Training on SOPs - Use of compatible tools for handling and forensics producing admissible evidence, Azerbaijan, *in person*, 18–19 November 2025
CyberSPEX	Regional Meeting in support of the implementation of the Second Additional Protocol to the Budapest Convention - Western European Countries, Belgium, *in person*, 20 - 21 November 2025
Octopus Project	Study visit to C-PROC of the delegation of Caribbean countries, Romania, *in person*, 21 November 2025
CyberSPEX	In-country meeting for the implementation of the Convention on Cybercrime (Budapest Convention) in Ireland, *in person*, 24 November 2025

CyberSEE	Workshop with North Macedonian national working group on the necessary amendments to existing legal framework to implement SAP provisions, North Macedonia, *in person,* 24 November 2025
CyberEast+	Course on Combating criminal disinformation through tools against cybercrime, Armenia, *in person*, 24–25 November 2025
CyberSEE	Domestic roundtable in North Macedonia of criminal justice authorities and private sector on 2AP, North Macedonia, *in person*, 25 November 2025
GLACY-e, Octopus Project, CyberSouth+	3rd African Forum on Cybercrime and Electronic Evidence, Kenya, *in person and online*, 25–27 November 2025
Octopus Project	Regional 24/7 Points of Contact Network training for Africa, Kenya, *in person*, 26 November 2025
GLACY-e	Support to the First International Congress on Cybercrime, Peru, *in person*, 26–28 November 2025
GLACY-e	Support to the national training on international cooperation on cybercrime and electronic evidence, Argentina, *in person,* 27 November 2025
CyberSPEX	Further development of the Help Course, *desk research*, February – November 2025
GLACY–e	Support for the legislative process on data protection, Mozambique, *desk study, online and in person*, May–December 2025
CyberSouth+	Adaptation of the judicial training materials on cybercrime and electronic evidence and national course delivery in Egypt, *online & in person*, July–November 2025
CyberSPEX	Prepare inventory of provider policies with respect to language of orders, WHOIS, notifications and confidentiality policies, *desk research*, July 2025 – January 2026
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 EJCN (EUROJUST), *desk research*, July 2025 – January 2026
Octopus Project	CYBOX onboarding users and further work on improvement*, online*, October-December 2025
Octopus Project	Ongoing work for the Cyberviolence Resource and the Octopus platform, *online*, October-December 2025
CyberSEE	Provide guidance to the Montenegrin national working group on the necessary amendments to existing national legal framework to implement 2AP provisions, *online*, November 2025–March 2026
CyberSEE	Provide guidance to the North Macedonian national working group on the necessary amendments to existing national legal framework to implement 2AP provisions, *online,* November 2025–March 2026

December 2025

GLACY-e	Train the Trainers: Advanced Judicial Course on Cybercrime and Electronic Evidence, Dominican Republic, *in person*, 01–05 December 2025
CyberEast+	Training organised for Ukraine: SCADA/energy sector attack investigations, Ukraine, *in person*, 02-03 December 2025
GLACY-e	4th Steering Committee, *online*, 03 December 2025
CyberEast+	Meeting with Internet service providers, Ukraine, *in person*, 04 December 2025
CyberEast+	Elections interference exercise in partnership with Democracy Department and Kyiv Office, Ukraine, *in person*, 08-12 December 2025
GLACY-e	Support to the 7th annual Victim Identification Task Force (VIDTF) Asia, Singapore, *in person*, 08-12 December 2025
CyberSEE	4th Project Steering Committee Meeting, Bosnia and Herzegovina, *in person*, 09 December 2025
CyberSPEX	3rd Steering Committee Meeting, Bosnia and Herzegovina, *in person*, 09 December 2025
CyberSPEX CyberSEE,	International workshop in support of the implementation of the Second Additional Protocol to the Budapest Convention - European Union countries, South-East Europe & Türkiye, Bosnia and Herzegovina, *in person*, 10-11 December 2025
GLACY-e	Training on Darknet and Crypto for Prosecutors and Law Enforcement, Costa Rica, *in person*, 09–11 December 2025
GLACY-e	Debriefing meeting on the draft conclusions of the gap analysis of the New Cybercrime Bill, Ghana, *online*, 15 December 2025
Octopus Project	[1/3] Webinar on non-consensual dissemination of intimate images (series of webinars on cyberviolence in Southeast Asia), *online,* 16 December 2025
Octopus Project	[2/3] Webinar on livestreamed child sexual exploitation and abuse (series of webinars on cyberviolence in Southeast Asia), *online,* 18 December 2025
Octopus Project	[3/3] Webinar on technology-facilitated trafficking in human beings linked to scam compounds (series of webinars on cyberviolence in Southeast Asia), *online,* 22 December 2025
GLACY–e	Support for the legislative process on data protection, Mozambique, *desk study, online and in person*, May 2025 – February 2026
Octopus Project	CYBOX onboarding users and further work on improvement, *online*, October-December 2025
Octopus Project	Ongoing work for the Cyberviolence Resource and the Octopus platform, *online*, October-December 2025
CyberSEE	Provide guidance to the Montenegrin national working group on the necessary amendments to existing national legal framework to implement 2AP provisions, *online*, November 2025–March 2026

CyberSEE	Provide guidance to the North Macedonian national working group on the necessary amendments to existing national legal framework to implement 2AP provisions, *online,* November 2025–March 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 (January – March 2026)

January 2026

GLACY-e	Training of Trainers, Gendered aspects of cybercrime, Peru, 12–16 January 2026
CyberSouth+	3rd Steering Committee of the CyberSouth+ Project, *online*, 14 January 2026
CyberSEE, C-PROC	Cyber-Skills Sharing Programme, 1st Edition, global, *in person*, January – March 2026
CyberSEE	Develop the Guide for investigation of cryptocurrencies, *online*, January – April 2026
CyberSEE	Assessment of the Montenegrin national legislation, benchmarked against SAP provisions, *online,* January – April 2026
CyberEast+	Cooperation forum with key infrastructure and service providers on reporting and data handling – Armenia, *in person*, 20-21 January 2026
C-PROC	Support participation to UN AHC session to prepare the RoP for the COSP to the UN Convention against Cybercrime, Austria, *in person*, 26-30 January 2026
GLACY-e	Operation Red Card II (AFJOC), Senegal, *in person*, 27-30 January 2026

February 2026

CyberSEE; GLACY-e; CyberSouth+	Cyber-Skills Sharing Programme, 1st Edition, global, *in person,* January–April 2026
CyberSEE	Develop the Judicial Training on cryptocurrencies, *online,* February–May 2026
CyberSEE	Regional workshop to combat disinformation, with WB3C Podgorica, Montenegro, *in person,* February 2026 (TBD)
GLACY-e	INTERPOL Crypto Investigation and Compliance Training (AME-Desk) - EN edition, LATAM, *online*, 04 February 2026
GLACY-e	INTERPOL Crypto Investigation and Compliance Training (AME-Desk) - ES edition, LATAM, *online*, 06 February 2026
CyberSEE	Participation of CERT MoI Serbia at the TF-CSIRT & FIRST Regional Symposium Europe, Spain, *in person,* 04-06 February 2026
CyberSPEX	Domestic Meeting with authorities and service providers on the implementation of the Second Additional Protocol to the Convention on Cybercrime in Italy, Rome, Italy, *in person,* 06 February 2026
CyberEast+	Cooperation forum with key infrastructure and service providers on reporting and data handling, Moldova, *in person,* 10-11 February 2026
CyberEast+	HELP course for defence attorneys, Azerbaijan, *in person*, 17-19 February 2026

GLACY-e	Awareness workshop with the service providers on Second Additional Protocol, Colombia, *in person*, 24 February 2026
GLACY-e	Introductory workshop with the academic sector on Second Additional Protocol, co-organized with the New Granada Military University (UNMG), Colombia, *in person*, 25 February 2026
GLACY-e	Introductory workshop with the diplomatic sector on Second Additional Protocol, co-organized with the Augusto Ramirez Ocampo Diplomatic Academy, Colombia, *in person*, 26 February 2026
GLACY-e	Multi-stakeholder dialogue platform with institutions of Colombia on Second Additional Protocol – review of the legislative reform, Colombia, *in person*, 26 February 2026
CyberSEE	Participation in the Europol Industry and Research Days, The Hague, The Netherlands, *in person,* 24-26 February 2026
CyberSEE	Regional meeting to assess the existing capacities and statistics of cybercrime units as well as the international and public/private cooperation, The Netherlands, *in person*, 24-26 February 2026
CyberSPEX	Workshop with German registries and registrars on Art. 6 of the Second Additional Protocol, *online*, February 2026
GLACY-e	Support on legislation: data protection - skeleton of the Bill, Fiji, *online*, by end of February 2026
GLACY-e	Support on legislation: Second Additional Protocol - desk study, Fiji, *online*, by end of February 2026
GLACY-e	Support on legislation: data protection - draft Bill, Fiji, *online*, by end of February 2026
GLACY-e	Support to the legislative reform - desk study on the SAP and national legislation, Chile, *in person and online*, February – Decemebr 2026
CyberSouth+	Training modules on cybercrime and digital investigations for criminal justice professionals, Palestine*, February – May 2026

March 2026

CyberSEE	Cyber-Skills Sharing Programme, 1st Edition, global, *in person,* January–April 2026
CyberSEE	Develop the Judicial Training on cryptocurrencies, *online,* February–May 2026
CyberSEE, Octopus Project – CYBERKOP Action	Regional Training on investigating OCSEA starting from NCMEC reports, Pristina/Tirana (TBD), *in person*, March 2026
CyberSEE, Octopus Project – CYBERKOP Action	Regional meeting with service providers on information sharing in cases of OCSEA, Pristina/Tirana (TBD), *in person*, March 2026
CyberSEE	Workshop with Bosnia and Herzegovina national working group on the necessary amendments to existing legal framework to implement SAP provisions, Bosnia and Herzegovina, *in person,* March 2026
CyberSEE	Domestic workshop to assess legislative progress in Bosnia Herzegovina, Sarajevo, Bosnia and Herzegovina, *in person,* March 2026

CyberSEE	Support Serbia organise regional workshop on online frauds under EMPACT policy cycle, Montenegro, *in person*, March 2026 (TBD)
CyberSEE	First training of the regional working group on seizing cryptocurrencies, Pristina/Podgorica (TBD), *in person,* March 2026
CyberSEE	Workshop with Albanian working group on the amendments to the existing legislation, Albania, *in person*, March 2026
CyberSEE	Domestic workshop to assess legislative progress in Albania, *in person,* March 2026
CyberSPEX	2nd Regional Meeting Scandinavian and Baltic Countries: Support the establishment and training of authorities to be declared under Articles 6.6, 7.5, 8.10, 14.7, and 14.10b of the Second Protocol, *in person*, March 2026 (TBD)
CyberSPEX	Thematic consultations with all EU m/s, *online*, March 2026 (TBD)
CyberSPEX	2nd Regional Meeting Mediterranean countries in cooperation with the EU Presidency of Cyprus: Support the establishment and training of authorities to be declared under Articles 6.6, 7.5, 8.10, 14.7, and 14.10b of the Second Protocol, *in person*, March 2026 (TBD)
CyberEast+	Review of reporting systems – Armenia: one or two advisory missions (TBD), *in person*, 01-31 March 2026
GLACY-e	Support to the Asia South Pacific Cybercrime Operation Meeting and Cyber Drill (ASPJOC), Asia-Pacific, *in person*, 03-05 March 2026
CyberEast+	Elections exercise with Expertise France, Armenia, *in person*, 16-20 March 2026
GLACY-e	Handbook on implementation of cybercrime laws: Second in person meeting of the Drafting Subcommittee, Vanuatu, *in person*, 17-19 March 2026
GLACY-e; CyberSEE; CyberSouth+	Applied Forensics Techniques for Crimes Against Children (CAC) Investigators workshop, Sweden *in person*, 23-24 March 2026
GLACY-e	Support on legislation: data protection - series of consultation workshops (private sector), Fiji, *in person*, 23-27 March 2026
CyberEast+	National discussions on responsible reporting and cyberviolence: civil society, ISP and academia forum, Ukraine, *in person*, 24-25 March 2026
GLACY-e; CyberSEE; CyberSouth+	Digital Forensics Research Conference Europe, Sweden *in person*, 24-27 March 2026
GLACY-e	Advice on strengthening cyber training strategies, Peru, *online*, by end of March 2026
GLACY-e	CyberGames x DSC 2026 - Online Stage, global, *online*, by end of March 2026
GLACY-e	Darknet and Crypto for Criminal Justice Authorities (pilot 2), LATAM, *in person*, by end of March 2026

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 – 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

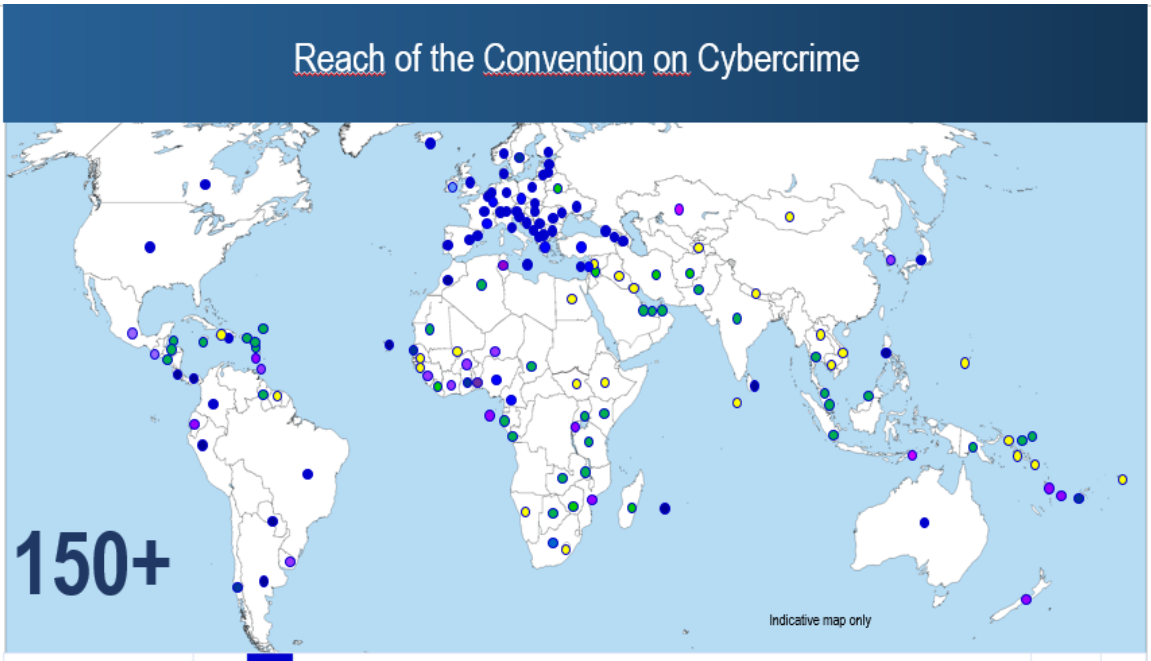
Duration: September 2023 – March 2026

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*



Parties:	81				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	40+	
Invited to accede:	16		Further States drawing on Budapest Convention for legislation:	20+	
=	99		=	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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE