COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2026)11

4 May 2026

Council of Europe Programme Office on Cybercrime in Bucharest: Activity Report for 2025

Contents

Executive summary

The Council of Europe Programme Office on Cybercrime (hereinafter: "the Office")[1] in Bucharest, Romania, is responsible for the implementation of global capacity building projects on cybercrime and electronic evidence ("e-evidence") on the basis of the Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185). The Office became operational in 2014, following a decision of the Committee of Ministers in 2013. That decision also included a request for the Secretary General to present an activity report to the Committee of Ministers on an annual basis.

In 2025, the Office consolidated its position as a cornerstone for global capacity building, legislative alignment, and stakeholder co-ordination in the fight against cybercrime. Through seven ongoing international projects, the Office delivered 294 activities, reaching criminal justice agencies throughout the world.

This extensive engagement led to a significant increase in the number of investigators, prosecutors and judges who are now better trained and equipped to handle cybercrime and electronic evidence. As a result, the rule of law and the effectiveness of criminal justice responses have been directly strengthened in numerous member states and partner countries.

Since its creation, the Office has supported around 2 700 activities, benefiting some 140 countries. By December 2025, it had 47 staff, including staff in other Council of Europe Offices, notably in Kyiv and Pristina.

The capacity-building projects supported the efforts at national, regional and international levels, in line with the Council of Europe's Reykjavík Declaration, by extending the Organisation's standards and good practice well beyond Europe.

The Office's work also produced direct legislative impact: by December 2025, 134 states had updated their domestic legislation to criminalise offenses against and by means of computers in line with the Council of Europe Convention on Cybercrime (Budapest Convention), compared to just 70 states in 2013.

The number of states participating in the Council of Europe Convention on Cybercrime (Budapest Convention) framework continues to be on the rise, with 97 states being either Parties (81), signatories (2), or invited to accede (14) as of January 2026 − almost doubling the participation since 2013.

1. For the period April 2014 to September 2015, see this report.
For the period October 2015 to September 2016, see this report.
For the period October 2016 to September 2017, see this report.
For the period October 2017 to September 2018, see this report.
For the period October 2018 to September 2019, see this report.
For the period October 2019 to September 2020, see this report.
For the period October 2020 to September 2021, see this report.
For the period October 2021 to December 2022, see this report.
For the period January to December 2023, see this report.
For the period January to December 2024 see this report.

The Office also facilitated the signature process for the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) on enhanced co-operation and disclosure of electronic evidence, which by January 2026 had been signed by 52 states (including two ratifications), underscoring the Office's key role in ensuring legal frameworks are up to date in light of technological advancements.

The Office notably expanded its thematic coverage of capacity building by new topics addressed in 2025 on the protection of children online, measures against the non-consensual dissemination of intimate images, the interplay of virtual assets and cybercrime, as well as the implications of artificial intelligence for criminal justice work.

A distinct achievement of 2025 included the Office work with training academies to ensure the scalability of newly acquired skills by embedding cybercrime and electronic evidence investigation modules into national training programs for investigators, prosecutors and judges.

Crucially, the Office grew partnerships and synergies with other international and regional organisations such as the Pacific Islands Law Officers Network (PILON), the Western Balkans Cyber Capacity Centre (WB3C), the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Union Agency for Law Enforcement Cooperation (Europol), the European Union Agency for Law Enforcement Training (CEPOL), the European Cybercrime Training and Education Group (ECTEG), the Global Forum for Cyber Expertise (GFCE), the Organization of American States (OAS), the United Nations Office on Drugs and Crime (UNODC), INTERPOL,[2] the Caribbean Community (CARICOM), the Organisation of Eastern Caribbean States (OECS), and the Organization for Security and Co-operation in Europe (OSCE), thereby maximising project impact and resource efficiency on a global scale.

The Office maintained and strengthened its central role in the "dynamic triad" of the Council of Europe Convention on Cybercrime (Budapest Convention), its Cybercrime Convention Committee and the Office itself, ensuring the Council of Europe's continued leadership and innovation in the field.

By expanding its global scope, adapting to new challenges and reinforcing collaboration with key stakeholders and international organisations, the Office demonstrated robust and innovative progress during 2025, laying a strong foundation for even greater impact in the coming years.

The Office continued to play an instrumental role in the work of Cybercrime Convention Committee, supporting the preparation of practical guidance for the Parties, co-funding and co-organising key plenary meetings and ensuring the effective operation of the critical 24/7 Network − an essential tool for international co-operation in cybercrime cases.

2. INTERPOL Global Complex for Innovation (IGCI) in Singapore is a partner of the Global Action on Cybercrime Enhanced (GLACY-e) project. Under a grant agreement, INTERPOL is responsible for the law enforcement component of this project.

To ensure that the Office remains a global leader in capacity building on cybercrime, the following key priorities emerge from its recent achievements and the evolving international context:

- Preserve and bolster its ability to operate on a national, regional and global scale, bringing Council of Europe standards to new jurisdictions and leveraging multilateral declarations such as the Reykjavík Declaration to extend influence well beyond Europe.

- Support more states in aligning domestic legislation on cybercrime and electronic evidence with the Council of Europe Convention on Cybercrime (Budapest Convention), aiming to further increase the number of states adopting and effectively implementing its provisions and related protocols**.**

- Accelerate the promotion, signature, ratification and practical implementation of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) by a wider group of states, facilitating cross-border access to electronic evidence in the dynamic, fast moving tech environment.

- Remain proactive by integrating emerging priority topics into training curricula and technical assistance – such as cyberviolence, disinformation, online child protection, misuse of virtual assets, artificial intelligence and election interference – to keep pace with the evolving digital crime landscape.

- Raise additional funds, mobilise voluntary contributions and ensure the operational and administrative sustainability of the Office, allowing it to launch new projects and scale activities as needed in response to global demand.

By pursuing these priorities, the Office can maintain its position at the forefront of the global response to cybercrime – driving standards, building capacity and strengthening international co-operation into the next decade and beyond.

1. Background and purpose of this report

The purpose of the present report is to inform the Committee of Ministers of the activities of the Council of Europe Programme Office on Cybercrime (hereinafter: “the Office”) in Bucharest, Romania, in 2025.

The Office became operational in April 2014 following an offer by the Government of Romania[3] and a decision by the Committee of Ministers in October 2013.[4] Its objective is to ensure the implementation of the capacity building projects on cybercrime of the Council of Europe in all regions of the world.

3. The Office is located at the UN House in Bucharest. Office space is allocated to the Council of Europe rent free by the Government of Romania under a Memorandum of Understanding.
4. Decisions CM/Del/Dec(2013)1180/10.4, 9 October 2013, at their 1180th meeting.

Taking stock of the experience of the Office over more than 11 years, growing accession to the Council of Europe Convention on Cybercrime (Budapest Convention), the synergies with the UN Convention against Cybercrime,[5] increasing demands for capacity building and new areas of impact (artificial intelligence, virtual assets, cyberviolence and disinformation), the present report also reflects on future priorities.

2. General context

The Office plays a critical role at a time of rapidly evolving cybercrime, the scale, sophistication and diversification of which consistently outpace national enforcement capabilities, exposing gaps in global responses. This highlights the necessity for technical assistance to help countries develop, implement, and enforce effective strategies, legislation, and operational skills on cybercrime and e-evidence.

Internationally, the adoption of the United Nations Convention against Cybercrime marks a watershed moment, where countries have acknowledged the need to harmonise global responses and strengthen co-operation in investigation and prosecution of crimes committed by means of information and communication technology systems.

In parallel, the Office remains instrumental in supporting the Council of Europe Convention on Cybercrime (Budapest Convention) the leading international standard in this field – and promoting the implementation of its Second Additional Protocol, which enhances cross-border access to e-evidence.

The Office's work at this intersection ensures both the practical skills and legal tools are in place to help states respond decisively to the challenges of digital crime and e-evidence in a complex and interconnected world.

Cybercrime landscape

Cybercrime represents one of the fastest growing and most complex categories of criminal activity, posing significant challenges for criminal justice authorities worldwide.

The offences committed are increasingly transnational, technologically sophisticated and highly adaptive, exploiting legal, technical, and jurisdictional gaps.

The most prevalent cybercrime threats include online fraud, social engineering, ransomware, cyber-enabled extortion and identity theft. These are done by a mixture of individuals and transnational criminal organisations. Phishing, business email compromise and investment scams remain among the most common and financially damaging offences, often relying on psychological manipulation rather than advanced technical skills. Ransomware attacks continue to target public institutions, healthcare providers and critical infrastructure, combining system encryption with data exfiltration to increase pressure on victims.

5. UN Doc. A/RES/79/243.

In parallel, stolen credentials and personal data are traded on illicit online markets, enabling further criminal activity. Emerging threats, including the criminal use of artificial intelligence, deepfakes and anonymisation technologies, are further complicating detection, attribution and evidence collection.

Effective responses to cybercrime require clear, harmonised and technology-neutral legal frameworks. Criminal justice authorities need legislation that adequately criminalises cyber-dependent and cyber-enabled offences, enables lawful access to electronic evidence and supports cross-border co-operation. Procedural laws must keep pace with technological change, addressing issues such as data retention, encryption, cloud-based evidence, and the role of private service providers. International alignment is particularly critical, as offenders routinely operate across multiple jurisdictions while investigations remain constrained by national legal boundaries.

Beyond legislation, criminal justice actors require sustained technical assistance and capacity development. This includes specialised training for investigators, prosecutors, and judges; access to modern digital forensic tools; and institutional mechanisms for co-operation with cybersecurity experts and the private sector. Strengthening operational capabilities and legal understanding is essential to close enforcement gaps, improve prosecution outcomes, and ensure that cybercrime responses respect due process and fundamental rights.

Council of Europe Convention on Cybercrime (Budapest Convention)

The Council of Europe Convention on Cybercrime (Budapest Convention) provides the first and most comprehensive international legal framework for harmonising cybercrime laws, improving investigative co-operation and enabling effective cross-border action against crimes committed via computer systems.

The Convention was a solid foundation for over 20 years of capacity building carried out by the Council of Europe, by offering guidance and a common legal model that helps states develop cybercrime legislation and international co-operation mechanisms beyond Europe.
The trend of accelerating interest in the Council of Europe Convention on Cybercrime (Budapest Convention) continued in 2025, when Rwanda, Sao Tome and Principe, Vanuatu and New Zealand became parties to the Convention, bringing the number of parties to 81. In addition, Seychelles, Malaysia, as well as Antigua and Barbuda, were invited to accede.

In addition, Malta ratified, and Rwanda acceded to the First Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) in 2025, showing the broader interest in the Convention’s framework.

These accessions – and requests for accession – were preceded by support from the Office, in particular in the reform of domestic legislation. As the Office prioritises assistance beyond legislation for countries that are parties or have been invited to accede, the number of countries requiring more extensive support keeps increasing.

In addition to capacity building, the increase in interest in the Council of Europe Convention on Cybercrime (Budapest Convention) since 2022 seems primarily due to two other factors:

- The opening for signature of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) (CETS No. 224) in May 2022.

- The United Nations Convention against Cybercrime adopted by the United Nations General Assembly on 24 December 2024.[6]

Second Additional Protocol to the Convention on Cybercrime

The Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) is aimed at strengthening international co-operation by enabling faster and more effective access to electronic evidence across borders which is crucial for investigating modern cybercrime. It also enhances support for countries by providing practical tools, safeguards for human rights, and clearer procedures that help states respond to cybercrime in a timely and co-ordinated manner. The innovative tools − those regarding direct co-operation with service providers in other parties and regarding co-operation in emergency situations in particular − are much needed by criminal justice practitioners.

The Protocol is synergetic with the European Union (EU) regulatory framework on e-evidence[7] by using aligned procedures for requesting and disclosing electronic evidence, so EU authorities can rely on the EU e-evidence framework within the EU while using the Protocol to co-operate efficiently with non-EU countries, ensuring consistency, speed and safeguards across jurisdictions.

By December 2025, this Protocol had been ratified by two states (Serbia, Japan) and signed by a further 50 states.[8] New signatories in 2025 were Latvia, Fiji, Norway, as well as Bosnia and Herzegovina. Five ratifications are needed for its entry into force.

6. The full title of this treaty as adopted by the United Nations General Assembly (UNGA) in December 2024 is “United Nations convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes”.
7. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and the Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.
8. Hungary and Costa Rica ratified the Second Additional Protocol on 5 February 2026 and 15 April 2026 respectively, bringing the number of ratifications to four. These ratifications did however not fall within the reporting period of the present Activity Report.

The Office supported the promotion and implementation of the Second Additional Protocol by providing technical assistance, legal guidance and capacity building activities − such as trainings, workshops and legislative support − to help countries understand the Protocol's mechanisms, align their domestic laws and apply its procedures effectively in practice.

The implementation and ratification of the Protocol will remain a priority for the Office in the coming years.

Cybercrime Convention Committee

The Cybercrime Convention Committee is aimed at ensuring the effective implementation and continued relevance of the Council of Europe Convention on Cybercrime (Budapest Convention) by guiding parties through policy development, assessments, co-operation mechanisms and engagement with key stakeholders.

In 2025, the Cybercrime Convention Committee continued to play a central role in steering the implementation of the Convention. Key achievements included the adoption, in June, of a Guidance Note on Article 26 on spontaneous information, as well as the launch of a questionnaire on cyberviolence to support updates to the Cyberviolence Resource.

The Cybercrime Convention Committee also advanced its analytical work by establishing a working group on artificial intelligence and commencing a mapping study on virtual assets and their relevance to the Convention.

In parallel, the Cybercrime Convention Committee strengthened international co-operation through meetings with industry and service providers.

The participation of numerous experts in the Cybercrime Convention Committee plenaries in June and November 2025 were funded by projects implemented by the Office.

The Office also ensures the functioning of the 24/7 Network (established according to Article 35 of the Council of Europe Convention on Cybercrime (Budapest Convention)) and organises the Network's annual meetings.

The Office will continue to support the Cybercrime Convention Committee in these endeavours. These topics will become important components of capacity building activities.

United Nations Convention against Cybercrime

The launching of the United Nations Convention against Cybercrime in October 2025 marked the culmination of the United Nations Ad Hoc Committee process, which held eight sessions between February 2022 and August 2024, alternating between New York and Vienna.

The launch reflected a shared commitment by states to strengthen international co-operation and harmonise responses to cybercrime at the global level. It also highlighted the importance of ensuring coherence with existing instruments and practices developed under established cybercrime frameworks.

The United Nations Convention reached 74 signatories by the end of 2025.

The Council of Europe contributed to this treaty process through the Cybercrime Convention Committee (in the form of briefing notes) and through the Office supporting the participation of subject-matter experts from Parties to the Convention and states invited to accede in each session. The aim was to ensure consistency of this additional treaty with the Council of Europe Convention on Cybercrime (Budapest Convention) and the inclusion of a minimum human rights and rule of law safeguards needed for international co-operation.

These results were achieved: the United Nations Convention against Cybercrime consists largely of provisions adapted from the Council of Europe Convention on Cybercrime (Budapest Convention), the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC).[9]

However, challenges remain regarding the effective implementation of its conditions and safeguards. For the next period it is essential that states implement the new United Nations Convention in a manner consistent with the Council of Europe Convention on Cybercrime (Budapest Convention), which can be achieved through joint capacity building activities involving the Council of Europe's Office and UNODC.

Partnerships relating to both Conventions may take the form of co-operation in supporting complementary implementation, investigative tools related to online child sexual exploitation and abuse, and capacity building with strong human rights and rule-of-law safeguards, while contributing expertise to the continued UN process.

3. Overview of projects and achievements in 2025

Projects

In 2025, the Office had six regional and global projects and one country-specific project (Ukraine) under implementation. By December 2025, the combined budgets of projects underway amounted to some EUR 40.8 million, over a multi-year period.

Project title	Duration	Budget	Funding
Octopus Project on supporting the implementation of the Convention on Cybercrime, its Protocols and related standards worldwide	Jan 2021 – Dec 2027	EUR 10 million	Voluntary contributions (Canada, France, Hungary, Iceland, Italy, Japan, Netherlands, Malta, UK and US[10]) [funding not fully secured]
GLACY-e project on Global Action on Cybercrime Enhanced	Aug 2023 – Dec 2028	EUR 13.25 million	EU/CoE joint project (including 10% CoE OB/JPP)

9. Regarding links between both conventions see: https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a
10. See also footnote 12.

CyberUA project on strengthening capacities on e-evidence of war crimes and gross human rights violations in Ukraine	Feb 2024 – Dec 2026	EUR 2 million	Voluntary contributions to the Ukraine Action Plan[11] and OBC [funding not fully secured]
CyberEast+ on enhanced action on cybercrime for cyber resilience in Eastern Partnership states	Mar 2024 – Feb 2027	EUR 3.89 million	EU/CoE joint project (including 10% CoE OB/JPP)
CyberSouth+ project on enhanced co-operation on cybercrime and e-evidence in the Southern Neighbourhood Region	Jan 2024 – Dec 2026	EUR 3.89 million	EU/CoE joint project (including 10% CoE OB/JPP)
CyberSEE project on enhanced action on cybercrime and e-evidence in South-East Europe and Türkiye	Jan 2024 – Jun 2027	EUR 5.55 million	EU/CoE joint project (including 10% CoE OB/JPP)
CyberSPEX project on enhanced co-operation on e-evidence by EU member states through the Second Additional Protocol to the Convention on Cybercrime	Mar 2024 – Dec 2026	EUR 2.23 million	EU/CoE joint project (including 10% CoE OB/JPP)

The projects implemented by the Office rely mainly on external funding, as described in the table above. Nonetheless the joint projects with the EU benefit from 10% co-funding from the Joint Programme Provision of the Ordinary Budget of the Council of Europe.

The EU remained the main donor through joint projects co-funded by the Council of Europe. The United States has made important funding available for the Octopus Project[12] in the past.

However, currently the continuation of the Octopus project, which is relevant also for the function of the Cybercrime Convention Committee, is not secured. Therefore, future efforts need to be made to raise additional funds for ensuring that the vital work done under the project will continue beyond 2026.

The Office also relies on the support of the Government of Romania which continues to provide rent-free office space.

In 2025, a significant development was made in respect of the continuation of the existing projects, as the GLACY-e project was extended for the period 2026-2028 with an additional budget of EUR 7.7 million. The CyberSPEX and CyberUA projects were extended on a no-cost basis until the end of 2026.

11. Council of Europe Action Plan for Ukraine "Resilience, Recovery and Reconstruction" (2023-2026).
12. Note: The Council of Europe was informed by the US authorities on 28 January 2025 that funding received from the United States was to be "paused". On 13 March 2025, the Council of Europe was then informed that the suspension had been lifted.

In addition, the preparation of the GlacyFOA project has commenced which is expected to be signed in the first quarter of 2026. This action is a joint initiative of the EU and Council of Europe aimed at addressing online fraud in West African countries.

Throughout the year, the Office supported − with some 47 staff − over 294 activities under these projects. A detailed inventory of all activities since 2014 is available online.

Achievements

Criminal justice capacities

In 2025, the Office contributed significantly to the strengthening of criminal justice capacities, in particular to the approximately 50 priority countries that were eligible for a broad range of assistance. Some 90 other countries participated in at least some of the activities.

Examples of specific activities and results under different projects include:

- Under the **CyberEast+** project on enhanced action on cybercrime for cyber resilience in Eastern Partnership states:

  Implementation of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) remained key for the project action in 2025, with a mix of in-country activities dealing with legal implementation and public-private co-operation aspects of the treaty, and the Regional Meeting addressing compliance with the EU requirements with regard to the Protocol.

  Training and capacity building action with law enforcement and judiciary was particularly varied in 2025, addressing themes of virtual currencies and Darknet investigations, ransomware investigations through national exercises, malware and network investigations, child abuse investigations with use of open-source intelligence, criminal disinformation, energy sector attacks and other areas. A highly technical annual Regional Cyber Exercise and follow-up bilateral exercise with Ukrainian partners ensured thematic focus on cyber interference with elections and disinformation operations.

  The project also worked in parallel on further improvement of mainstream cybercrime and e-evidence training programmes, in both regional and bilateral formats. Further training opportunities were explored via Regional Meeting on use of AI in investigations and forensics, as well as bilaterally with defence attorneys and Bar Associations.

  Interagency co-operation included a series of bilateral actions with countries, focusing on compatible tools and procedures in line with agreed Standard Operating Procedures, as well as inter-operability of reporting systems. Cross-border co-operation relied on joint activities with project partners and EU agencies, with the Second Additional Protocol and law enforcement co-operation in focus.

Civil society engagement and outreach was strengthened by continued annual support to European Dialogue on Internet Governance (EuroDIG) 2025 (regional level) and dedicated sessions on cyberviolence in the project's countries involving civil society actors.

The project supported 47 activities during this period.

- Under the **CyberUA** project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine:

  Long-term processes for improving of legislation and international co-operation on data and evidence of war crimes and gross human rights violations (in particular the implementation of the Council of Europe Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol) were the focus of continuous project support. Authorities remained closely engaged with the project on this work.

  The skilling of criminal justice authorities was improved through dedicated training sessions and practical exercises. The project covered both basic/introductory needs (admissibility, open-source intelligence, substantive law on aggression, evidence processing and introductory forensics) and far more technical and customised expertise (including virtual asset investigations, malware and live data forensics and cyberattack simulations) through activities organised in Ukraine and outside the country. The project involved close co-operation with prosecution and law enforcement training institutions on specialised training sessions.

  One of the practical contributions in which the project supported criminal justice in cases of war crimes/gross human rights violations is working with investigators, prosecutors and the judiciary of Ukraine to better understand and apply already existing international and domestic norms and possibilities. Additional outcomes of the project were the completed Report on Crime of Cyber Aggression and the preparation of the National Position on the applicability of international humanitarian law to cyberattacks. Both of these were achieved with close engagement from national partners.

  The project also continued its work with civil society and media (victims organisations, investigative journalists and other relevant groups) through teaching basic cybercrime/e-evidence/open-source intelligence courses. Cybersecurity experts, as well as private sector/critical infrastructure entities, were gathered for training and discussions on ways to ensure better access to and exchange of information and evidence concerning war crimes/gross human rights violations.

  In 2025, the project has reached close to 600 counterparts from Ukraine through 29 activities targeting all policy areas of the project.

- Under the **CyberSEE** project on enhanced action on cybercrime and e-evidence in South-East Europe and Türkiye:

Significant progress was achieved across the region in implementing the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention). Albania, Montenegro, North Macedonia and Serbia advanced legal reform processes with project support through high-level consultations, technical workshops, legislative assessments and tailored drafting recommendations.

In Bosnia and Herzegovina, initial institutional concerns were addressed through practitioner-led advocacy supported by the project, resulting in the country's signature of the Second Additional Protocol in November 2025.

Türkiye initiated amendments to its criminal legislation to introduce modern cybercrime and e-evidence provisions, supported by project engagement and recommendations aligned with the standards of Council of Europe Convention on Cybercrime (Budapest Convention).

In Serbia, the Cybercrime Strategy (2026-2030) and its first Action Plan (2026-2028) were finalised in September 2025 with CyberSEE support.

The capacities of criminal justice authorities were strengthened through structured training programmes developed with domestic training institutions, including cybercrime curricula, national trainer pools, Training of Trainers, certification schemes, and progressive training from basic to advanced levels for police and judiciary. Practical interventions focused on priority crime areas such as online child sexual exploitation and abuse and the illegal use of cryptocurrencies. Innovative formats, including Cyber Games, proved effective in enhancing operational skills and international co-operation.

The project supported law enforcement engagement within European and regional frameworks, notably the European Multidisciplinary Platform Against Criminal Threats (EMPACT), and strengthened operational co-operation with Europol, INTERPOL and Eurojust. Capacities were further enhanced in international co-operation, information exchange with cybersecurity institutions, and collaboration with the private sector through specialised workshops, templates and legal tools in line with the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention).

Interagency and public–private co-operation were reinforced through regional meetings, joint trainings, case-based exercises and multistakeholder forums, including the European Dialogue on Internet Governance (EuroDIG) and the South Eastern European Dialogue on Internet Governance (SEEDIG).

Major events such as the Underground Economy Conference and CYBERVAW Conference promoted global co-operation, survivor-centred approaches and shared responses to emerging cyber threats.

The project supported 80 activities during the reporting period.

- Under the **CyberSPEX** project on enhanced co-operation on e-evidence by EU member states through the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention):

  The project supported EU member states in the domestic implementation of the Second Additional Protocol through co-ordinated bilateral and regional actions. Key EU stakeholders, including the European Judicial Cybercrime Network, CEPOL and the SIRIUS Project, were engaged to ensure alignment and sustainability of future activities.

  Legal drafters and practitioners from all 27 EU member states enhanced their understanding of the Protocol and exchanged good practices through Regional Meetings covering the Baltic and Scandinavian, Central and Eastern European, Mediterranean and Western European regions. These meetings accelerated national implementation processes, leading to significant progress in Austria, Estonia, Hungary, Italy, Latvia, Slovenia and Sweden. Hungary became the first EU member state to promulgate its implementation and ratification law in December 2025.[13]

  All 27 EU member states were supported with comprehensive implementation materials, including a legal assessment template, an implementation guide, a manual on the interaction between the Protocol and EU instruments and templates for co-operation under Articles 6-9 developed under CyberSPEX. These resources are now used across all projects managed by the Office.

  Law enforcement practitioners were trained on international co-operation procedures through a dedicated seminar within CEPOL's "Cross-border Exchange of e-Evidence" course, delivered in co-operation with the European Judicial Training Network. Member states also exchanged experiences with other Parties through major international workshops and conferences organised with partners such as EUROJUST, GLACY-e and the CyberSEE.

  Targeted in-country workshops supported draft working groups in Finland, Slovenia and the Slovak Republic. CyberSPEX further encouraged non-signatory EU member states to join the Protocol, contributing to Latvia's signature in March 2025. Additional support was provided to Ireland where an in-person visit in November 2025 was led by the Council of Europe Director General of Human Rights and Rule of Law (DGI), accompanied by the Cybercrime Convention Committee Chair. The project is in dialogue with counterparts to support the internal process for modernising the interception law in Ireland as the remaining missing part prior to the ratification of the Council of Europe Convention on Cybercrime (Budapest Convention).

13. See also footnote 8.

EU member states gained a deeper understanding of public/private co-operation in criminal investigations and proceedings in a second workshop with service providers and industry organised by the Cybercrime Convention Committee and CyberSPEX.

Overall, the project supported 47 activities during the reporting period.

- Under the **CyberSouth+** project on enhanced co-operation on cybercrime and electronic evidence in the Southern Neighbourhood Region:

  Increased emphasis was placed on consolidating legislative dialogue, advancing specialised capacities and translating co-operation into operational outcomes across Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, Palestine*[14] and Tunisia.

  Legislative dialogue progressed through regional exchanges on international standards, including the Council of Europe Convention on Cybercrime (Budapest Convention) and the UN Convention and the former's First Additional Protocol. Morocco progressed with amendments to its Criminal Procedure Code, while other partner countries engaged in preparatory legislative reflection, including on emerging areas such as cyber-enabled violence and the implications of artificial intelligence.

  Judicial training was further strengthened through advanced modules, exchanges on national training manuals and a shift towards modular approaches. This included the adaptation of judicial training methodologies in Egypt, as well as the implementation of HELP courses and advanced judicial training in several countries. Law enforcement capacities were reinforced through increasingly specialised and practice-oriented training, including scenario-based courses and regional exercises. Priority areas included online child sexual exploitation and abuse, cyberviolence against women, cryptocurrency-related crime, ransomware and advanced digital forensics.

  Operational co-operation moved beyond training into practice, notably through regional cybercrime co-operation exercises, participation in the Cyber Games and joint activities involving law enforcement and cybersecurity actors, including the regional conference on crisis management in the event of cyber-attacks and the launch of the first joint MENA regional cybercrime operation under the INTERPOL framework. These efforts highlighted strong regional expertise, with practitioners from the region achieving leading results in competitive operational exercises.

14. * This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the member states on this issue.

Co-ordination with regional and international partners, including INTERPOL, Europol, Eurojust, DCAF and other EU-funded initiatives, remained central to implementation, while participation in major international fora supported inter-regional exchange and visibility of regional experience.

The project supported 44 activities during this period.

- In relation to the **Octopus Project**, which supports the implementation of the Council of Europe Convention on Cybercrime (Budapest Convention), its additional protocols and related standards worldwide:

  The Octopus Project serves as a key platform for bringing together parties to the Council of Europe Convention on Cybercrime (Budapest Convention) during Cybercrime Convention Committee meetings, enabling co-ordinated policy dialogue and exchange of best practices in combating cybercrime. By providing technical assistance and targeted capacity building, the project facilitates the accession of new countries to the Council of Europe Convention on Cybercrime (Budapest Convention), thereby reinforcing the Convention's global impact. Furthermore, the project supports the substantive work of the Cybercrime Convention Committee by promoting harmonised legislative frameworks, effective cross-border co-operation, and sustainable mechanisms for implementing the provisions of the Council of Europe Convention on Cybercrime (Budapest Convention).

  Significant progress was achieved in advancing global responses to cybercrime and promoting the effective use of e-evidence. Legislative reforms were supported and advanced in numerous countries, including the Seychelles, Kazakhstan, Malaysia, Benin, Sierra Leone, Fiji, Peru and Zambia, fostering greater alignment with the Council of Europe Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol.

  The project developed practical resources − such as a handbook to guide cybercrime legislative reforms in the Pacific − and provided expert-level support for countries engaging in policy reform and implementation of the Second Additional Protocol.

  Additionally, standards of the Council of Europe Convention on Cybercrime (Budapest Convention) were promoted jointly with the OSCE in Tajikistan and Kyrgyzstan, expanding the project's international reach.

  Capacity building was accelerated by providing targeted trainings to over 50 criminal justice and law enforcement practitioners from Grenada, Antigua and Barbuda, and across Southeast Asia, focused on investigation and prosecution of cybercrime, handling of e-evidence, and emerging areas such as ransomware and crypto-investigations.

  The Octopus Project also enhanced knowledge sharing through the maintenance and expanded use of the Cyberviolence resource, the Octopus Platform and the CYBOX online platform, facilitating the exchange of expertise and the development of e-learning materials for the global criminal justice community.

Participation in major events − including the Octopus Conference, the Europol Cybercrime Conference, and the 24/7 Network meeting − strengthened international co-operation, best practice sharing, and capacity building on priority topics such as artificial intelligence, cyberviolence and gender-based cybercrime.

Overall, the Octopus Project provided critical leadership in shaping both policy and practice in the global fight against cybercrime.

New voluntary contributions were received in 2025 from Malta, the Netherlands, the United Kingdom, Canada and Japan.

Through the **CYBERKOP**[15] action of the Octopus Project, the capacities of criminal justice authorities were strengthened through the development and delivery of a dedicated training programme on the Investigation of Cybercrimes for First Responders within the Kosovo*[16] Police, complimented by specialised Open-Source Intelligence training for investigators and prosecutors, basic cybercrime training, and participation in trainer certification programmes. These interventions contributed to more consistent investigative practices and increased availability of qualified national trainers.

The action also supported improvements in the legal and judicial framework by contributing to the drafting of the Law on Personal Data Protection for Law Enforcement Institutions and enhancing magistrates' capacity to handle cybercrime and e-evidence through targeted judicial training. International judicial co-operation was further reinforced through a study visit to the Council of Europe, including the European Court of Human Rights. The European case-handling workshop marked a regional milestone, demonstrating strengthened alignment with international standards, human rights safeguards and policy dialogue on data protection.

The project supported 65 activities during the reporting period.

- Under the **GLACY-e** project on Global Action on Cybercrime Enhanced:

  In 2025, three selected countries of the project (San Tome and Principe, Rwanda, and Vanuatu) became parties to the Council of Europe Convention on Cybercrime (Budapest Convention), while Fiji signed the Second Additional Protocol.

  Legislative reforms on cybercrime were actively supported in Benin, Dominican Republic, Ghana, Malawi, Malaysia, Mozambique, Nigeria and Uruguay alongside assistance for data protection reforms in Fiji and Mozambique.

  Argentina, Kenya and Malawi were onboarded as selected countries in the project.

15. The CyberKOP Action consists of a set of activities under the Octopus Project specifically for Kosovo*.
16. *All references to Kosovo, whether 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.

Capacity building efforts were comprehensive, with 75 professionals from 22 Asian countries enhancing their expertise in cyber incident response through "Operation Secure" to which the project contributed and the strengthening of competencies of national trainers and on expanding the pool of national trainers in Brazil, Colombia, Dominican Republic and Ghana. The mainstreaming of cybercrime training modules into Colombia's judicial academies was supported, and multiple workshops in Chile focused on developing training modules addressing artificial intelligence and cybercrime.

The project also contributed to the creation of Standard Operational Procedures in both Fiji and Sierra Leone, strengthening their ability to respond effectively to cybercrime threats. Importantly, 24/7 Points of Contact were enhanced in Benin, Côte d'Ivoire, and Cameroon, and a handbook on the implementation of cybercrime legislation began development through the PILON (Pacific Islands Law Officers Network) Subcommittee's first in-person meeting.

The project successfully co-organised the third edition of the African Forum on Cybercrime and Electronic Evidence, hosted by the Kenyan Government. The event brought together more than 350 high-level audience of policymakers, criminal justice professionals and cybersecurity practitioners from across Africa.

Through regional meetings and targeted training, the project strengthened collaboration and learning among hub countries, including at flagship events such as the Octopus Conference. Specialised exercises improved co-operation on cybercrime and electronic evidence among the Pacific Island states, while advanced online training on child sexual exploitation facilitated peer learning between GLACY-e countries and partners from South-East Europe and Türkiye. The project supported the seventh annual Victim Identification Task Force operation in Asia, the largest ever, led to the identification and prioritisation of cases involving 136 children and 70 suspects from over 33 000 images and videos, enabling investigative action across several jurisdictions.

In addition, hub countries and other selected countries were supported to attend a number of international and regional events: the International Conference on Combating Cyberviolence Against Women (CYBERVAW), the 2025 Digital Forensics Conference, the Eurojust/Council of Europe co-organised workshop on the Second Additional Protocol, the 2025 Underground Economy Conference, the annual meeting of the 24/7 Points of Contact Network, as well as the Europol Conference. Monitoring meetings with representatives of eight hub countries led to the identification of further capacity building on cybercrime at regional and domestic level.

The project supported 89 activities during the reporting period.

Capacity building initiatives

Through its various projects, the Office launched numerous impactful initiatives in 2025 in the fields of online child sexual exploitation and abuse, cyberviolence, artificial intelligence and election interference.

Online Child Sexual Exploitation and Abuse: A multi-regional approach was adopted to build capabilities against child exploitation online. Law enforcement representatives in Algeria, Morocco, and Egypt received dedicated training on investigating online child sexual exploitation and abuse cases, including advanced workshops and the integration of specialised forensic methodologies.

The "Advanced cybercrime training on online child sexual exploitation and abuse investigations and open-source intelligence for the EaP countries" further reinforced knowledge sharing and practical skills in Eastern Partnership states.

Plans for expanded basic and advanced online child sexual exploitation and abuse judicial training courses and manuals were mapped out for future action, ensuring sustainable and scalable impact.

Cyberviolence: The Office prioritised combating cyberviolence with a strong gender perspective. The International Conference on Combating Cyberviolence Against Women (CYBERVAW) established action-oriented follow-up and legislative advancement.

Evidence-based resources, such as the Cyberviolence Resource and targeted regional activities across Southeast Asia and other regions, were developed and disseminated. The integration of work between the Budapest, Lanzarote and Istanbul Conventions fostered a comprehensive approach to gender-based cybercrime.

Thematic webinars, a planned study on non-consensual dissemination of intimate images, and collaborations with civil society organisations ensured broad engagement and knowledge dissemination.

Artificial intelligence (AI): Recognising the growing role of AI in criminal activity, the Office organised regional workshops to strengthen the use of AI in cybercrime investigations. These activities targeted law enforcement and judicial actors, offering training in AI-powered technical tools and addressing legislative and operational challenges presented by evolving threats. The Octopus Conference included specific sessions on impact of AI on cybercrime.

Election interference: In response to the threat of digital interference in democratic processes, regional and national technical exercises, specialised training, and policy discussions focusing specifically on cyber interference with elections were organised. These included simulated exercises for Ukrainian law enforcement and election officials.

The Cyber Games activity, which is an interactive format of capacity building, has proven to be highly relevant and impactful. This activity brought together practitioners from all regions in realistic, team-based exercises that strengthened operational skills in areas such as ransomware, digital forensics and cryptocurrency investigations, while reinforcing international co-operation and trust.

Together, these initiatives showcased a comprehensive, multi-level strategy in tackling complex threats in the cyber sphere while enhancing international collaboration, legal reform and operational training.

Partnerships and synergies

Partnerships with other organisations are an essential feature of capacity building by the Office. They help scale activities, thereby multiplying impact.

During 2025, the Office co-operated closely with a wide range of international and regional partners. This included the EU and specific EU agencies (Europol, Eurojust, CEPOL), INTERPOL, the OSCE, PILON, CARICOM, OECS and various United Nations entities, to strengthen policy alignment, operational co-operation and capacity building on cybercrime and electronic evidence.

Through joint conferences, trainings, operational exercises and multistakeholder consultations, these partnerships supported legislative reforms, implementation of the Council of Europe Convention on Cybercrime (Budapest Convention) and its additional protocols, and enhanced cross-border investigations. They covered many areas such as ransomware, cryptocurrencies, online child sexual exploitation and abuse, as well as cyberviolence. Furthermore, collaboration focused on aligning cybercrime action with human rights, rule of law, democracy, gender equality and internet governance standards. One example is the support provided to the first in-person meeting of the PILON sub-committee, which focused on drafting a handbook on the implementation of cybercrime legislation, bringing together experts to advance practical guidance aligned with the Council of Europe Convention on Cybercrime (Budapest Convention).

The Office received the Delegation of the European Union to Barbados and the Eastern Caribbean States, the OECS and CARICOM/CARIFORUM and representatives from the relevant institutions responsible for cybercrime and cybersecurity policies in Barbados, the Dominican Republic, Grenada, Guyana, Jamaica, Suriname, as well as Trinidad and Tobago. The meeting aimed at providing insights into effective responses to cybercrime.

The Office strengthened substantive co-operation with other sectors in the Council of Europe Secretariat to ensure coherent, rights-based and cross-sectoral responses to cybercrime and electronic evidence.

For example, it worked with the departments responsible for gender equality and violence prevention, notably in advancing responses to cyberviolence and technology-facilitated violence against women through initiatives. This was done through the CYBERVAW Conference, the Cyberviolence Resource, and contributions to survivor-centred and rights-based policy discussions.

Co-operation with child protection actors supported capacity building on investigating online child sexual exploitation and abuse, aligning cybercrime responses with Lanzarote Convention standards.

The Office also co-operated with Council of Europe field offices, particularly in North Africa, the Western Balkans and Eastern Europe, to deliver integrated capacity building activities and reinforce regional ownership.

Further collaboration with education and training actors supported sustainable judicial and law enforcement training strategies, including HELP course updates and mainstreaming cybercrime modules into national curricula.

In the area of internet governance, partnerships were strengthened through joint engagement with the European Dialogue on Internet Governance (EuroDIG) and the South Eastern European Dialogue on Internet Governance (SEEDIG), promoting multistakeholder dialogue, public-private co-operation, and alignment of digital policies with democratic values and EU frameworks.

4. Conclusions and looking ahead

Throughout the year, the Office continued to promote the Council of Europe's cybercrime standards and reinforced the Organisation's recognition as a global leader on cybercrime and electronic evidence. This was achieved by translating the Council of Europe Convention on Cybercrime (Budapest Convention) and its additional protocols into authoritative policy guidance, legislative reforms and practical co-operation mechanisms implemented worldwide through trusted multistakeholder partnerships.

The success of the Office is reinforced by its ability to convene governments, international organisations, industry and civil society in trusted policy fora − such as the Cybercrime Convention Committee, the Octopus Conference and thematic working groups − where emerging challenges are translated into coherent, rights-based and operationally viable policy responses across regions.

Over the past 11 years, through the delivery of around 2 700 activities, the Office has produced important results, outcomes and impact. This includes increased interest in and accession to the Council of Europe Convention on Cybercrime (Budapest Convention),[17] alignment of the domestic legislation of states worldwide with its standards[18] and the strengthening of the capacities of criminal justice practitioners, as well as supporting the negotiation and subsequent implementation of the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention).

The main factors of success were:

- The Office's relationship within a dynamic triad of: (a) the legislative framework of the Council of Europe Convention on Cybercrime (Budapest Convention); (b) the work of the Cybercrime Convention Committee; and (c) the individual capacity building projects.

- The Office serves countries and stakeholders in all regions of the world.

17. In 2013, 53 states were parties (41) or had signed it (two) or had been invited to accede (ten). By the end of 2025, 97 states were parties (81) or had signed it (two) or had been invited to accede (14).
18. For example, 70 states had in 2013 offences defined in their criminal law similar to those of the Convention on Cybercrime; only six of those were from Africa. By the end of 2025, 134 states have achieved this, including 34 African states.

- The relevance of its work and its reputation built on quality and timely support to countries with impact at the strategic, policy and operational levels.

- The ability to adapt and to formulate tailored support that responds to changing needs, including the threats posed by the evolution of technology, the Russian war of aggression against Ukraine, the rise in ransomware attacks, threats to freedom of expression, cyberviolence, online fraud and other emerging cyber threats.

The priorities for 2026 and beyond include:

- Maintaining and further strengthening the dynamic triad of the Council of Europe Convention on Cybercrime (Budapest Convention, with its additional protocols), the Cybercrime Convention Committee and the Office.

- Raising funds to ensure the continuation of the Octopus Project, which is essential for advancing global co-operation, supporting new accessions and strengthening the operational effectiveness of the Council of Europe Convention on Cybercrime (Budapest Convention).

- Ensuring the Office continues to operate at a global scale, thereby facilitating the reach of other Council of Europe standards beyond Europe − in line with the Reykjavík Declaration − e.g. in the areas of AI, data protection or the protection of children.

- Expanding capacity building activities on: (a) online child protection and the non-consensual dissemination of intimate images; (b) virtual assets in relation to cybercrime and electronic evidence; and (c) AI.

- Expanding partnerships and synergies with other organisations to scale the reach and impact of projects and activities.

- Promoting the implementation and ratification of the Second Additional Protocol on electronic evidence, given that this Protocol is crucial for the continued relevance of the framework of the Council of Europe Convention on Cybercrime (Budapest Convention).

- Engaging constructively with the new United Nations Convention against Cybercrime, including through co-operation with the UNODC to promote alignment between the two conventions and ensure a strong emphasis on conditions and safeguards.

- Expanding the Office action through new regions and by initiating new projects and mobilising additional resources.

Building on more than a decade of achievements and impact, the Office is well positioned to consolidate and expand its role as the Council of Europe’s global engine for translating cybercrime standards into effective, rights-based responses, ensuring the continued relevance of the Council of Europe Convention on Cybercrime (Budapest Convention) framework and strengthening human rights, democracy and the rule of law in the worldwide fight against cybercrime.

5. Table of Abbreviations

Abbreviation	Full Name
AI	Artificial Intelligence
CARICOM	Caribbean Community
CEPOL	European Union Agency for Law Enforcement Training
DCAF	Geneva Centre for the Democratic Control of Armed Forces
ECTEG	European Cybercrime Training and Education Group
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
EuroDIG	European Dialogue on Internet Governance
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
GFCE	Global Forum for Cyber Expertise
INTERPOL	International Criminal Police Organisation
OAS	Organisation of American States
OECS	Organisation of Eastern Caribbean States
OSCE	Organization for Security and Co-operation in Europe
PILON	Pacific Islands Law Officers Network
SEEDIG	South Eastern European Dialogue on Internet Governance
T-CY	Cybercrime Convention Committee
UNCAC	United Nations Convention against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime
WB3C	Western Balkans Cyber Capacity Centre