COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2025)11

29 April 2025

Council of Europe Office on Cybercrime in Bucharest:

C-PROC Activity Report for 2024

Contents

Executive summary

The Council of Europe Programme Office on Cybercrime (hereinafter “C-PROC” or the “Office”) in Bucharest, Romania, is responsible for the implementation of capacity-building projects on cybercrime and electronic evidence (“e-evidence”) on the basis of the Convention on Cybercrime and in all regions of the world. The Office became operational in 2014 following a decision of the Committee of Ministers in 2013. The present report serves to inform the Committee of Ministers of the activities of C-PROC in 2024.

In 2024, the Council of Europe through C-PROC remained a global leader in the provision of capacity-building and legislative advice on cybercrime. Following the conclusion of several projects at the end of 2023, five new projects commenced between January and March 2024. The Office was thus responsible for the management of seven projects with a combined budget of over EUR 34 million and supported over 310 activities in all regions of the world throughout the year. In the eleven years since its creation, C-PROC has supported over 2400 activities benefiting some 140 countries. Between 2013 and 2024, the number of states with substantive criminal law in line with the Convention on Cybercrime increased from 70 to 132. Capacity building by C-PROC has also been a major factor in the growing reach of and accession to this Convention (increase from 41 parties in 2013 to 77 by the end of 2024). The work of C-PROC is essential for successful global outreach of the Council of Europe.

By December 2024, C-PROC had 54 staff, including – for the first time – staff in other Council of Europe offices, notably Kyiv and Pristina.

The European Union remained the main donor through its contributions to five joint projects. France, Japan, the United Kingdom and the United States provided voluntary contributions to the Octopus Project, while some Council of Europe member states – via the Action Plan for Ukraine – contributed to capacity-building on e-evidence of war crimes in Ukraine.

Numerous audit, evaluation and similar exercises, including an audit conducted by the Directorate of Internal Oversight on C-PROC in 2024, have confirmed its risk management and internal controls, as well as its compliance with contractual obligations towards donors.

Important developments in 2024 of relevance to C-PROC included:

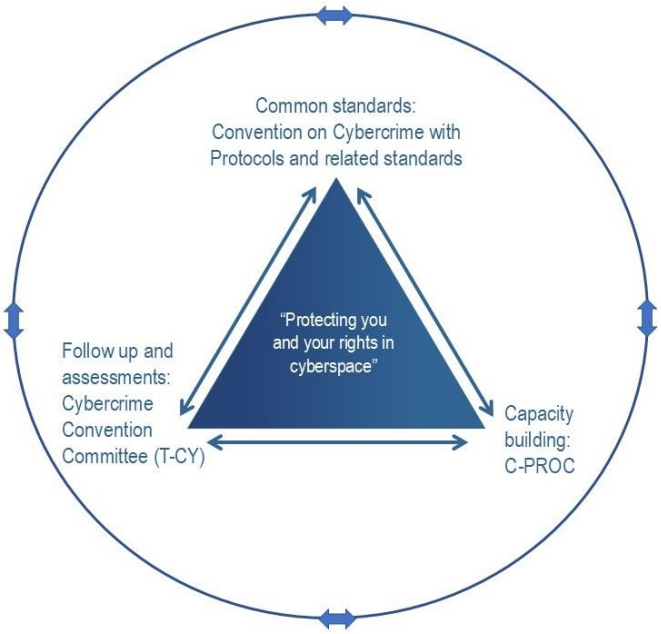
- Increasing interest in accession to the Convention on Cybercrime. In 2024, Benin, Côte d’Ivoire, Ecuador, Fiji, Grenada, Kiribati, Sierra Leone and Tunisia became Parties to the Convention, bringing the overall number of Parties to 77. In addition, Kenya, Malawi, Mozambique and Papua New Guinea were invited to accede. Growing membership to the Convention and the need to address new challenges (related to artificial intelligence, ransomware, virtual assets and others) significantly increases demands for capacity-building.

- Legal reforms to implement the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence commenced in a number of Parties in 2024: this Protocol is not only critical for fostering the rule of law in cyberspace but also for the continued relevance of the Convention on Cybercrime. Support to its implementation and ratification will be a priority for C-PROC.

- The adoption by the United Nations General Assembly of an additional international treaty against cybercrime in December 2024: the Council of Europe – through C-PROC and the Cybercrime Convention Committee - supported the negotiations of this treaty between 2022 and 2024. While largely consistent with the Convention on Cybercrime, and while the latter will remain the most relevant international framework in the foreseeable future, this new treaty raises a number of questions also with respect to capacity-building and the role of C-PROC.

In order to prepare for the future and for the Council of Europe to remain a global leader in capacity-building on cybercrime, C-PROC will:

- build on the factors that have enabled its success between 2014 to 2024 (global scope of activities; fully reflecting the “dynamic triad” of common standards, assessments and capacity-building; a dedicated office with specialised staff; project development and fund raising; cost-effective and proper management of resources);



- adjust the substantive focus (support the implementation of the Second Additional Protocol as a matter of priority; assist countries in the implementation of the new United Nations treaty against cybercrime as appropriate; expand activities on online child protection and the non-consensual dissemination of intimate images; further address the use of virtual assets for criminal purposes; develop a systematic approach for capacity-building on cybercrime, e-evidence and artificial intelligence);

- enable the scaling up of activities (expanding partnership and synergies with other organisations; placing staff in other offices; further development of online tools and platforms).

Following up on the Reykjavík Declaration adopted by the 4th Summit of Heads of State and Government of the Council of Europe in May 2023 with respect to the external dimension, the experience of C-PROC may provide valuable experience when it comes to the outreach beyond Europe regarding other open conventions, notably the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, on the protection of personal data, and on the protection of children, to name some.

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 in Bucharest, Romania, in 2024 (hereinafter "C-PROC" or the "Office").[1]

The Office became operational in April 2014 following an offer by the Government of Romania[2] and a decision by the Committee of Ministers in October 2013.[3] 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.

The present report provides an overview of the activities for 2024, while taking stock of the experience of the Office over more than ten years, growing accession to the Convention on Cybercrime (Budapest Convention, ETS No. 185), increasing demands for capacity-building and relevant international developments.

2. Context: relevant developments in 2024

It is recalled that the Office is one element of a dynamic triad. Developments in 2024 regarding the common standards of the Convention on Cybercrime and its additional protocols, and the work of the Cybercrime Convention Committee (T-CY) may be influenced by, or have an impact on, C-PROC. The wider context in 2024 also included the preparation and adoption of an additional international treaty on cybercrime by the United Nations.

State of accession to the Convention on Cybercrime

The trend of accelerating interest in the Convention on Cybercrime continued in 2024 when Benin, Côte d'Ivoire, Ecuador, Fiji, Grenada, Kiribati, Sierra Leone and Tunisia became Parties to the Convention, bringing the number of Parties to 77. In addition, Kenya, Malawi, Mozambique and Papua New Guinea were invited to accede.

These accessions – and requests for accession – were preceded by support from C-PROC, in particular to the reform of domestic legislation. With the Office giving priority to assistance beyond legislation to countries that are Parties or have been invited to accede, the number of countries requiring more extensive support keeps increasing. Growing demands by an expanding number of countries bring challenges for C-PROC.

[1] The decision setting-up the Office requested the Secretary General to present such annual reports.
For the report covering 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.

[2] C-PROC 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.

[3] Decisions CM/Del/Dec(2013)1180/10.4, 9 October 2013, at their 1180th meeting.

In addition to capacity-building, the increase in interest in this Convention since 2022 seems primarily due to two other factors:

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

- The negotiation of an additional international convention, that is, the United Nations treaty against cybercrime between February 2022 and August 2024 followed by its adoption by the United Nations General Assembly on 24 December 2024.[4]

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

The innovative tools of this Protocol – 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. With this Protocol, the framework of the Convention on Cybercrime remains highly relevant.

By December 2024, this Protocol had been ratified by two (Serbia, Japan) and signed by a further 46 States. Five ratifications are needed for its entry into force.

Support to its implementation and ratification will remain a priority for C-PROC in the coming years.

United Nations treaty process

The United Nations treaty against cybercrime was negotiated by an Ad Hoc Committee (AHC) which held eight sessions between February 2022 and August 2024, alternating between New York and Vienna. It involved detailed consideration of the Convention on Cybercrime and its two additional protocols on xenophobia and racism (ETS No. 189)[5] and on electronic evidence.

The Council of Europe contributed to this treaty process through the T-CY (in the form of briefing notes) and through C-PROC supporting the participation in each session of subject-matter experts from Parties to the Convention and states invited to accede. The aim was to ensure consistency of this additional treaty with the Convention on Cybercrime 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 treaty largely consists of provisions adapted from the Council of Europe Convention on Cybercrime and from the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC).[6]

As a positive consequence, states are now much more familiar with the Convention on Cybercrime of the Council of Europe.

---

[4] 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 co-operation 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”.

[5] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

[6] Regarding links between both conventions see:
https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a

At the same time, none of the advanced provisions of the Second Additional Protocol on electronic evidence have been included in the United Nations treaty. It is likely, therefore, that additional states will seek to join the Convention on Cybercrime in order to benefit from its Second Additional Protocol.

In the future, partnerships and synergies related to both conventions may take the form of co-operation between C-PROC and the United Nations Office on Drugs and Crime (UNODC) in capacity-building activities.

T-CY decisions on artificial intelligence and virtual assets

The 31st Plenary of the T-CY in December 2024 decided[7]:

- To commence work on virtual assets with a focus on the applicability of the tools of the Convention on Cybercrime and its Second Additional Protocol regarding the criminal use of virtual assets.

- To establish a T-CY working group on cybercrime, e-evidence and artificial intelligence (AI) and to task this group to prepare a mapping study with a focus on the applicability of the tools of the Convention on Cybercrime and its Second Additional Protocol in this respect.

C-PROC will support the T-CY in these endeavours, and these issues will become important components of capacity-building activities.

New capacity-building projects

The completion of several large projects by the end of 2023 entailed considerable risks to C-PROC in terms of a possible discontinuation of project activities and of staff contracts. The Octopus Project, which is funded by voluntary contributions, also faced a serious shortage of funds.

Although the preparation of new projects had been completed by autumn 2023, delays were encountered in the conclusion of financing agreements in early 2024.

However, between January and March 2024, the joint projects of the Council of Europe and the European Union - CyberEast+, CyberSouth+, CyberSEE and CyberSPEX - were launched.[8] Initial funding for the CyberUA project on e-evidence of war crimes in Ukraine had been identified under the Action Plan for Ukraine. In October 2024, the United States contributed more than EUR 2 million to the Octopus Project.[9] France, Japan and the United Kingdom also contributed to this project in 2024.

Therefore, C-PROC had substantial resources at its disposal in 2024. Disruptions caused by delays in contracting in the beginning of the year remained limited.

[7] https://rm.coe.int/t-cy-2024-12-plen31-rep-v5adopted/1680b2df6c

[8] The financing agreement for the GLACY-e project following up on GLACY+ had already been signed in mid-2023.

[9] Note: The Council of Europe was informed by the US authorities on 28 January 2025 that funding received from the USA was to be “paused”. On 13 March 2025, the Council of Europe was then informed that the suspension had been lifted.

Nevertheless, current funding levels are not sufficient to meet increasing demands. Moreover, funding for CyberUA and the Octopus Project have not been fully secured.

Developing new projects and resource mobilisation are ongoing tasks of C-PROC.

3. Overview of projects and achievements in 2024

Projects

In 2024, C-PROC had six regional and global projects and one country-specific project (Ukraine) under implementation.[10] By December 2024, the combined budgets of projects underway amounted to some EUR 34.6 million, although about EUR 5 million for CyberUA and the Octopus Project had not yet been secured:

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, UK and US[11]) [funding not fully secured]
GLACY-e project on Global Action on Cybercrime Enhanced	Aug 2023 – Jan 2026	EUR 5.55 million	EU/CoE joint project (including 10% CoE OB/JPP)
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2024	EUR 18.9 million	EU/CoE joint project (including 10% CoE OB)
CyberUA project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine	Feb 2024 – July 2026	EUR 3.5 million	Voluntary contributions to the Ukraine Action Plan[12] and OB [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 electronic 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 electronic 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 – Feb 2026	EUR 2.23 million	EU/CoE joint project (including 10% CoE OB/JPP)

[10] Excluding the GLACY+ project that ended in February 2024.

[11] See also footnote 10.

[12] Council of Europe Action Plan for Ukraine "Resilience, Recovery and Reconstruction" (2023-2026).

Between January and December 2024, C-PROC, with some 54 staff, supported over 310 activities under these projects. A detailed inventory of all activities since 2014 is available online.

The Office relies on external funding. The Octopus Project is funded by voluntary contributions; CyberUA by voluntary contributions and the ordinary budget under the Action Plan for Ukraine; whereas joint projects with the EU include 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. In 2024, the United States again made important funding available for the Octopus Project[13], to which Japan, France and the United Kingdom added contributions. Some member states of the Council of Europe contributed to the CyberUA project via funding to the Action Plan for Ukraine. The Office also relies on the support of the Government of Romania which continues to provide rent-free office space.

[13] See footnote 10.

Achievements

Criminal justice capacities

In 2024, C-PROC contributed significantly to the strengthening of criminal justice capacities, in particular in the approximately 40 priority countries that were eligible for a broad range of assistance. Some 100 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:

  Further to project support, Georgia became the 44th state to sign the Second Additional Protocol to the Convention on Cybercrime in June 2024.

  Following an inception phase from May to July 2024, the project worked with project counterparts in Armenia, Republic of Moldova and Ukraine on implementation requirements of the Second Additional Protocol, as well as on ensuring compliance with the Convention on Cybercrime.

  Training and capacity-building action targeted skills of the judiciary (Republic of Moldova), parallel cybercrime and financial investigations (Armenia) and Ukraine-specific support on ransomware investigations, malware and network investigations, as well as the use of the Convention on Cybercrime in armed conflict (Ukraine). The project also developed a revised training course on international co-operation, delivered in Armenia and Republic of Moldova.

  In partnership with other projects of C-PROC, law enforcement officers of the region improved their skills via dedicated training at the Underground Economy Conference 2024, as well as on cryptocurrencies and child sexual abuse investigations.

  As the flagship event of the project in 2024, the joint regional cross-project "Cybercrime Co-operation Exercise" brought together 50 participants from 12 countries to investigate cyberattacks on critical infrastructure with a practical real-time scenario.

  The project engaged with civil society regionally (EuroDIG 2024) to address matters of co-operation with other sectors (data protection, AI, internet governance) in the context of action on cybercrime.

  The project also commenced work on national reports on cybercrime threats and challenges for each of the countries of the Eastern Partnership, in co-operation with civil society organisations.

  The project supported the participation of subject-matter experts in the meetings of the UN Ad Hoc Committee tasked to prepare an additional international treaty on cybercrime.

The project supported 26 activities during this period.

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

  Following its start in March 2024, the project (jointly with the CyberEast+ project) resumed its work with the authorities of Ukraine to complete the reform of legislation in compliance with the Convention on Cybercrime.

  A focus of the project was the building of capacities of law enforcement and prosecutors/judiciary for handling e-evidence of war crimes and GHRV.

  Training courses covered the admissibility, processing and chain of custody of e-evidence, preservation and production of data, cryptocurrency and darknet investigations, use of international co-operation tools, and law enforcement/CSIRT[14] co-operation (in co-operation with the CyberSEE project). A co-operation exercise with key counterparts in Kyiv taught skills of investigations and forensics in case of a simulated attack on critical infrastructure.

  The project engaged civil society and media organisations through training on cybercrime and e-evidence, and held a consultation forum with private sector entities under the lead of the National Security and Defence Council, contributing to improved reporting and exchange of intelligence on war crimes/GHRV.

  A conference on the exchange of e-evidence of war crimes and GHRV in Strasbourg brought together key national counterparts of the project, civil society representatives and international partners aimed at improving co-operation.

  The project also commenced work on an online resource on e-evidence and open-source intelligence (OSINT) of war crimes and GHRV, as well as on an assessment of hard- and software requirements by Ukrainian partners.

  The project supported 20 activities during this period.

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

  Criminal justice professionals enhanced their knowledge on judicial co-operation on cybercrime, on attribution and confiscation of cryptocurrencies, investigation of online child abuse, handling e-evidence and using advanced forensic tools at events organised in co-operation with other organisations.

[14] Computer Security Incident Response Team.

Further steps were taken to integrate modules on cybercrime and e-evidence into the curricula of police academies and judicial training institutions during regional workshops in Montenegro and Türkiye.

Closer co-operation between law enforcement agencies and Computer Emergency Response Teams (CERTs) was supported by a regional workshop and an international exercise on real-time information exchange, both held in Albania.

Over 500 experts representing law enforcement agencies, the cybersecurity community, private industry professionals, financial services and academia from across the globe joined for exclusive workshops and case discussions during the Underground Economy Conference at the Council of Europe in Strasbourg with examples of international operations against botnets and ransomware groups.

Albania was supported to initiate legislative reforms for the ratification of the Second Additional Protocol to the Convention on Cybercrime.

The annual meeting of the 24/7 Points of Contact Network supported by CyberSEE and other C-PROC projects served as a platform for strengthening international and public/private co-operation under the Convention on Cybercrime.

The project supported the participation of subject-matter experts in the meetings of the UN Ad Hoc Committee tasked to prepare an additional international treaty on cybercrime.

The project supported 70 activities during this period.

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

  Following the launching event in June 2024, the domestic implementation processes of the Second Additional Protocol in the EU member states were supported through bilateral coordination efforts. EU stakeholders such as the European Judicial Cybercrime Network and the SIRIUS Project[15] were engaged to allow co-ordinated action for future activities.

  Over 140 participants from law enforcement, judiciary and legislators as well as EU agencies gained knowledge about the Protocol in a series of online workshops on procedures enhancing international co-operation between public authorities and direct co-operation mechanisms with service providers for the disclosure of computer data.

[15] SIRIUS (Support to Investigation and Prosecution in Europe of Serious Crime) is a project of EUROPOL and EUROJUST on cross-border access to electronic evidence.

All 27 EU member states were supported to assess the status quo of the implementation process and to identify necessary reforms by using a legal assessment template and an implementation guide designed under the CyberSPEX project.

Practitioners from law enforcement were introduced to the international co-operation procedures of the Protocol through a recorded webinar published on a platform of the EU Law Enforcement Training Agency (CEPOL).

Parallel implementation of the EU's e-evidence regulation[16] package and the Second Additional Protocol was promoted through several meetings and conferences, such as the SIRIUS Annual Conference.[17]

The sharing of experience within different regions was supported through meetings with contact points from Scandinavian and Baltic countries (Estonia, Finland, Latvia, Lithuania, Sweden) as well as those from the Mediterranean region (Cyprus, Greece, Italy, Malta, Portugal, Spain).

An exchange of knowledge on the alignment of domestic legislation was held with those countries that have commenced reforms of their legislation (Austria, Estonia France, Slovak Republic, Spain).

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

The project supported 19 activities during this period.

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

  Following a three-month inception phase, CyberSouth+ was officially launched in April 2024, bringing in three new partners – Egypt, Libya and Palestine[*] – that joined Algeria, Lebanon, Jordan, Morocco and Tunisia in common efforts to address cybercrime. In this connection, a visit to Egypt was carried out for meeting relevant counterparts and framing future co-operation.

  Tunisia became Party to the Convention on Cybercrime in 2024, and the dialogue with the Government and Parliament of Tunisia continued in view of aligning the domestic legislation of Tunisia with the requirements of this Convention and with international human rights standards, including with respect to the freedom of expression.

[16] Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings https://commission.europa.eu/law/cross-border-cases/judicial-co-operation/types-judicial-co-operation/e-evidence-cross-border-access-electronic-evidence_en

[17] SIRIUS | Eurojust | European Union Agency for Criminal Justice Cooperation

[*] 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.

Project partners benefitted from dedicated activities on the First Additional Protocol to the Convention on Cybercrime on the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Judicial capacities to address cybercrime were reinforced in Algeria, Libya, Jordan, Morocco, Palestine* and Tunisia, where cybercrime and e-evidence, training-of-trainers modules and workshops on legislation were jointly carried out with national judicial academies. An analysis and a dedicated workshop on training curricula on cybercrime adopted by these academies were conducted with all partners to assess the sustainability of national capacities to educate future magistrates.

The specialisation of law enforcement officials continued through both national and regional exercises on darknet and cryptocurrencies investigations, live data forensics, ransomware attacks and online child sexual exploitation and abuse (OCSEA), bringing together investigators from all eight partners.

The project supported inter-agency co-operation among cybercrime and cybersecurity actors in Tunisia. It also reinforced co-operation with AICTO,[18] INTERPOL and DCAF,[19] jointly carrying out national and regional activities.

The project supported criminal justice professionals from all eight partners to attend key international cybercrime workshops and events (such as the Underground Economy 2024, the annual meeting of the 24/7 Points of Contact Network and the EUROPOL Cybercrime Conference).

The project co-ordinated activities with the Council of Europe Offices in Tunis and Rabat, with the Council of Europe's Data Protection Unit and Children's Rights Division, as well as with other projects in the region of the European Union, Germany, the United Kingdom, the United States and UNODC.

The project supported 58 activities during this period.

- Under the **Octopus Project** on supporting the implementation of the Convention on Cybercrime, its additional protocols and related standards worldwide:

  Countries of Southeast Asia (Brunei, Cambodia, Indonesia, Laos, Malaysia, Singapore, Thailand, and Vietnam), Central Asia (Kazakhstan), Africa (Cameroon, The Gambia, Seychelles, Mauritania, Malawi) and Latin America (Guatemala) were supported in legislative reforms on cybercrime and e-evidence.

[18] Arab Information and Communication Technology Organisation (League of Arab States).

[19] Geneva Centre for Security Sector Governance (originally: Geneva Centre for the Democratic Control of Armed Forces).

Particular emphasis was put on ensuring the sustainability of judicial training including through the creation of a pool of national judicial trainers on cybercrime and e-evidence. Examples include support to Malaysia, Indonesia, Thailand, Mauritius, Brazil, but also regionally in the Pacific region and Southeast Asia. The project furthermore supported joint activities of the International Network of National Trainers (such as practitioner-to-practitioner webinars on OCSEA, cyberviolence, financial investigations, co-operation in emergency situations). It also contributed to further advance judicial training by engaging Spanish-speaking judges and prosecutors.

The authorities of Kazakhstan were supported in their participation in regional exercises (including on LEA/CSIRT co-operation, as well as law enforcement and judicial training strategies), but also through in-country training on financial investigations and ransomware.

The project assisted Grenada in becoming a Party to the Convention on Cybercrime and in meeting requirements for international co-operation under the treaty.

Globally, the project facilitated expert dialogues on enhanced international co-operation; detection, investigation and disruption of cybercrime; spontaneous information sharing, cybercrime trends and methods for law enforcement and cybersecurity industry to counteract criminal activities online; freedom of expression and public safety; cyberscams and other topics. This was complemented by engagement with parliamentarians in the Caribbean and African regions, the diplomatic community in Bucharest and exchange of views with service providers.

The Octopus Project continued to support the work of the T-CY, including in finalising the assessment of Article 19 of the Convention (“Search and seizure of stored computer data”).

The project supported the participation of subject-matter experts in the meetings of the UN Ad Hoc Committee tasked to prepare an additional international treaty on cybercrime.

A number of resources maintained by the project, such as the Cyberviolence Resource, HELP course on cybercrime, translations of the freedom of expression discussion paper and Octopus Platform served as important opportunities for criminal justice practitioners worldwide to increase their knowledge. Additionally, CYBOX, the new online platform for exchange, training, and resource sharing on cybercrime and e-evidence, was launched in 2024.

New voluntary contributions were received in 2024 from France, Japan, the United Kingdom and the United States.[20]

[20] See footnote 10.

Through the **CYBERKOP**[21] action of the Octopus Project, criminal justice professionals in Kosovo* enhanced their knowledge on judicial co-operation on cybercrime (including the drafting agreements on judicial co-operation in criminal matters; data preservation; spontaneous information; the relevant EU instruments for international co-operation; as well as the investigation of online child abuse, virtual assets and the use of forensics tools). Specialised support was provided to domestic working groups in drafting legislation, regulatory frameworks and standard operating procedures. Closer coordination between criminal justice practitioners, cybersecurity experts and the private sector was achieved during a domestic workshop on tackling cybersecurity threats. A workshop on cryptocurrencies enhanced the skills of financial intelligence experts, law enforcement officers, prosecutors and the Central Bank to prevent and control the criminal use of virtual assets.

The project supported 73 activities during this period.

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

  In 2024, six selected countries of the project (Benin, Côte d'Ivoire, Ecuador, Fiji, Kiribati and Sierra Leone became Parties to the Convention on Cybercrime, while four others (Mozambique, Malawi, Kenya and Papua New Guinea) were invited to accede. Additionally, Benin acceded to the First Additional Protocol to the Convention and Sierra Leone signed the Second Additional Protocol.

  The GLACY-e project supported additional countries in their reforms of cybercrime legislation, namely Guatemala, Lesotho, Mauritania, Malawi, Nigeria, Panama, Rwanda and The Gambia.

  In terms of capacities for judicial training, the project contributed to the strengthening of competencies of national trainers and on expanding the pool of national trainers in Brazil, Colombia, Mauritius and the Philippines. Furthermore, judicial training workshops and study visits were held for Fiji, Thailand, Costa Rica and Peru and a series of practitioner-to-practitioner workshops was organised within the framework of C-PROC's International Network of National Judicial Trainers.

  The project also focused on increasing the knowledge of the hub[22] and selected countries on financial investigations and cryptocurrencies, through a series of regional virtual assets trainings for African region and a dedicated on demand training course on cryptocurrencies for the hub countries of Latin America.

[21] The CyberKOP Action consists of a set of activities under the Octopus Project specifically for Kosovo*.
* 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.

[22] "Hub countries" are countries that are parties to the Convention on Cybercrime and with which C-PROC has had long-standing co-operation. These countries now serve as "hubs" to share their experience within their respective region.

Several regional and international thematic workshops and events were led by the GLACY-e project: the Digital Security Challenge 2024,[23] the regional prosecution and judicial training on cybercrime and e-evidence for the Pacific, the Regional workshop on the Second Additional Protocol for Latin America, a Eurojust/Council of Europe co-organised workshop on spontaneous information, and the plenary of the International Network of National Judicial Trainers.

The project supported the participation of subject-matter experts in the meetings of the UN Ad Hoc Committee tasked to prepare an additional international treaty on cybercrime.

In addition, priority countries and other selected countries were supported to attend a number of international and regional events: INTERPOL's Africa, Asia South Pacific and Americas Working Groups meetings on Cybercrime for Heads of Cybercrime Units; the INTERPOL Digital Piracy Workshop; the Underground Economy 2024; the annual meeting of the 24/7 Points of Contact Network; as well as the EUROPOL Conference.

The project supported 104 activities during this period.

Tools and resources

Numerous guides, platforms as well as other tools and resources were prepared or further developed in 2024, such as:

- The CYBOX online platform for exchange, training and resource sharing on cybercrime and e-evidence was launched with the Octopus Project in the lead. 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.

- Templates and a guide to facilitate the preparation of legislation and implementation of the Second Additional Protocol to the Convention on Cybercrime were prepared under the CyberSPEX project.

- A guidebook on how to draft and implement judicial training strategies was finalised with the contribution of all C-PROC projects.

- A resource on ransomware attacks was put online by the CyberSEE project. In 2024, the Council of Europe also became a member of the Counter Ransomware Initiative (CRI).

- The cyberviolence online resource was maintained by the Octopus Project.

[23] 47 participants from 21 countries sharpened their skills at the Digital Security Challenge, a unique capture-the-flag competition.

Partnerships and synergies

Partnerships and synergies with other organisations are an essential feature of capacity-building by C-PROC. They help scale up activities and multiply messaging and impact. During the year 2024:

- C-PROC co-operated and engaged in partnerships, among others, with the African Union Commission, the Community of Portuguese Language-speaking countries (CPLP), the Counter Ransomware Initiative (CRI), the European Commission, the EU Agency for Criminal Justice Co-operation (EUROJUST), the EU Agency for Law Enforcement Co-operation (EUROPOL), the EU Agency for Law Enforcement Training (CEPOL), the European Cybercrime Training and Education Group (ECTEG), the Economic Community of West African States (ECOWAS), the Forum of Presidents of Legislative Powers in Central America and the Caribbean (FOPREL), the Global Forum for Cyber Expertise (GFCE), the International Association of Prosecutors (IAP), INTERPOL[24], the League of Arab States, the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), the Pacific Islands Law Officers Network (PILON), the Parliamentarians for Global Action (PGA), the Southeast Europe Police Chiefs Association (SEPCA), the UNODC and the Western Balkans Cyber Capacity Centre (WB3C). Additionally, C-PROC co-operates with national authorities of various countries (such as the Australian Federal Police (AFP), the United States Department of Justice, the Government of Romania as the host country of C-PROC, and many others).

- A range of activities was conducted jointly with other capacity-building projects funded by the EU (CyberNet, EL PACCTO 2.0, SIRIUS project) that address cybercrime and e-evidence, or with the support of TAIEX,[25] in order to promote consistent international policies on capacity-building on cybercrime. C-PROC remains very well connected to large networks of experts and institutions in all regions of the world and is recognised as a key partner.

Synergies were created with other Council of Europe instruments and actions, for example:

- Capacity-building activities on data protection (in line with the Convention ETS No. 108[26], as amended by CETS No. 223[27]) or on the protection of children against sexual exploitation and sexual abuse (in line with the Lanzarote Convention[28]), the creation of the online resource on cyberviolence, or support to typology studies on money laundering.

[24] INTERPOL Global Complex for Innovation (IGCI) in Singapore is a partner of the GLACY+ project. Under a grant agreement, INTERPOL is responsible for the law enforcement component of this project.
[25] Technical Assistance and Information Exchange instrument of the European Commission (TAIEX), one example being the regional judicial training for the Pacific Chief Justices.
[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
[27] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).
[28] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

- The CyberSEE project, in partnership with the "End Online Child Sexual Exploitation and Abuse @Europe Plus project (EndOCSEA@Europe+)", organised a joint training for law enforcement, judges and prosecutors on preventing and combatting OCSEA in Montenegro.

- Side events on OCSEA were organised by the Octopus Project in co-operation with the Children Rights Division on the margins of the T-CY Plenary and the "Regional workshop on cybercrime, e-evidence and OCSEA in Southeast Asia".

- C-PROC also joined efforts with the North-South Centre of the Council of Europe in addressing racism and xenophobia online and co-ordinated all activities in the Southern Mediterranean and South East Europe with the field offices.

Support to the Cybercrime Convention Committee (T-CY)

The dynamic triad of common standards, follow up/assessments and capacity-building is the main factor in the global success of the framework of the Convention on Cybercrime. The following example illustrates the functioning of this triad in practice and the support of C-PROC to the T-CY in 2024:

In June 2024, the T-CY tasked its Bureau to commence work on a Guidance Note on Article 26 of the Convention ("Spontaneous information") and to invite Parties to respond to a questionnaire by the T-CY Secretariat and C-PROC.

In September 2024, C-PROC held an international event in The Hague, jointly with EUROJUST, on this topic.

In December 2024, the report with the findings of that event and of the replies to the questionnaire (jointly prepared by the T-CY Secretariat and C-PROC) was shared with the T-CY Plenary.

These findings will help the T-CY Bureau to prepare a draft Guidance Note by June 2025.

The C-PROC in 2024 also assisted the T-CY Bureau in preparing a draft questionnaire on the practices of Parties to the Convention regarding virtual assets and the relevance of the Convention on Cybercrime and its Second Additional Protocol in this respect. This questionnaire was adopted by the 31st Plenary of the T-CY in December 2024.

The participation of numerous experts in the T-CY Plenaries in June and December 2024 were funded by C-PROC projects.

Finally, C-PROC is also ensuring the functioning of the 24/7 Points of Contact Network (established according to Article 35 of the Convention on Cybercrime) and is organising the Network's annual meetings.

Gender mainstreaming in capacity-building on cybercrime and e-evidence

Cybercrime can affect women and men in different ways. Some commonly reported types of technology-facilitated gender-based violence include cyberbullying, sexual harassment, image-based abuse or threatening communications, but also online child sexual exploitation and abuse (OCSEA). Women and girls are particularly vulnerable to these crimes. At the same time, women have a crucial role to play in effective criminal justice responses to cybercrime - whether as policymakers or legislators developing and adopting legislation on cybercrime; or as criminal justice practitioners investigating, prosecuting or adjudicating cybercrime and related offences.

Therefore, C-PROC has developed several tools for supporting national authorities, including the cyberviolence resource maintained by the Octopus Project. This follows a mapping study on cyberviolence of the T-CY of 2017.

C-PROC projects promote synergies between different agreements of the Council of Europe, in particular the Convention on Cybercrime, the Istanbul Convention (CETS No. 210)[29] and the Lanzarote Convention (CETS No. 201) to address cyberviolence.

Interventions of C-PROC are also guided by the Gender Equality Strategy of the Council of Europe 2024-2029.

Examples of activities in 2024 include:

- A specialised training course on gendered aspects of cybercrime developed by the GLACY-e project in co-operation with experts of Ecuador. This serves as a pilot course with a view to further delivery in other countries and regions.

- A regional training course on cybercrime and e-evidence for women investigators and prosecutors in the Southern Mediterranean region organised by the CyberSouth+ project.

Experience underlines that C-PROC should:

- expand activities in countries worldwide to address cybercrime and cyberviolence, including gendered aspects of these crimes, such as non-consensual dissemination of intimate images (NCDII);

- promote the role of women in preventing, investigating and prosecuting cybercrime and related offences.

[29] Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210).

4. Conclusions and looking ahead

In the first ten years of its existence, from 2014 to 2024, through 18 projects and over 2400 activities benefitting some 140 countries, C-PROC has produced important results, outcomes and impact, including in terms of increased interest in and accession to the Convention on Cybercrime,[30] alignment of the domestic legislation of states worldwide with the standards of this Convention,[31] and the capacities of criminal justice practitioners. It engaged in partnerships and synergies with a wide range of institutions, adapted to new challenges (COVID, Russian war of aggression against Ukraine, rise in ransomware attacks, threats to freedom of expression, etc.). Moreover, C-PROC supported the negotiation of the Second Additional Protocol to the Convention on Cybercrime as well as its implementation once it had been adopted.

Through these activities, it has demonstrated how Council of Europe standards may be globalised. The experience of C-PROC – with the co-operation and trust it has established with the authorities of countries in all regions of the world and its mode of operation – is unique at the Council of Europe. The Council of Europe's action on cybercrime, including through C-PROC, can serve as a model and facilitate the outreach beyond Europe also with regard to other Council of Europe treaties.

The main factors of success were that:

- C-PROC represents the capacity-building element of a dynamic triad of: (a) the common standards of the Convention on Cybercrime with its Protocols as well as related standards; (b) follow up and assessments by the Cybercrime Convention Committee (T-CY); and (c) capacity-building by C-PROC. These three elements are within the responsibility of the Cybercrime Division.

- C-PROC serves countries in all regions of the world.

- Project development and fundraising are among the core responsibilities of C-PROC. Between 2014 and 2024, C-PROC prepared and implemented 18 projects with a combined budget of approximately EUR 86 million. In this connection, it mobilised some EUR 76 million in extra-budgetary resources.

- Cost-effective and proper management of resources is the foundation for trust by donors. Numerous audits, evaluation and similar types of exercise on C-PROC have confirmed its risk management and internal controls, as well as of it meeting contractual obligations towards donors. Office space is provided rent-free by the Government of Romania.

[30] In 2013, 53 States were Parties (41) or had signed it (2) or been invited to accede (10). By the end of 2024, 95 States were Parties (77) or had signed it (2) or been invited to accede (16).
[31] 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 2024, 132 states has achieved this, including 34 African states.

Through C-PROC, the Council of Europe will strive to remain a global leader in capacity-building on cybercrime and e-evidence to continue to make a meaningful contribution to human rights, democracy and the rule of law in cyberspace. This is to be achieved also in the future by:

- maintaining or further strengthening the dynamic triad of the Convention on Cybercrime with its additional protocols, the T-CY and C-PROC;
- keeping the global scope of C-PROC activities and thus facilitating the reach of other Council of Europe standards beyond Europe – in line with the Reykjavík Declaration – such as with regard to AI, data protection or the protection of children;
- expanding partnership and synergies with other organisations to scale up the reach and impact of projects and activities;
- supporting the implementation of the Second Additional Protocol on e-evidence as the priority for C-PROC, given that this Protocol is crucial for the continued relevance of the framework of the Convention on Cybercrime;
- 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 e-evidence; and (c) AI;
- engaging constructively with the new United Nations treaty against cybercrime, including through co-operation with UNODC;
- preparing additional projects and mobilising extra-budgetary resources;
- allocating the resources necessary for the management of the Office.

In 2024, C-PROC made again a significant contribution to the strengthening of legislation and criminal justice capacities on cybercrime and e-evidence worldwide in line with the Convention on Cybercrime and its additional protocols, as well as with human rights and rule of law requirements. This was achieved through over 310 activities under seven projects with a combined volume of over EUR 34 million.

Increased interest in and accession to the Convention on Cybercrime and alignment of the domestic legislation of countries worldwide with the provisions of this Convention is also a result of the activities of C-PROC since it became operational in 2014.

Co-operation between the Office and the T-CY was particularly strong in 2024, with C-PROC facilitating the T-CY's work on Article 26 ("Spontaneous information") of the Convention and on virtual assets, as well as organising the T-CY's exchange with industry (in addition to co-funding participants in T-CY Plenaries). This underlined again the value of the dynamic triad of common standards, follow up/assessments and capacity-building.

Project development and resource mobilisation remained an important feature of C-PROC. In 2024, five new projects were launched by the Office, all of them including support to the implementation of the Second Additional Protocol on e-evidence among their objectives. One of these projects is specifically focusing on e-evidence of war crimes in Ukraine (but remains to be fully funded).

An internal audit by the Directorate of Internal Oversight, completed in 2024, confirmed the results of numerous previous audits and evaluations, including the Office's risk management and internal controls, as well as of it meeting contractual obligations towards donors.

Between 2022 and 2024, C-PROC supported the participation of subject-matter experts from Parties and States invited to accede to the Convention in the United Nations treaty process. This helped ensure that the treaty against cybercrime adopted by the UN General Assembly in December 2024 is largely consistent with the Convention on Cybercrime and comprises a minimum of human rights safeguards.

C-PROC is set to remain a global leader in capacity-building on cybercrime also in the future. Substantial additional resources will be required to meet the growing demands by an expanding number of countries. The priorities for 2025 and beyond include support to:

- the implementation and ratification of the Second Additional Protocol on e-evidence;
- addressing challenges of AI in relation to cybercrime and e-evidence;
- addressing the use of virtual assets for criminal purposes;
- taking measures against online child sexual exploitation and abuse as well as the non-consensual dissemination of intimate images;
- extending the reach of Council of Europe standards on AI, data protection, the protection of children and others beyond Europe;
- the implementation of the new United Nations treaty against cybercrime in co-operation with UNODC, as appropriate.