COUNCIL OF EUROPE
1949 - 2024
CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2024)12

5 April 2024

Council of Europe Office on Cybercrime in Bucharest:

C-PROC activity report for 2023

Contents

Executive summary 3
1. Background and purpose of this report 5
2. Review: Ten years of C-PROC 5
Rationale 5
Projects, activities and impact 6
3. Overview of projects and achievements in 2023 10
Projects 10
Achievements 12
Criminal justice capacities 12
Studies and guides for practitioners 16
Online training platform on cybercrime and e-evidence 16
Resources on cybercrime legislation 16
4. C-PROC projects in 2024 18
5. Conclusions 19

Appendix: Inventory of C-PROC activities 2014-2023 (online)

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 (ETS No. 185) and in all regions of the world. The Office was established ten years ago following a decision of the Committee of Ministers in October 2013. The present report is to inform the Committee of Ministers of the activities of C-PROC in 2023.

In the ten years since its creation, C-PROC – through over 2 100 activities benefitting more than 130 countries – has made 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 human rights and rule of law requirements. Between 2013 and 2023, the number of states with substantive criminal law in line with this Convention increased from 70 to 131. Capacity building by C-PROC has been a major factor for the growing reach and membership of this Convention (increase from 41 parties in 2013 to 69 by the end of 2023).

The Office has attracted more than EUR 60 million in extra-budgetary resources; these have been properly managed as confirmed by audits and evaluations. In 2023, the European Union (EU) was the largest donor through joint projects, and the United States of America, the United Kingdom, Japan and others contributed funding to the Octopus Project. While relying on voluntary contributions, C-PROC has become a sustainable structure that should continue to operate in the same manner in the future.

In 2023, the Office, through six projects (with a cumulative budget of over EUR 49 million and some 40 staff), supported 305 activities in all regions of the world (including 102 training events for judges, prosecutors and investigators) culminating in the Octopus Conference in Bucharest, Romania, from 13 to 15 December.

During the period 2022-2023, C-PROC enabled the participation of experts from parties and states invited to accede to the Convention on Cybercrime in the United Nations Ad Hoc Committee tasked to elaborate a treaty on “the use of information and communication technologies for criminal purposes” (UN AHC) to ensure that such a future treaty – if adopted – is consistent with the Convention on Cybercrime and comprises at least a minimum of human rights and rule of law safeguards. This process, so far, resulted in increased interest in the Convention on Cybercrime as confirmed by numerous requests for accession since it began.

With or without an additional UN treaty, the Convention on Cybercrime with its Protocols and the Cybercrime Convention Committee (T-CY) will remain the most relevant international framework on cybercrime in the years to come, especially as it is backed up by the capacity building activities of C-PROC.

In December 2023, several C-PROC projects were completed which put a strain on available resources. However, five new projects have since been prepared with funding largely mobilised with a launch between January-March 2024. Additional voluntary contributions are nevertheless needed to meet increasing demands.

Priorities for 2024 include: supporting the implementation of the Second Additional Protocol to the Convention on Cybercrime (CETS No. 224), further strengthening capacities for the use of electronic evidence for the prosecution of war crimes in Ukraine, assisting countries – in particular those already invited to accede to the Convention on Cybercrime – to become parties while meeting human rights and rule of law requirements, and helping criminal justice authorities address challenges related to ransomware attacks and virtual currencies.

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 2023.[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.

Given that C-PROC has now been in operation for ten years, this report also comprises a summary review of its achievements.

2. Review: Ten years of C-PROC

Rationale

The Council of Europe began to support the implementation of the Convention on Cybercrime[4] through initial capacity building activities from 2002 and through dedicated projects, but with limited resources, from 2006 onwards.

In February 2013, the second meeting of the United Nations (UN) Intergovernmental Expert Group on Cybercrime concluded that capacity building was not only an effective way to address the challenge of cybercrime, but was also the one area that found broadest international agreement. It became clear that a more consistent approach by the international community was needed in this respect.

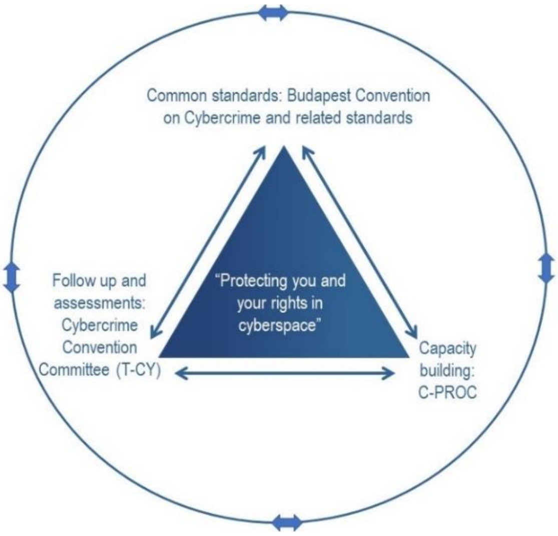
The decision of the Committee of Ministers in October 2013 to create a dedicated office tasked to support countries worldwide in the strengthening of their criminal justice capacities, in line with the Convention on Cybercrime and human rights and rule of law requirements, was the response of the Council of Europe. Following a proposal by the Government of Romania, C-PROC was established in Bucharest.

[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.

[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.

[4] The "Budapest" Convention on Cybercrime (ETS No. 185) is supplemented by the 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) of 2003, and the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) of 2022. Implementation of these Protocols is also supported by C-PROC.


Common standards: Budapest Convention on Cybercrime and related standards
"Protecting you and your rights in cyberspace"
Follow up and assessments: Cybercrime Convention Committee (T-CY)
Capacity building: C-PROC

The approach of the Council of Europe regarding cybercrime consists of the triad of: (a) common standards (Convention on Cybercrime, Protocols and related instruments); (b) follow up and assessments by the Cybercrime Convention Committee (T-CY); and (c) capacity building by C-PROC.

The concept of capacity building on cybercrime as formulated in 2013[5] has proven to be valid and continues to guide the work of C-PROC.

While C-PROC may enter into dialogue with and support any country or territory in the development of legislation in line with the Convention on Cybercrime, priority is given to those states that are parties or have requested accession or have been invited to accede to this treaty. C-PROC projects then support the respective governments and criminal justice institutions in the implementation of the Convention (and its Protocols).

Projects, activities and impact

In April 2014, the Office commenced activities by supporting countries through three projects with a combined budget of approximately EUR 8 million. By December 2023, C-PROC was managing projects with a combined budget of over EUR 49 million. Extra-budgetary resources amounting to approximately EUR 60 million have been mobilised over the past ten years.[6]

Between April 2014 and December 2023, C-PROC supported over 2 100 activities[7] benefitting more than 130 countries[8] in all regions of the world.

Projects typically assisted in the strengthening of:

- domestic legislation on cybercrime and e-evidence, as well as data protection or online child sexual exploitation and sexual abuse;
- strategies and policies on cybercrime, including raising awareness among policy makers;
- law enforcement capacities, including through standard operating procedures, tools for the seizure of cryptocurrencies and others;

[5] Council of Europe / Global Project on Cybercrime (2013): Capacity building on cybercrime, discussion paper (https://rm.coe.int/16802fa3e6).

[6] This amount does not include 10% co-funding by the Council of Europe to joint projects with the EU. Information on past and current projects is available here: Cybercrime Programme Office (C-PROC) - Cybercrime (coe.int).

[7] The full inventory of activities supported by C-PROC since April 2014 is available here: https://rm.coe.int/cproc-reps-inventory-activities-v38-29nov2023/1680ad9884.

[8] This number of "130 countries" includes detailed support to some 35 to 40 priority countries benefitting from the full range of capacity building activities over several years, and support to over 95 countries for in-country legislative reforms or participation of their criminal justice experts in multiple regional or international training and other activities. Not included in this number are experts from another 50 or so countries that only participated in a few activities. Only 12 out of 193 UN member states have not participated in C-PROC activities at all since 2014.

- judicial training on cybercrime and e-evidence;
- public/private co-operation, in particular between service providers and criminal justice authorities;
- co-operation between cybersecurity bodies (including computer emergency response teams) and criminal justice authorities;
- international co-operation, including by streamlining mutual assistance procedures, making available request templates and other tools and enhancing 24/7 points of contact.

Activities also contributed to the UN Agenda 2030 for Sustainable Development, in particular to Sustainable Development Goal 16 (“Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels”).

Projects and related activities delivered results and produced impact at multiple levels, starting with criminal justice officials who are more skilled and better equipped to meet the challenges of cybercrime and e-evidence. Developing capacities for sustainable training by judicial and law enforcement training academies has been a priority.

Successful investigations and prosecutions, including international operations, are being carried out all over the world. This is often a result of the legal framework coupled with the skills, tools and platforms for co-operation provided by C-PROC, in addition to relations of trust resulting from regional and international activities.

A marked increase in countries with domestic legislation on cybercrime and electronic evidence can be attributed to C-PROC. To illustrate this point, in 2013 some 70 states had adopted provisions on offences against and by means of computers in line with the Convention on Cybercrime, compared to some 130 states in December 2023.[9]

Capacity building by C-PROC has been a major factor for increased membership in the Convention on Cybercrime:

- By 2013, 41 states were parties, 2 states had signed it and 10 states had been invited to accede.
- By December 2023, 69 states were parties, 2 states had signed it and 20 states had been invited to accede.

C-PROC furthermore supported the T-CY. For example, the Octopus Project and other projects supported the participation of representatives of parties and of states invited to accede in meetings of the T-CY. The Octopus Project co-funded Spanish interpretation in T-CY plenaries.

[9] C-PROC has been closely following developments on cybercrime legislation worldwide since 2013 and publishes a yearly cursory overview of the “Global state of cybercrime legislation”: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2023-v4-public/1680adadf0.

In 2022 and 2023, C-PROC also facilitated the signature of the new Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence.[10] By December 2023, 43 states had signed this Protocol (of which two had also ratified it).[11]

C-PROC has been strengthening a criminal justice response to cybercrime that is not only effective, but also meets human rights and rule of law, including data protection, requirements. At the policy level, C-PROC has therefore contributed to a free, open and global cyberspace and to the multi-stakeholder model of internet governance.

Over the past ten years, C-PROC projects have had to adapt to new challenges. For example:

- In order to address the proliferation of ransomware attacks and related illicit financial flows via virtual currencies, from 2021 onwards C-PROC carried out domestic, regional and international training, workshops or practical simulation exercises for practitioners and developed guides on seizing cryptocurrencies and conducting criminal investigations of ransomware attacks. These complemented the Guidance Note on ransomware adopted by the T-CY.[12]

- Due to the covid-19 pandemic, C-PROC had to change the way it implemented activities from March 2020. Within a few weeks C-PROC was ready to carry out activities online. Numerous online resources, guides and other tools have since been developed or enhanced.[13] The E-learning HELP course on cybercrime and electronic evidence was launched[14], translated into 14 languages and more than 3 800 persons had enrolled by end-2023. The CYBOX platform for online training on cybercrime and e-evidence is about to become operational.[15]

- The onset of the full-scale aggression of the Russian Federation against Ukraine in February 2022 brought the question of electronic evidence related to war crimes and gross violations of human rights to the foreground. Under the CyberEast joint project with the European Union (EU), C-PROC prepared a gap analysis with respect to the collection and processing of such evidence; organised forensic training for investigators and prosecutors; trained judges on cybercrime and electronic evidence; and in 2023, designed a specific project – CyberUA – to help Ukraine address this challenge in a more comprehensive manner. This project was launched in early 2024.

[10] Including the conference for the opening for signatures in May 2022. https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.

[11] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.

[12] https://rm.coe.int/t-cy-2022-14-guidancenote-ransomware-v4adopted/1680a9355e.

[13] See for example, the resource on cyberviolence Cyberviolence - Cyberviolence (coe.int) or the resources available at the Octopus Community Home - Octopus Cybercrime Community (coe.int).

[14] See https://www.coe.int/en/web/cybercrime/-/council-of-europe-help-online-course-on-cybercrime-and-electronic-evidence.

[15] See https://www.coe.int/en/web/cybercrime/cybox.

- In an increasing number of countries, including in some parties to the Convention on Cybercrime or in states seeking accession to it, legislation on cybercrime includes provisions criminalising the “dissemination of false information”, “offensive messages”, “causing annoyance”, “spreading of rumours” and other conduct. In some instances, such provisions may restrict the freedom of expression beyond what is necessary and proportionate. C-PROC projects address this concern when providing advice on legislation. In December 2023, a discussion paper was produced to facilitate a more structured dialogue on this matter.[16]

- In 2022, the Convention on Cybercrime was supplemented by the Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). C-PROC promoted implementation of this Protocol in 2022 and 2023, and further support is now built into all new C-PROC projects.

- By adopting Resolution 74/247[17] in December 2019, the UN General Assembly (UNGA) established an Ad Hoc Committee (UN AHC) tasked “to elaborate comprehensive international convention on countering the use of information and communications technologies for criminal purposes”. The actual negotiations commenced on 28 February 2022 and were to be completed through six negotiating sessions by February 2024.[18] C-PROC supported the participation of experts from parties and states invited to accede to the Convention on Cybercrime in this treaty process so that the additional future treaty is consistent with the standards of the Convention on Cybercrime, as well as human rights and rule of law requirements. Experience during these negotiations, and the latest versions of the draft text of the UN convention, confirmed the necessity and value of this support.[19] Providing UN member states participating in this process with a better understanding of the benefits of the framework of the Convention on Cybercrime generated additional interest in it. Since the start of that process in February 2022, Cameroon, Côte d’Ivoire, Ecuador, Grenada, Kazakhstan, Kiribati, Korea, Mozambique, Rwanda, São Tomé and Príncipe, Sierra Leone, Timor Leste and Uruguay requested accession to the Convention on Cybercrime. Brazil, Cameroon and Nigeria also became parties to it.

In short, in the first ten years since its creation, C-PROC:

- has made a significant contribution to the strengthening of legislation and criminal justice capacities on cybercrime and electronic evidence in line with the Convention on Cybercrime and human rights and rule of law requirements worldwide; membership in this Convention increased considerably because of support by C-PROC;

[16] Cybercrime and freedom of expression: discussion paper - Cybercrime (coe.int).

[17] The Resolution had been proposed by the Russian Federation.

[18] https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.
N.B. In February 2024, the UN AHC decided to suspend the 7th session and continue it in July or August 2024 in order to reach agreement on a draft text of an additional convention. This extended session is yet to be confirmed.

[19] Note: for each session, the Bureau of the Cybercrime Convention Committee had also prepared briefing notes to facilitate co-ordination and common positions of the parties to the Convention.

- permitted global outreach, generated partnerships and synergies with numerous organisations and initiatives, and produced results and impact in all regions of the world;

- attracted considerable extra-budgetary funding from donors; and

- became a synonym for capacity building on cybercrime and electronic evidence.

Numerous audits and evaluations have confirmed that the Office is managed in a cost-effective manner, and that resources entrusted to the Council of Europe for it by donors are made use of in line with rules and procedures.

3. Overview of projects and achievements in 2023

The Octopus Conference on Co-operation on Cybercrime (Bucharest, Romania, 13-15 December 2023) was the culmination of another successful year of C-PROC in terms of outreach and impact worldwide. Over 500 experts from some 130 countries participated in this conference and the Deputy Secretary General of the Council of Europe made a keynote speech. Octopus 2023 served again as a catalyst for global co-operation on cybercrime and electronic evidence. In addition to plenary and workshop sessions, it included closing events for projects ending and launching events for new C-PROC projects. This conference was preceded by over 300 other activities in 2023.

Projects

In 2023, C-PROC had five regional and global projects under implementation and a sixth project (GLACY-e) was phased in from August 2023.

By December 2023, the combined budgets of projects underway amounted to some EUR 49.7 million, which represented a further increase compared to the previous year.[20]

However, from these six projects, four were completed or phased out by the end of 2023.

Between January and December 2023, C-PROC, with some 40 staff, supported approximately 305 activities under the following projects:

[20] September 2015: EUR 6 million, September 2016: EUR 22 million, September 2017: EUR 24.4 million, September 2018: EUR 26.7 million, September 2019: EUR 32.3 million, September 2020: EUR 38 million, September; 2021: EUR 38 million; December 2022: 39.2 million.

Project title	Duration	Budget	Funding
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2024	EUR 18.9 million	EU/CoE joint project (including Council of Europe 10% OB/JPP[21])
GLACY-e project on Global Action on Cybercrime Enhanced	Aug 2023 – Jan 2026	EUR 5.55 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
OCTOPUS Project	Jan 2021 – Dec 2027	EUR 10 million[22]	Voluntary contributions (Canada, Hungary, Iceland, Italy, Japan, Netherlands, UK and USA)
iPROCEEDS-2 project targeting proceeds from crime on the internet and securing electronic evidence in South-eastern Europe and Türkiye	Jan 2020 – Dec 2023	EUR 4.95 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberSouth on capacity building in the Southern Neighbourhood	July 2017 – Dec 2023	EUR 5 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)
CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region	June 2019 – Dec 2023	EUR 5.33 million	EU/CoE joint project (including Council of Europe 10% OB/JPP)

A detailed inventory of activities supported or carried out is available online.

The Office relies on external funding. The Octopus Project is fully funded by voluntary contributions, whereas joint projects with the EU include 10% co-funding from the Joint Programme Provision of the Ordinary Budget of the Council of Europe.

During the past year, more than 90% of its budget was funded by extra-budgetary resources, that is voluntary contributions and EU contributions to joint projects. The EU remained the main donor through joint projects co-funded by the Council of Europe. In 2023, the United States of America again made important funding available for the Octopus Project, to which the United Kingdom, Japan and Iceland added contributions. The Office also relies on the support of the Government of Romania, which continues to provide rent-free office space.

In the course of the past ten years, C-PROC was able to rely on an increasing level of resources that helped meet growing demands for support from an expanding number of countries committed to implementing the Convention on Cybercrime and its Protocols.

However, with the CyberSouth, CyberEast and iPROCEEDS-2 projects ending in December 2023, GLACY+ ending in February 2024 and the Octopus Project experiencing a shortage in funding, C-PROC is facing a dent in available resources in 2024. This may be a temporary challenge as several new projects are set to commence in early 2024 (see section 4 below).

[21] Joint Programme Provision of the Ordinary Budget of the Council of Europe (OB/JPP).
[22] Funding not fully secured yet.

Achievements

Criminal justice capacities

In 2023, C-PROC contributed significantly to the strengthening of criminal justice capacities, in particular in the 35-40 priority countries that were eligible for a broad range of assistance. Over 90 other countries participated in at least some of the activities.

Examples of specific activities are:

- **Octopus Project:** The project fostered international dialogue, co-operation and commitment through the organisation of regional and international initiatives, such as the Octopus Conference, the International Conference on co-operation in Africa, dedicated sessions on war crimes and e-evidence at the IGF 2023 in Kyoto and the World Forum for Democracy, as well as support to events such as Botnet and Malware Ecosystems Fighting Conference, Cyber Crime Conference in Rome, the RightsCon Summit, the Global Conference on Cyber Capacity Building in Ghana, the 2nd Cyber Affairs Summit Conference in Argentina, the Regional Workshop for the Parliamentarians in the Caribbean, the International Symposium on Cybercrime Response in South Korea, the East Africa Legislative Summit, or the EUROPOL Cybercrime Annual Conference.
  Particular emphasis was put on ensuring the sustainability of judicial training in Africa, but also internationally; enhancing skills and knowledge of Ibero-American and Portuguese-speaking cybercrime prosecutors; fostering public/private co-operation in Latin America; countering online child sexual exploitation and abuse; strengthening 24/7 points of contact network; supporting implementation of the Second Additional Protocol and implementing a dedicated stream of activities on online xenophobia and racism.
  The CYBERKOP action in Kosovo* was launched.
  Legislative assessments and advisory missions supported Barbados, Cameroon, Ghana, Kazakhstan, Malawi, Malaysia, Mauritania, Mexico and Seychelles, and provided further avenues for strengthening legal frameworks.
  A number of resources were made available, such as the Study on implementation of the First Additional Protocol to the Convention on Cybercrime on xenophobia and racism, a discussion paper on cybercrime and freedom of expression, the updated Cyberviolence resource and the CYBOX online training platform on cybercrime and electronic evidence.

  The Octopus Project supported the work of the T-CY and facilitated the co-ordination of positions and participation of experts from Africa, Asia-Pacific, the Caribbean and Latin America in the UN. AHC tasked to prepare a new cybercrime treaty.

  The project supported some 60 activities in 2023.

[23] * 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.

- **CyberEast**: Further to project support, Armenia became the 43rd state to sign the Second Additional Protocol to the Convention on Cybercrime in November 2023. The regional Report on Article 15 (safeguards and guarantees) has been updated to reflect the 2023 state of play for the Eastern Partnership region.

  The project focused on completing training sessions on cybercrime and electronic evidence at three levels (introductory, intermediate and advanced) for all project countries, all major target groups (law enforcement, prosecutors, judges), in co-operation with training institutions wherever possible, and engaging defense attorneys into capacity building for the first time in Georgia and the Republic of Moldova.

  Additionally, the project reinforced capacities of criminal justice authorities and interagency co-operation via a series of trainings on cyber incident and cybercrime taxonomy and handling, financial investigations, open-source intelligence and held two flagship co-operative Regional Cyber Exercises in Georgia and Romania.

  The project engaged with civil society both nationally (Republic of Moldova, Ukraine) and regionally (EuroDIG 2023) to address matters of oversight and accountability for cybercrime action. Joint regional cross-project initiatives included a Regional Exercise on joint investigative teams under the Second Additional Protocol, two regional discussions on parallel financial investigations and intelligence and co-operation between Computer Security Incident Response Teams (CSIRTs) and law enforcement as part of CyberWeek in the Republic of Moldova.

  Targeted support to Ukraine (in addition to their full engagement in regional activities) included a study on gaps and challenges concerning electronic evidence of war crimes and related offences, intermediate-level forensic training for law enforcement agencies, and dedicated judicial training for judges from Dnipro and Odesa regions.

  The project was completed in December 2023 with the adoption of a renewed Declaration on Strategic Priorities for Co-operation on Cybercrime in the Eastern Partnership Region.

  41 activities were supported by this project during this period.

- **iPROCEEDS-2**: Closer co-operation between criminal justice authorities and cybersecurity community was achieved through international scenario-based exercises, domestic workshops, conferences, seminars, trainings, meetings, regional simulations and joint symposiums, focused on the investigation of cyber-attacks, incident management and the promotion of international standards and regulations.

  Capacities of law enforcement agencies were enhanced through joint activities dedicated to the investigation of virtual currencies, OCSEA (online child sexual exploitation and abuse), financial investigations, access to specialised databases and new tools for co-operation.

  The Annual Meeting of the 24/7 Points of Contact served as a platform for sharing operational models and capacity building. Closer links between the public and private sector were achieved by supporting domestic meetings, with a focus on the co-operation between criminal justice authorities and service providers. The Underground Economy Conference offered opportunities for sharing the latest tools developed by the industry.

The expertise of judges and prosecutors to handle cybercrime cases was strengthened through sustainable training on e-evidence, international co-operation and the certification of training skills.
The project supported some 110 activities during this period.

- **CyberSouth**: the work on legislation and its compliance with Council of Europe standards continued with Tunisia in view of its accession to the Convention on Cybercrime, with Jordan and with Lebanon, including on data protection legislation. Judicial capacities to address cybercrime were reinforced in Algeria, Lebanon, Morocco and Tunisia, where training-of-trainers modules led to the establishment of pools of national trainers and national institutions integrated cybercrime programme into national curricula. Public-private partnership improved in all priority countries, including with multinational service providers, resulting in an increased number of international requests.
  Law enforcement work was supported by facilitating continuous education and practical exercises. International co-operation on cybercrime in the Middle Eastern and Northern African (MENA) and African regions was strengthened thanks to the international Conference organised in Bouznika (Morocco) with the participation of 34 countries. Co-ordination on cyber issues with the League of Arab States and contacts with the new partners were established in view of the next project phase, CyberSouth+.
  The project supported some 52 activities in this period.

- **GLACY+:** Legislative reforms and policy reviews were supported in Africa, Asia, Latin America and the Pacific on cybercrime and e-evidence (Cameroon, Dominican Republic, Malawi, Mexico, Mozambique, Nauru, Nepal, Nigeria, Rwanda, Timor Leste). Dedicated activities in the Dominican Republic, Ghana, Mexico, Peru and Uruguay enhanced dialogue between policymakers and practitioners.
  The advisory workshops on the search, seizure and confiscation of online crime proceeds implemented by the project partner INTERPOL in Benin, Colombia, Costa Rica, Dominican Republic, Senegal and Sri Lanka increased countries' knowledge on parallel financial investigations and some even generated on the spot freezing of illicit proceeds online.
  International co-operation was strengthened through a series of annual events focused on scenario-based exercises on data preservation, mutual legal assistance, parallel financial investigation, and other co-operative mechanisms for Africa and Latin America. The train the trainers for first responders course was deployed to some 74 future national trainers from Africa, Asia-Pacific and Latin America regions. These trainings generated a spin off training on electronic evidence for around 270 first responders in Chile, Dominican Republic, Paraguay and Peru, delivered by regional/national trainers.[24] 71 Spanish-speaking professionals[25] learned enhanced investigative skills, including a robust understanding of open-source investigation methodologies in a six-week online training course on Fundamentals of Open-Source Investigation.

[24] With some logistical support (catering) or no support at all from the project.
[25] From Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Paraguay, Peru and Uruguay.

GLACY+ further deepened its focus on judicial training through national training workshops in Chile, Côte d'Ivoire, Ghana, Kenya, Nigeria and Peru and a series of practitioner-to-practitioner workshops organised within the framework of C-PROC's International Network of National Judicial Trainers.

Several regional and international thematic workshops and events were led by the project: Meetings of the network of Ibero-American prosecutors specialised in cybercrime and the Forum of Portuguese-speaking prosecutors specialised in cybercrime[26], a Eurojust/Council of Europe co-branded workshop on international co-operation provisions of the Second Additional Protocol to the Convention on Cybercrime[27], the Regional CSIRT/LEA simulation exercise for interagency co-operation for selected African countries[28]; a regional workshop on public-private co-operation in Latin America[29], a regional meeting on judicial training strategies for selected African countries;[30] and the Plenary International Network of National Judicial Trainers[31].

In addition, priority countries and selected other countries were supported by the project to attend a number of international and regional events: the International Conference on cybercrime and e-evidence in Africa; the Regional training on Joint Investigative Teams and improved co-operation with foreign service providers under the Second Additional Protocol; the International Conference on xenophobia and racism committed through computer systems; the 2024 Annual Meeting of the 24/7 Network of Contact Points; the Annual Europol Conference; the 2023 Underground Conference; and the 2023 Octopus Conference. The project enjoyed visibility at the Global Conference on the Cyber Capacity Building, where it organised two sessions on the sustainability of the capacity building. Some 139 activities were supported by the project in this period.

- **GLACY-e:** This project commenced in August 2023 with an inception phase running in parallel to the GLACY+ project. This phase was used to clarify the role of hub and selected countries and to develop the workplan for 2024. In December 2023, the GLACY+ closing event also served as the GLACY-e launching conference which permitted an assessment of the impact and results of the first and the setting of priorities of the latter project.

[26] Brazil, May 2023.
[27] The Netherlands, September 2023.
[28] Mauritius, September 2023.
[29] Chile, November 2023.
[30] France, November 2023.
[31] Romania, December 2023.

Studies and guides for practitioners

In 2023, C-PROC prepared additional guides and studies to provide practitioners with practical tools to investigate cybercrime and bring about prosecutions, to handle e-evidence based on international good practices and to prepare legislation ensuring more consistent support to criminal justice authorities in different countries. In the same year:

- "Freedom of Expression within the Context of Action on Cybercrime – Practical considerations", this discussion paper is aimed at supporting policymakers, legislators and criminal justice practitioners in developing and implementing policies and legislation on cybercrime consistent with the right to the freedom of expression (December 2023);

- "Implementing the First Protocol to the Convention on Cybercrime on Xenophobia and Racism: Good practice study" (December 2023), aimed at documenting experience with and facilitating the implementation of this Protocol.

Several other guides, studies and surveys were initiated in 2023 (Guidebook on cybercrime training strategies; Research on cybercrime victims; Survey on cybercrime strategies in GLACY+ countries) and will be finalised in 2024.

Online training platform on cybercrime and e-evidence

In 2023, C-PROC launched the beta version of "CYBOX", the training platform on cybercrime and e-evidence, in response to the need for training activities in online or hybrid format. The platform is to be fully operational by spring 2024 with a view to serving as a virtual hub for training for any country co-operating with the Office, as well as a repository of training materials and courses on the topic. In addition, all activities of the International Network of National Judicial Trainers will be moved to CYBOX on a private, privileged space to be accessible only by its members.

Resources on cybercrime legislation

The strengthening of domestic legislation on cybercrime and e-evidence is an important component of all projects. Examples of such support over the past years are provided above.

C-PROC keeps track of developments regarding cybercrime legislation worldwide and in December 2023 published its updated cursory survey on the "global state of cybercrime legislation". This survey confirms further progress by countries in all regions of the world in the alignment of their domestic laws with the standards of the Convention on Cybercrime. Moreover, C-PROC is maintaining information on developments regarding legislation in "country wikis" and "legal profiles" on the Octopus Platform.

Partnerships and synergies

Capacity building creates synergies and C-PROC activities continued to be carried out in partnership with multiple organisations, among them the EU 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 African Union Commission, the European Cybercrime Training and Education Group (ECTEG), the Caribbean Community (CARICOM), the Community of Portuguese Language-speaking countries (CPLP), 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[32], Parliamentarians for Global Action (PGA), the Organization of American States (OAS), the Pacific Island Law Officers Network (PILON), the UN, the United States Department of Justice, the Government of Romania as the host country of C-PROC and many others. Moreover, various activities were conducted jointly with other capacity building projects funded by the EU (CyberNet, OCWAR-C[33]) that address cybercrime and e-evidence or with support of the TAIEX[34], 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 are also created with other Council of Europe instruments and actions, for example by supporting capacity building activities on data protection in line with the Convention ETS No. 108 as amended by CETS No. 223[35] or on the protection of children against sexual exploitation and sexual abuse in line with the Convention CETS No. 201[36], the creation of the online resource on cyberviolence, or support to typology studies on money laundering.

[32] 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.

[33] Project West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C).

[34] Technical Assistance and Information Exchange instrument of the European Commission (TAIEX)
One example being the series of workshops for Ghanaian judges and prosecutors.

[35] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

[36] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

4. C-PROC projects in 2024

Anticipating the completion of several projects between December 2023 and February 2024, the preparation of new projects and the mobilisation of extra-budgetary resources commenced in 2022 and was a priority of C-PROC in 2023. By the end of 2023, agreements for five new projects had been finalised and were ready for signature.

The list of projects implemented by C-PROC in 2024 will consist of the following:

Project title	Duration	Budget	Funding
OCTOPUS Project	Jan 2021 – Dec 2027	EUR 10 million	Voluntary contributions (Canada, Hungary, Iceland, Italy, Japan, Netherlands, UK and USA) [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 Council of Europe 10% OB/JPP)
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[37] and Ordinary Budget [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 Council of Europe 10% 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 Council of Europe 10% 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 Council of Europe 10% 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 Council of Europe 10% OB/JPP)

With a combined budget of over EUR 34 million – not all of which has yet been secured – C-PROC will have an appropriate level of resources at its disposal for 2024.

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

5. Conclusions

In the ten years since its creation, C-PROC – through its projects and more than 2 100 activities – made a significant contribution to the strengthening of legislation and criminal justice capacities on cybercrime and electronic evidence worldwide, in line with the Convention on Cybercrime and human rights and rule of law requirements. The Octopus Conference 2023 (Bucharest, 13-15 December 2023), with over 500 cybercrime experts from some 130 countries, highlighted the reach of the Convention and of C-PROC. This Conference was preceded by more than 300 other activities supported by the Office in 2023. With the work of the C-PROC, the Council of Europe remains a global leader for capacity building in this field.

Since 2013, C-PROC has attracted considerable extra-budgetary resources that have been properly managed as confirmed by audits and evaluations. While relying on voluntary contributions, C-PROC has become a sustainable structure that should continue to operate in the same manner.

Enabling the participation of experts from parties and states invited to accede to the Convention on Cybercrime in the UN Ad Hoc Committee tasked to elaborate a treaty on "the use of information and communication technologies for criminal purposes" will continue to help ensure that such a future treaty – if adopted – is consistent with the Convention on Cybercrime and comprise the necessary human rights and rule of law safeguards. This also helped UN member states obtain a better understanding of the benefits of the framework of the Convention on Cybercrime and generated numerous requests for accession to it.

With or without an additional UN treaty, the Convention on Cybercrime with its Protocol on xenophobia and racism (ETS No. 189) and its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence, and with the T-CY, will remain the most relevant international framework on cybercrime in the years to come, especially as it is backed up by capacity building by C-PROC.

Requests to C-PROC for capacity building continue to increase because of growing interest in and membership of the Convention on Cybercrime and its Protocols, and because of new and increasingly complex challenges that require innovative and more sophisticated solutions.

The completion of several projects between December 2023 and February 2024 is putting a strain on resources available to C-PROC. However, new projects have been prepared and are ready to commence in early 2024:

- CyberUA project on strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine (voluntary contributions; not yet fully funded);

- CyberEast+ on enhanced action on cybercrime for cyber resilience in Eastern Partnership States (joint project with the EU);

- CyberSouth+ project on enhanced co-operation on cybercrime and electronic evidence in the Southern Neighbourhood Region (joint project with the EU);

- CyberSEE project on enhanced action on cybercrime and electronic evidence in South-East Europe and Türkiye (joint project with the EU);

- CyberSPEX project on enhanced co-operation on e-evidence by EU member states through the Second Additional Protocol to the Convention on Cybercrime (joint project with the EU).

In addition, the ongoing Octopus Project and the GLACY-e joint project on Global Action on Cybercrime Enhanced are available for global outreach. However, additional resources are needed, in particular for the Octopus Project.[38]

Priorities in 2024 are:

- To support the implementation of the Second Additional Protocol to the Convention on Cybercrime through all projects, including the CyberSPEX project for EU member states;

- To further strengthen capacities for the collection and use of electronic evidence for the prosecution of war crimes and gross violations of human rights in Ukraine;

- To assist countries – in particular those already invited to accede to the Convention on Cybercrime – to meet their requirements and become parties;

- To help criminal justice authorities address challenges related to ransomware attacks and virtual currencies and to enhance their co-operation with bodies responsible for cybersecurity;

- To support the strengthening of human rights and rule of law safeguards in countries participating in project activities. This includes in particular support to the implementation of data protection "Convention 108+"[39] and addressing concerns regarding the impact of cybercrime legislation on the freedom of expression;

- To promote further synergies of the Convention on Cybercrime and its Protocols with other relevant Council of Europe instruments, including those on data protection[40], the sexual exploitation and sexual abuse of children[41], violence against women and domestic violence[42] Conventions, money laundering and financing of terrorism.[43] Further partnerships and synergies with other organisations will also be sought;

[38] The Octopus Project in 2023 was funded by the United States of America, the United Kingdom and Japan, but also Iceland and Italy. Note: the Octopus Project is also supporting the activities of the T-CY.

[39] Convention ETS No. 108 as amended by the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS No. 223).

[40] Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS No. 223).

[41] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[42] Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210).

[43] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).

- To launch the CYBOX online platform for training and exchange – developed under the Octopus Project – in order to permit the scaling up of online training on cybercrime and e-evidence.

While C-PROC has been highly effective for the past ten years, requests for capacity building are constantly increasing. Reflections are needed on how to address these demands in the years to come. Developing a concept for future capacity building on cybercrime and electronic evidence is therefore also on the agenda for 2024.