



# OCTOPUS PROJECT

to support implementation of the  
Budapest Convention on Cybercrime and its Protocols worldwide

## Outline

Version 12 June 2023

---

Project title:	Octopus Project (DG1/2542) to support implementation of the Budapest Convention on Cybercrime, its Protocols and related standards
Project area:	Parties and observers to the Budapest Convention on Cybercrime Other States prepared to implement the Budapest Convention and its Protocols
Duration:	84 months (1 January 2021 – 31 December 2027)
Budget:	Up to EURO 10 million
Funding:	Voluntary contributions from State Parties and Observers to the Convention on Cybercrime and other public and private sector organisations
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

---

### BACKGROUND AND JUSTIFICATION

While the threat of cybercrime continues to increase, progress has been made in international cooperation on cybercrime and electronic evidence. The Budapest Convention on Cybercrime is considered to play an important role not only with respect to strengthening legislation and criminal justice action but in promoting broad commitment by governments, international organisations and public as well as private sector stakeholders to co-operation against cybercrime. With the 2<sup>nd</sup> Additional Protocol to this treaty on enhanced co-operation and disclosure of electronic evidence the mechanism of the Budapest Convention will remain of significant relevance and will more effectively address challenges related to e-evidence in foreign, multiple or unknown jurisdictions.

From 2006 to 2013, this process was supported by the [Global Project on Cybercrime \(Phases 1 – 3\)](#), from 2014 to 2020 through the [Cybercrime@Octopus](#) project and starting 2021 by the [Octopus project](#). These and other projects implemented by the Council of Europe have contributed significantly to increased membership in the Budapest Convention and its protocols and a stronger criminal justice response to cybercrime with rule of law safeguards in more than 100 countries.

Given the impact of these projects, it is proposed to extend and expand the Octopus Project to better respond to donors' interests and evolving needs of the project's beneficiaries and stakeholders. Additional streams of activities – specific actions - are added for Kosovo\*<sup>1</sup>, the Caribbean region and Central Asia to better respond to the identified needs and priorities for these countries.

A particular context that came to the forefront in the period 2020-2022 continues to be taken into consideration in further implementation of the Project:

---

<sup>1</sup> \* All references to Kosovo, whether to the territory, institutions, or population, in this text shall be understood in full compliance with United National Security Council Resolution 1244 and without prejudice to the status of Kosovo.

- The COVID-19 pandemic meant that in 2021 activities had to be carried out through virtual means. More emphasis is thus put on the online delivery of activities and the making available of online resources, as well as of an online training platform.
- Following UN General Assembly Resolution 74/247 of December 2019, the preparation of a new international treaty [on crime related to information and communication technologies](#) commenced in January 2022. It will be important that representatives from Africa, Asia/Pacific, Latin America and the Caribbean that have experience with the Budapest Convention can participate in this process and share their expertise. This process furthermore necessitates enhanced outreach and capacity building in these regions.
- Following four years of negotiations, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was opened for signature on 12 May 2022 and by May 2023 had been signed by 37 State Parties to the Convention and ratified by 1 State (Serbia); further signatures are expected in the very near future. Implementation and ratification of this new treaty will be a major task in the coming years. Therefore, additional support will be needed in terms of both legislative reforms and targeted training regarding the new tools of this Protocol. This is particularly important in the light of the UN treaty process.
- The aggression of the Russian Federation against Ukraine is accompanied by cyberattacks and measures to curtail online freedoms and control information. Within this context, it will be essential to reach out to States worldwide and present the Budapest Convention as a framework that stands for a free, open and global Internet where restrictions are limited and subject to rule of law safeguards.

The Octopus Project is therefore not only aimed at supporting implementation of the Budapest Convention, its additional Protocols and related standards, but will also take into account the above considerations along the following objectives (immediate outcomes)

- Assistance to countries in the implementation of the Convention and 1<sup>st</sup> Additional Protocol on Xenophobia and Racism, and its 2<sup>nd</sup> Additional Protocol, including in terms of data protection and other safeguards through support to reforms of legislation, training and other capacity building measures. This would include targeted support to the Caribbean region, Central Asia and Kosovo\*<sup>2</sup>.
- Support to the Cybercrime Convention Committee (T-CY) which is representing the Parties to the Budapest Convention and is the primary body overseeing its implementation. It is preparing [Guidance Notes](#), [assessing implementation](#) of the Convention by the Parties, and identifying solutions to new challenges. Already in June 2013, the T-CY had decided that the Committee should be co-funded by voluntary contributions to projects. The Octopus Project will also support the participation in the United Nations treaty process by Parties and States that have signed or been invited to accede to the Budapest Convention, if requested.
- Organisation of Octopus Conferences. The [Octopus Conference](#) is the flagship event of the Council of Europe on cybercrime since 2004. It involves multiple public and private sector stakeholders from around the world and serves as a laboratory of ideas for the criminal justice response to cybercrime, permits sharing of experience and includes capacity building workshops. In the Octopus Conference 2021, about 1200 cybercrime experts from some 120 countries participated.

---

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

- Implementation of online resources and tools for the online delivery of capacity building activities on cybercrime and electronic evidence. The Cybercrime Programme Office (C-PROC) is responsible for all capacity building activities of the Council of Europe on cybercrime, and will also be implementing the Octopus Project. These resources will be further improved and maintained but also additional tools will be developed to facilitate the virtual sharing of experience and the delivery of training activities.

## PROJECT IMPACT, OUTCOMES AND ACTIVITIES

<b>Project impact</b>	<b>Cybercrime and other offences involving electronic evidence are prevented and controlled in line with international human rights and rule of law standards and good practices.</b>
<b>Project objective (intermediate outcome)</b>	<p><b>To ensure a more effective criminal justice response to cybercrime and electronic evidence worldwide through implementation of the Budapest Convention on Cybercrime (CETS 185), its Protocols and related standards.</b></p> <p>End of project targets:</p> <ul style="list-style-type: none"> <li>- 80 Parties and 15 Observers to the Convention.</li> <li>- 40 Parties to the 1st Protocol.</li> <li>- 20 Parties to the 2nd Additional Protocol and entry into force.</li> <li>- 130 States with substantive and 100 States with procedural powers in line with the Budapest Convention.</li> </ul>
<b>Immediate outcome 1.1</b>	<p><b>Countries have stronger legal bases and criminal justice capacities for the investigation, prosecution, adjudication of and cooperation on cybercrime and electronic evidence in line with the Budapest Convention, its Protocols and related standards.</b></p> <p>End of project targets:</p> <ul style="list-style-type: none"> <li>- Draft laws available in 20 countries</li> <li>- At least 135 countries have aligned their substantive laws and at least 110 their procedural law with the Budapest Convention or its Protocols</li> <li>- At least 150 in-country or regional workshops held</li> <li>- Contribution to up to 100 events of other organisations</li> </ul> <p>Assumption:</p> <ul style="list-style-type: none"> <li>- States make use of advice and other support to join the Budapest Convention and its Protocols.</li> </ul>
Output 1.1.1	Draft amendments / recommendations for amendments are available for countries in order to bring their domestic legislation on cybercrime, electronic evidence, OCSEA and protection of personal data, in line with the Budapest Convention and its Protocols and other relevant international standards.
Activities	<ul style="list-style-type: none"> <li>- Provide legislative and other advice to countries worldwide</li> <li>- Support the organisation of country-specific and regional workshops on legislation</li> </ul>
Output 1.1.2	Criminal justice authorities of countries committed to implement the Budapest Convention assisted to improve their capacities to investigate, prosecute and adjudicate cybercrime and other offences (including forms of cyberviolence) involving electronic evidence, as well as to engage in international cooperation.
Activities	<ul style="list-style-type: none"> <li>- Support the organisation of in-country or regional training on cybercrime and electronic evidence</li> <li>- Train trainers and provide advice and other support to training institutions</li> </ul>

	<ul style="list-style-type: none"> <li>- Support the development of guides, standard operating procedures and other tools for criminal justice practitioners</li> <li>- Contribute to events organised by other organisations</li> </ul>
<b>Immediate outcome 1.2</b>	<p><b>The Cybercrime Convention Committee (T-CY) is better able to carry out the consultations of the Parties, including assessments, guidance notes and other functions, in line with its workplan and Rules of Procedure.</b></p> <p>End of project targets:</p> <ul style="list-style-type: none"> <li>▪ 2nd Additional Protocol is in force and good practices will have been shared regarding its implementation.</li> <li>▪ 4th round of assessments completed and follow up will have been initiated.</li> <li>▪ At least 3 Guidance Notes adopted.</li> <li>▪ At least 7 T-CY country visits.</li> <li>▪ 2 Plenary, 4 Bureau meetings per year.</li> </ul> <p>Assumptions:</p> <ul style="list-style-type: none"> <li>▪ A fully functioning T-CY is necessary to ensure implementation of the Budapest Convention and encourage accessions by additional States</li> </ul>
Output 1.2.1	Two T-CY Plenary meetings held per year with the participation of representatives of Parties and Observer States
Activities	<ul style="list-style-type: none"> <li>- Support the participation of T-CY members and observers in the meetings of the Committee</li> <li>- Provide logistical support to T-CY meetings as well as funding for translation and interpretation</li> </ul>
Output 1.2.2	Increased outreach by the T-CY
Activities	<ul style="list-style-type: none"> <li>- Support T-CY visits to States in view of accession and implementation of the Budapest Convention and its Protocols</li> <li>- Support the participation of T-CY members in relevant fora, including in the United Nations treaty process</li> </ul>
Output 1.2.3	T-CY assessments and other studies completed
Activities	Support the assessments and other activities of the T-CY through research and analyses
<b>Immediate outcome 1.3</b>	<p><b>Octopus Conferences serve as a platform for global dialogue and cooperation on cybercrime and electronic evidence.</b></p> <p>End of project targets:</p> <ul style="list-style-type: none"> <li>▪ 6 Octopus conferences with more than 350 experts per event from at least 100 different countries.</li> </ul> <p>Assumption:</p> <ul style="list-style-type: none"> <li>▪ Octopus conferences mobilise broad support to the Budapest Convention</li> </ul>
Output 1.3.1	Octopus Conferences held every 18 months
Activity	Organise Octopus Conferences
<b>Immediate outcome 1.4</b>	<p><b>Online tools in support of capacity building activities on cybercrime and electronic evidence are available, updated and used.</b></p> <p>End of project targets:</p> <ul style="list-style-type: none"> <li>▪ Tools of the Octopus Platform updated with reliable data.</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Cyberviolence resource populated.</li> <li>▪ Online training platform is set up and being used by C-PROC and interested countries</li> </ul> <p>Assumption:</p> <ul style="list-style-type: none"> <li>▪ An increasing number of activities will need to be carried out virtually or in hybrid format even after the current COVID-19 pandemic.</li> <li>▪ Countries are making use of the available tools and contribute to keeping them up to date</li> </ul>
Output 1.4.1	Improved <a href="#">Octopus Platform</a> and <a href="#">Cyberviolence resource</a> as resources for legislation, training and cooperation
Activities	Further improve the online information tools such as Octopus Platform and Cyberviolence resource in terms of contents and functionalities
Output 1.4.2	Online training platform on cybercrime and electronic evidence is set up and used by criminal justice authorities of interested countries
Activities	Set up a dedicated online training platform on cybercrime and electronic evidence, available for criminal justice authorities and respective training institutions of countries cooperating with C-PROC
<b>Immediate Outcome 1.5</b>	<p><b>Transposition of the standards of the Budapest Convention on Cybercrime and its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence in Kosovo*</b></p> <p>End of project targets</p> <ul style="list-style-type: none"> <li>▪ Domestic legislation on cybercrime and electronic evidence is aligned with the international standards of the Budapest Convention and the Second Additional Protocol.</li> <li>▪ Increased number of investigators, prosecutors and judges with enabled cybercrime skills;</li> <li>▪ Guides or templates on handling electronic evidence and public/private and international co-operation are available and used by Kosovo* authorities;</li> <li>▪ Enhanced extent and effectiveness of engaging in international and public/private co-operation.</li> </ul> <p>Assumption</p> <ul style="list-style-type: none"> <li>▪ The authorities make use of advice and other support provided in the framework of the project, including with regard to aligning the legislation with the Budapest Convention and its Protocols.</li> </ul>
Output 1.5.1	The regulatory framework for cybercrime investigations and electronic evidence is amended in line with the standards of the Budapest Convention and its Second Protocol
Activities	Provision of assessments, advice, workshops and other activities to review and reform applicable regulations transposing the standards of the Budapest Convention and the Second Protocol.
Output 1.5.2	The capacities of investigators, prosecutors and judges of Kosovo* on cybercrime and electronic evidence have been strengthened.
Activities	<ul style="list-style-type: none"> <li>- Provision of capacity-building and practical exercises (simulation exercises, scenario-based training, mock trials or exchange programmes) for investigators, prosecutors and judges</li> <li>- Support to the set-up of cybercrime online reporting mechanism for Kosovo Police.</li> </ul>

Output 1.5.3	Competent criminal justice authorities of Kosovo* are able to effectively engage in public/private and international co-operation using the tools provided by the Budapest Convention and the Second Additional Protocol.
Activities	<ul style="list-style-type: none"> <li>- Review of procedures, development guidelines and provision of training on co-operation with domestic and multi-national service providers, including regarding requests for subscriber information and co-operation in emergency situations.</li> <li>- Review of procedures, development of templates and guides and provision of training sessions on international co-operation, including regarding matters addressed by the Budapest Convention and the Second Protocol (requests for data preservation and for stored computer data; video conferencing, joint investigations, emergency requests) for competent authorities, including a 24/7 point of contact.</li> </ul>
<b>Immediate Outcome 1.6</b>	<p><b>Countries of the Caribbean region have stronger legal bases and criminal justice capacities for the investigation, prosecution, adjudication of and cooperation on cybercrime and electronic evidence in line with the Budapest Convention on Cybercrime, its Protocols and related standards.</b></p> <p>End of project targets</p> <ul style="list-style-type: none"> <li>▪ Domestic legislation on cybercrime and electronic evidence in 14 target countries of the Caribbean region is largely in line with the standards of the Budapest Convention, or respective draft laws are available;</li> <li>▪ Up to 5 countries of the Caribbean region undertake reforms to align its legal framework with the standards of the Second Additional Protocol;</li> <li>▪ Recommendations for improvement of legislation on cyberviolence are available in interested countries of the region;</li> <li>▪ Increased number of investigators, prosecutors and judges with enabled cybercrime skills;</li> <li>▪ Up to 3 judicial training institutes of the region start delivering trainings on cybercrime and electronic evidence;</li> <li>▪ Enhanced extent and effectiveness of international and public/private co-operation</li> </ul> <p>Assumption</p> <ul style="list-style-type: none"> <li>▪ Target countries of the Caribbean region States make use of advice and other support to join the Budapest Convention and its Protocols.</li> </ul>
Output 1.6.1	Regulatory framework of countries in the Caribbean region: Draft laws or amendments available to further align domestic legislation with international standards.
Activities	<ul style="list-style-type: none"> <li>- Prepare an updated assessment of legislation on cybercrime and electronic evidence in the Caribbean region.</li> <li>- Support country-specific and regional dialogue between stakeholders (including parliaments and civil society) on reforms of legislation.</li> <li>- Support domestic working groups in the preparation of draft laws.</li> </ul>
Output 1.6.2	Criminal justice capacities of countries in the Caribbean region: Increased capacities for the investigation, prosecution, adjudication of and cooperation on cybercrime and electronic evidence.
Activities	<ul style="list-style-type: none"> <li>- Prepare an assessment of criminal justice capacities regarding cybercrime and electronic evidence in the Caribbean region.</li> <li>- Cooperate with judicial training institutes of the region in the development of a training programme on cybercrime and electronic evidence:</li> </ul>

	<ul style="list-style-type: none"> <li>- Training of trainers</li> <li>- Adaption of training modules on cybercrime and e-evidence</li> <li>- Delivery of pilot courses</li> </ul> <ul style="list-style-type: none"> <li>- Support the development of law enforcement training strategies on cybercrime and electronic evidence and the delivery of pilot courses for investigators.</li> <li>- Provide advice on the establishment of 24/7 points of contact and their role regarding preservation requests and cooperation in emergencies.</li> <li>- Promote cooperation between criminal justice authorities with multi-national service providers.</li> </ul>
Output 1.6.3	Addressing cyberviolence: Recommendations for a more effective criminal justice response to protect victims of cyberviolence.
Activities	<ul style="list-style-type: none"> <li>- Prepare an assessment of the criminal justice response to cyberviolence in the Caribbean region.</li> <li>- Develop proposals for further legislative reforms to address different forms of cyberviolence.</li> <li>- Cooperate with criminal justice authorities and victim support organisations in the development of recommendations regarding the procedures for reporting cyberviolence.</li> </ul>
<b>Immediate Outcome 1.7</b>	<p><b>Countries of Central Asia have stronger legal bases and criminal justice capacities for the investigation, prosecution, adjudication of and cooperation on cybercrime and electronic evidence in line with the Budapest Convention on Cybercrime, its Protocols and related standards.</b></p> <p>End of project targets</p> <ul style="list-style-type: none"> <li>▪ Draft laws available in 2 countries of Central Asia aligning its legislation with the standards of the Budapest Convention, recommendations for improvement of legislation are available for the other countries.</li> <li>▪ Increased number of investigators, prosecutors and judges with enabled skills on cybercrime, electronic evidence and international cooperation in countries interested in the framework of the Budapest Convention.</li> </ul> <p>Assumption</p> <ul style="list-style-type: none"> <li>▪ States make use of advice and other support to join the Budapest Convention and its Protocols.</li> </ul>
Output 1.7.1	Regulatory framework of countries in Central Asia: Draft laws or amendments available to further align domestic legislation with international standards including rule of law and human rights safeguards.
Activities	<ul style="list-style-type: none"> <li>- Prepare an updated assessment of legislation on cybercrime and electronic evidence in the countries of Central Asia.</li> <li>- Support country-specific and regional dialogue between stakeholders (including parliaments and civil society) on reforms of legislation.</li> <li>- Support domestic working groups in the preparation of draft laws.</li> </ul>
Output 1.7.2	Criminal justice capacities of countries in Central Asia interested in the framework of the Budapest Convention: Increased capacities for the investigation, prosecution, adjudication of and cooperation on cybercrime and electronic evidence in line with rule of law and human rights standards.
Activities	<ul style="list-style-type: none"> <li>- Prepare an assessment of criminal justice capacities regarding cybercrime and electronic evidence in countries of Central Asia interested in the framework of the Budapest Convention.</li> <li>- Provision of in-country and regional capacity-building and practical exercises for investigators, prosecutors and judges on cybercrime and electronic evidence</li> </ul>

	<ul style="list-style-type: none"><li>- Provide advice on the establishment of 24/7 points of contact and their role regarding preservation requests and cooperation in emergencies.</li><li>- Promote cooperation between criminal justice authorities with multi-national service providers.</li></ul>
--	--

## CONTACT

Cybercrime Programme Office of the  
Council of Europe (C-PROC)

[Alexander.seger@coe.int](mailto:Alexander.seger@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE