COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2020)32

12 November 2020

Council of Europe Office on Cybercrime in Bucharest:

C-PROC activity report for the period October 2019 – September 2020

Contents

Executive summary

The Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania, is responsible for ensuring the implementation of capacity-building projects in the area of cybercrime and electronic evidence, on the basis of the Budapest Convention and in all regions of the world.

The present report is to inform the Committee of Ministers of the activities of the Office, from October 2019 to September 2020.

C-PROC supported approximately 240 activities over the reporting period. Through the Office, the Council of Europe remains a global leader for capacity building in cybercrime and electronic evidence.

In 2020, the Office was affected by COVID-19 in that the pandemic not only led to a massive increase in cybercrime, underlining the relevance of the Budapest Convention and related capacity building, but also in that it shaped the way in which the Office had to carry out its activities from March 2020 onwards. All of the 130 activities between April and September 2020, other than desk studies, were implemented online.

C-PROC – in spite of the COVID-19 pandemic – contributed significantly to:

- the strengthening of criminal justice capacities and legislation on cybercrime and electronic evidence;
- new memberships and implementation of the Budapest Convention;
- the process of preparation of the 2nd Additional Protocol to the Budapest Convention;
- synergies with other relevant organisations and instruments.

By September 2020, C-PROC was one of the largest external offices of the Council of Europe with a cumulative budget of more than EUR 38 million for active projects and with 35 staff.

The Office relied on external funding. During the past year, more than 90% of its budget was funded by voluntary contributions. The European Union remained the main donor through joint projects co-funded by the Council of Europe. The United States of America also made major funding available. Other donors during this period were Estonia, the United Kingdom and Japan. The Office further benefits from the support of the Government of Romania, which continues to provide rent-free office space.

The formula of the Budapest Convention as the common standard backed up by the Cybercrime Convention Committee (T-CY) and capacity building through C-PROC continued to ensure impact. With the future 2nd Additional Protocol, the mechanism of the Budapest Convention is likely to remain the most relevant international standard for years to come.

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 (C-PROC) in Bucharest, Romania, during the period October 2019 to September 2020.[1]

The Office has been in operation since 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 of the Council of Europe in cybercrime, in all regions of the world.[4]

This reporting period was marked in particular by the COVID-19 pandemic from March 2020 onwards, and the present report shows how the Office continued to make an impact within this context.

C-PROC and the COVID-19 pandemic

COVID-19 related cybercrime

Cybercrime – that is, offences against and by means of computer systems – has evolved into a significant threat to fundamental rights, democracy and the rule of law, as well as to international peace and stability, and it has a major social and economic impact.

While this was illustrated in recent years by ransomware attacks, such as “WannaCry”, *inter alia* crippling hospitals, or election interference, COVID-19 related cybercrime has further amplified the phenomenon. This led some to call it also a “digital pandemic”. COVID-19 forced societies to rely even more on computer systems to communicate, shop, share and receive information and otherwise mitigate the impact of social distancing and other measures taken to contain the pandemic. Teleworking and virtual meetings have become the norm.

This reliance was and is still being exploited on a massive scale by malicious actors for phishing campaigns and malware distribution, ransomware and other critical information infrastructure attacks, fraud schemes and the spreading of disinformation. Online child sexual exploitation and abuse also increased.[5]

Criminal justice authorities need to engage in full co-operation to detect, investigate, attribute and prosecute the above offences and bring to justice those who exploit the COVID-19 pandemic for their own criminal purposes. With the Budapest Convention, a framework for effective co-operation with the necessary rule of law safeguards is available to 65 states.

[1] The decision setting up the Office (see below) 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

[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 its 1180th meeting.

[4] For the approach of the Council of Europe on cybercrime see the summary in the appendix.

[5] This has been confirmed by EUROPOL, INTERPOL and reports of numerous other public and private sector organisations, including the COVID-19 Cyber Threat Coalition. An online resource by C-PROC provides further information.

C-PROC, among other things, created an online resource to promote such co-operation. The future 2nd Additional Protocol will provide additional means for efficient co-operation, including in emergency situations.

Impact of COVID-19 on capacity building

COVID-19 not only led to a massive increase in cybercrime, underlining the relevance of the Budapest Convention and related capacity building by C-PROC, but it very much shaped the way in which the Office had to carry out its activities from March 2020 onwards:

- All of the 130 activities between April and September 2020, other than desk studies, were implemented online. These ranged from open or restricted webinars, to advisory workshops on cybercrime legislation, country-specific meetings on the development of standard operating procedures for electronic evidence, table-top exercises for policy makers, law enforcement training workshops and other types of activities.[6] The Office also supported virtual meetings related to the negotiations on the 2nd Additional Protocol to the Budapest Convention, in the Cybercrime Convention Committee (T-CY).

- Additional online resources were developed or further improved, including:

  - the Octopus Community with "country wikis", "legal profiles", country-specific procedures for international co-operation, as well as training materials and guides;
  - a tool on webinars;
  - a portal on COVID-19 related cybercrime;
  - resources on cyberviolence.

- The infrastructure of C-PROC was improved to provide the necessary bandwidth and technical capacity for online activities. Staff was highly versatile and adapted or was trained to organise virtual activities, and the Office obtained administrator access to the platforms needed for such activities.

- The Office engaged in increased co-operation online with a range of partners, including the European Union, INTERPOL, CARICOM, the Anti-Phishing Working Group, the United Nations and many others.

[6] See list of activities in the appendix or examples in the "news" at www.coe.int/cybercrime.

Overview of projects and results in the period October 2019 – September 2020

Overview of current projects

In the period October 2019 to September 2020, C-PROC supported approximately 240 activities under the following projects.

List of projects (October 2019 – September 2020)			
Project title	Duration	Budget	Funding
Cybercrime@Octopus	January 2014 – December 2020	EUR 4 million	Voluntary contributions (Estonia, Hungary, Monaco, Netherlands, Romania, Slovak Republic, UK, Japan, USA and Microsoft)
GLACY+ project on Global Action on Cybercrime Extended	March 2016 – February 2024	EUR 18.9 million	EU/CoE JP (including 10% Council of Europe Ordinary Budget,OB)
iPROCEEDS project targeting proceeds from crime on the internet in South-eastern Europe and Turkey	January 2016 – December 2019	EUR 5.56 million	EU/CoE JP (10% OB)
iPROCEEDS-2 project targeting proceeds from crime on the Internet and securing electronic evidence in South-eastern Europe and Turkey	January 2020 – June 2023	EUR 4.95 million	EU/CoE JP (10% OB)
EndOCSEA@EUROPE project against Online Child Sexual Exploitation and Abuse	July 2018 – June 2021	EUR 0.97 million	End Violence against Children Fund
CyberSouth on capacity building in the Southern Neighbourhood	July 2017 – December 2021	EUR 5 million	EU/CoE JP (10% OB)
CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region	June 2019 – June 2022	EUR 4.22 million	EU/CoE JP (10% OB)

A detailed inventory of activities supported or carried out, and other information is available online.

By September 2020, the combined budget of projects underway amounted to some EUR 38 million. This represents a further increase compared to previous years.[7]

[7] 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.

The Office relies on external funding. During the past year, more than 90% of its budget was funded by voluntary contributions. The European Union remained the main donor through joint projects co-funded by the Council of Europe. The United States of America also made major funding available. The other donors during this period were Estonia, the United Kingdom and Japan. The Office further benefits from the support of the Government of Romania, which continues to provide rent-free office space.

While Cybercrime@Octopus and EndOCSEA@EUROPE are fully funded by voluntary contributions, joint projects with the European Union include 10% co-funding from the budget of the Council of Europe.

Results

Criminal justice capacities

From October 2019 to September 2020, C-PROC made a significant contribution to the strengthening of criminal justice capacities, in countries from all over the world. In addition to the 45 priority countries which are currently eligible to receive the full menu of support – ranging from reforms of legislation and sustainable training programmes for criminal justice practitioners to practical exercises and procedures for interagency, public/private and international co-operation – about 80 other countries participated in at least some of the activities.[8]

Examples of activities are:

- CyberEast: 14 training sessions and workshops on cybercrime investigations and computer forensics, co-operation with service providers and online crime proceeds were organised in close co-operation with national training academies;
- CyberSouth: support to standard operating procedures and toolkits for first responders on cybercrime and electronic evidence in Jordan and Morocco; support to working groups on judicial training materials in Lebanon and Tunisia;
- EndOCSEA@EUROPE: reviews of training strategies for law enforcement agencies of Armenia, Azerbaijan and Ukraine; training package on Online Child Sexual Exploitation and Abuse (OCSEA) for law enforcement, judges and prosecutors;
- GLACY+: remote delivery of in-country or regional activities, such as First responders course; or E-Learning such as E-Evidence Boot Camp, E-FIRST Course;
- iPROCEEDS-2: participation of criminal justice practitioners of project countries and areas in the distance Master programme on Forensic Computing and Cybercrime Investigation at University College Dublin.

The T-CY report on the "Budapest Convention on Cybercrime: benefits and impact in practice" (July 2020) confirmed once more the value of the Council of Europe-specific approach through which, in a dynamic process, the standards of the Budapest Convention and the follow-up by the Cybercrime Convention Committee are constantly reinforced by capacity building by C-PROC.

[8] For specific examples see Appendix.

This triangle generates impact on:

- domestic legislation on cybercrime and electronic evidence;
- domestic investigations based on such legislation;
- international co-operation, including of serious and organised cases of cybercrime;
- public/private co-operation;
- the strengthening of criminal justice capacities.

This in turn contributed to the implementation of the UN Agenda 2030 for Sustainable Development, in particular, 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").

Cybercrime legislation

Assistance to the strengthening of domestic legislation on cybercrime and electronic evidence is a major component in all projects. As a result, numerous countries either adopted such legislation or advanced with their reforms between October 2019 and 2020.

C-PROC is closely following developments in this respect. The updated "Global state of cybercrime legislation" (published in March 2020) shows that further states had adopted substantive domestic criminal legislation in line with the Budapest Convention. By February 2020, 106 states (or 55% of UN members) had such legislation in place. Additional countries followed their example between March and September 2020. Many of them had benefited from C-PROC assistance, often not only on cybercrime but also on data protection legislation in line with 'Convention 108+' (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223).

Country-specific information in the form of "wikis" and legal profiles is made available at the Octopus Community.

Membership and implementation of the Budapest Convention

The rationale of capacity building is to support governments in a process of change to achieve defined goals. If these goals are related to an effective criminal justice response to cybercrime in line with the Budapest Convention, this process is supported by C-PROC.

Capacity building remains a primary factor for increased membership of the Budapest Convention. It is an incentive for many countries to seek accession and it helps countries which are preparing to become Parties to meet the obligations of the Convention and to engage in effective international co-operation.

Between October 2019 and September 2020, Colombia and Peru have become Parties, and Brazil, Burkina Faso, Guatemala, New Zealand and Niger have been invited to accede to the Budapest Convention. C-PROC is assisting numerous other countries in their reform of domestic legislation prior to a request for accession.

2nd Additional Protocol to the Budapest Convention

The preparation of the 2nd Additional Protocol commenced in September 2017 and is undertaken within the framework of the Cybercrime Convention Committee (T-CY). This new Protocol is to provide for more effective co-operation on cybercrime and electronic evidence, including:

- Provisions for more efficient mutual assistance;
- Expedited co-operation in emergency situations;
- Direct co-operation with service providers and registrars in other Parties;
- Data protection safeguards.

If agreement can be found on these provisions, the Protocol will be of much operational value for practitioners, setting international standards for efficient co-operation with appropriate safeguards and ensuring the continued relevance of the Budapest Convention.

C-PROC is facilitating this work through the Cybercrime@Octopus project, financed by voluntary contributions. Support to several Protocol Drafting Plenaries, and numerous Drafting Group and subgroup meetings helped to significantly advance negotiations. The Octopus Conference in November 2019 served as a platform for multi-stakeholder consultations on draft provisions of the Protocol.

The prospect of this Protocol is enhancing interest in the Budapest Convention and creates more demand for capacity building. New C-PROC projects already include the possibility to support implementation of the Protocol in different regions of the world once it is available.

Synergies

Capacity building creates synergies. As in previous years, C-PROC activities were carried out in partnership with multiple organisations, among them the European Union, EUROJUST, EUROPOL, the EU Institute for Security Studies, the African Union Commission, CARICOM, the Community of Portuguese Language-speaking countries (CPLP), ECOWAS, FOPREL, the Global Forum for Cyber Expertise (GFCE), the International Association of Prosecutors, INTERPOL, the Organization of American States, the Pacific Island Law Officers Network (PILON), the United Nations, the US Department of Justice and the US Department of State, the Government of Romania as the host country of C-PROC and many others. The Octopus Conference brought stakeholders from more than 115 countries to the Council of Europe in Strasbourg in November 2019. In June and July 2020, a series of joint webinars of the European Union and the Council of Europe was offered to facilitate the sharing of experience of practitioners in the elaboration of international policies on cybercrime. C-PROC is therefore well connected to large networks of experts and institutions in all regions of the world.

Synergies are also created with other Council of Europe instruments. GLACY+ assisted several countries in the implementation of data protection ‘Convention 108+’.

EndOCSEA@Europe is implemented by the Children’s Rights Division with the support of C-PROC and illustrates the synergies between the Budapest and Lanzarote Conventions.

The online resources on “cyberviolence” are another example of synergies between the Budapest, Lanzarote and Istanbul Conventions.

Conclusions

Impact

The Cybercrime Programme Office of the Council of Europe, between October 2019 and September 2020 – and in spite of the COVID-19 pandemic – further contributed significantly to the strengthening of criminal justice capacities and legislation on cybercrime and electronic evidence, and also to the implementation of the Budapest Convention and synergies with relevant organisations and instruments.

Through C-PROC, the Council of Europe remains a global leader for capacity building in cybercrime and electronic evidence.

The formula of the Budapest Convention as the common standard, backed up by the Cybercrime Convention Committee (T-CY) and capacity building through C-PROC have continued to ensure impact. With the future 2nd Additional Protocol, the Budapest Convention is likely to remain the most relevant international standard for years to come.

Priorities

While the Office will continue to follow the path that has proven to produce results and impact in partnership with other organisations, specific priorities for the forthcoming 12 months are:

- To further increase its ability for the online delivery of capacity-building activities, and further improve online resources. While timelines for the pandemic and related restrictions are difficult to predict, it is quite certain that online activities will remain an important feature in the future. If well designed, a mix of physical and virtual activities can help to produce greater impact at lower cost. In addition to the range of virtual activities already carried out by C-PROC, in the coming months this could include:

    - creating virtual networks of practitioners within and across different regions of the world;
    - offering other organisations and initiatives a platform for the delivery of joint activities;
    - setting up of a platform for e-learning and training;
    - further development of online resources (new judicial training courses, electronic evidence guide, guide on cybercrime statistics, country wikis and legal profiles on online child sexual exploitation and abuse, and others).

- To promote further synergies between the Budapest Convention and related Council of Europe standards, including its 1st Protocol on xenophobia and racism (CETS 189) as well as data protection (CETS 223), Lanzarote (CETS 201) and Istanbul (CETS 210) Conventions.

- To support the finalisation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime.

- To prepare new projects and mobilise resources. The current portfolio of projects covers priority regions in Europe (Eastern Partnership region, and South-eastern Europe and Turkey) as well as countries in other parts of the world committed to implementing the Budapest Convention. Some projects will come to an end in the near future, and follow-up will be required:

  - The current project Cybercrime@Octopus will end in December 2020. It will be followed by the new Project Octopus with a budget of up to EUR 5 million and a duration of four years from January 2021 to December 2024. A recent US contribution of US$ 1.5 million provides initial funding. Discussions with other donors are underway.
  - The project End-OCSEA@Europe on online child abuse is scheduled to end in June 2021. A follow-up project would be necessary.
  - The project CyberSouth is to end in December 2021 and reflections on possible follow up would need to commence soon.

  Overall, C-PROC is well resourced at this point. The COVID-19 related necessity of moving all activities online is likely to lead to important savings within projects. A re-budgeting and re-planning with a possible extension of projects may need to be undertaken in consultation with donors in the near future.

C-PROC is well prepared to continue to evolve in terms of quality, expertise, impact and synergies for global co-operation on cybercrime and e-evidence.