COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2021)32

15 November 2021

Council of Europe Office on Cybercrime in Bucharest:

C-PROC activity report for the period October 2020 – September 2021

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 on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime and in all regions of the world. The purpose of the present report is to inform the Committee of Ministers of the activities of the Office from October 2020 to September 2021.

C-PROC operated within a context of (a) evolving challenges of cybercrime and electronic evidence to human rights, democracy and the rule of law, (b) the increasing reach and impact of the Convention on Cybercrime since its opening for signature 20 years ago, (c) the finalisation of the Second Additional Protocol to the Convention, (d) the beginning of a United Nations (UN) process aimed at a new treaty on countering the use of information and communication technologies for criminal purposes, and (e) the COVID-19 pandemic.

C-PROC supported 395 activities involving more than 120 countries between October 2020 and September 2021 – most of them carried out online due to COVID-19 related restrictions. The Office maintained its reputation as a centre of excellence for capacity building on cybercrime and electronic evidence.

C-PROC focused on:

- the strengthening of criminal justice capacities and legislation on cybercrime and electronic evidence;
- the development of guides and tools on cybercrime matters and their implementation;
- increasing membership and implementation of the Budapest Convention;
- the process of preparation of the Second Additional Protocol to the Budapest Convention;
- synergies with other organisations and projects.

By September 2021, C-PROC was one of the largest external offices of the Council of Europe with a cumulative budget of approximately EUR 38 million for active projects and 37 staff.

The Office continues to broadly rely on external funding. More than 90% of its budget is 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 Hungary, the United Kingdom, Canada and Japan. The Office also relies on the support of the Government of Romania, which provides 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 forthcoming Second Additional Protocol, the Budapest Convention is likely to remain the most relevant international mechanism for years to come.

Priorities for the next year include (a) support to the implementation of the Second Additional Protocol, (b) strengthening of human rights, rule of law and data protection safeguards, (c) further enhancing capabilities for the online delivery of activities, (d) synergies with other Council of Europe instruments and mechanisms as well as with other organisations, and (e) extension of current and design of new projects to secure funding for future capacity building.

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 (C-PROC) between October 2020 and September 2021.[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.

C-PROC is a key element of the Council of Europe approach to cybercrime, consisting of (a) the Budapest Convention and related standards, (b) follow-up assessments by the Cybercrime Convention Committee (T-CY), and (c) capacity building.

2. Context

The challenges of cybercrime and electronic evidence

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 and has a major social and economic impact. Current cybercrime threats and trends reportedly include the following:

- The COVID-19 pandemic has increased reliance on information and communication technology and accelerated the digital transformation of societies. This reliance is criminally exploited in the form of phishing campaigns and malware distribution, ransomware attacks (including against health facilities), fraud schemes, disinformation or increased online sexual violence against children.[4]

- Ransomware, which prevents access to or use of data, systems or networks unless payments are made, typically in cryptocurrency, is currently considered the number one cybercrime threat. Ransomware attacks have interfered with or paralysed government and private sector organisations, including critical infrastructure.[5] The shutting down of hospital services through ransomware has reportedly led to fatalities.[6]

- Supply chain attacks, where not only networks or systems are attacked but software or other devices connected to them via the supply chain, thus bypassing security measures.[7]

- Democratic processes, including elections, continue to be at risk of cyber attacks and interference. While measures have been taken in many countries to enhance the security of computer systems used in elections, attempts to destabilise elections through illegal access to computer systems of parliaments, political parties, politicians or election campaigns are still reported.

[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
For the period October 2019 to September 2020 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] See the online resource made available by C-PROC.

[5] For examples see https://www.blackfog.com/the-state-of-ransomware-in-2021/

[6] See for example: https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

[7] See for example: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

- The cost of cyberattacks (damage or theft of data or money, lost productivity and disruption of business activities, theft of intellectual property, fraud, forensic investigation, recovery or restoration of data or systems, reputational damage) reportedly exceeded USD one trillion in 2020.[8] For example, in August 2021, the German internet industry association BITKOM quantified the annual damage of cyber attacks against German industry at over EUR 220 billion.[9]

- The online sexual exploitation and sexual abuse of children is further exacerbated by the COVID-19 pandemic in the form of increased child sexual abuse materials, online grooming, online abuse communities, online risk taking by minors and live streaming of abuse.[10] In 2020, the CyberTipline operated by the National Centre for Missing and Exploited Children received 21.7 million reports of child abuse from service providers with over 65 million video files and images of child abuse. By far the largest number of reports was received from Facebook (20.3 million).[11] Every month, Facebook reportedly removes some 250,000 WhatsApp accounts suspected of sharing child abuse images.[12] The scale of such abuse and the number of offenders and victims in multiple jurisdictions raises major challenges to investigations and prosecutions.

- Moreover, the darkweb provides for illicit market places for any type of criminal activity, including tools and services for the commission of further crime (crime-as-a-service).[13] Cybercrime facilitates or finances other forms of crime, including organised crime and terrorism.

- All types of crime, not only cybercrime, may entail evidence on computer systems. This means that the effectiveness of many instruments of the Council of Europe related to criminal matters will be significantly enhanced if the respective Parties also have the procedural and international co-operation tools of the Budapest Convention and its forthcoming Second Additional Protocol at their disposal. Examples range from the Criminal Law Convention on Corruption (ETS 173) to the conventions and/or protocols on money laundering and financing of terrorism (CETS 198), trafficking in human beings (CETS 197), terrorism (ETS 190, CETS 196, CETS 217), protection of children against sexual exploitation and abuse (CETS 201), violence against women and domestic violence (CETS 210), counterfeiting of medical products and similar crimes involving threats to public health (CETS 211), manipulation of sports competitions (CETS 215), trafficking in human organs (CETS 216) and others.

20 years of Budapest Convention on Cybercrime

The Convention on Cybercrime was opened in Budapest, Hungary, on 23 November 2001. Over the course of 20 years the impact of this instrument has become global. For example:

- By September 2021, 66 States, including 21 non-member states of the Council of Europe were Parties, 11 had signed it or been invited to accede and several requests for accession were in process in line with Article 37 of the Convention. With each new Party, the value of the Convention as a framework for international co-operation on cybercrime and electronic evidence has been increasing. An example is the 24/7 Network of contact points pursuant to Article 35.

[8] https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion-120120700249_1.html

[9] https://www.bitkom-research.de/de/pressemitteilung/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr

[10] See for example: https://www.end-violence.org/sites/default/files/paragraphs/download/esafety%20OCSE%20report%20-%20salter%20and%20wong.pdf

[11] Source: https://www.missingkids.org/content/ncmec/en/ourwork/impact.html and https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf

[12] https://www.theguardian.com/global-development/2021/feb/09/exclusive-rise-in-child-abuse-images-online-threatens-to-overwhelm-uk-police-officers-warn

[13] See for example, https://securityintelligence.com/news/darkmarket-dark-web-marketplace-taken-down/ and https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

- More than 120 states had substantive criminal law provisions in their domestic law broadly corresponding to those of the Convention. More than 90 states also had procedural powers in place to investigate cybercrime and collect electronic evidence. And over 150 states had used it as a guideline or at least as a source of inspiration when reforming domestic legislation.[14]

- The Convention thus had a clear influence on investigations and prosecutions in states that have reformed their domestic laws based on this treaty. It also had an impact on the rule of law through the implementation of the safeguards of the Convention (such as judicial oversight under Article 15) to prevent the misuse of investigative powers. And in a number of states the reform of criminal legislation is accompanied by reforms of data protection legislation, often with the support of the Council of Europe and in line with Conventions 108 and now also “108+”.

- The Convention is a catalyst for capacity building which, in turn, is a primary factor for increased membership of the Budapest Convention. The rationale for co-operation programmes implemented by C-PROC is that while any country may be assisted in the reform of domestic legislation in line with the Budapest Convention, a state that has gone further and requested accession or has become a Party may become a “priority country” eligible for the full range of training and other technical assistance activities so as to permit implementation of the Convention.

This last point helps explain the reasons for the global impact of the Convention. Apart from the fact that it provides a framework for a criminal justice response that meets human rights and rule of law requirements, the Convention is backed up by the Cybercrime Convention Committee (T-CY) for assessments and follow up, and by the capacity-building activities of C-PROC.[15] These permit continuous co-operation, outreach and reform in line with this treaty.

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

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, current tools are not sufficient for an effective criminal justice response and also to permit governments to meet their positive obligation to provide the means to protect the rights of individuals against crime.

Therefore, after almost four years of consultation, on 28 May 2021, the Cybercrime Convention Committee completed negotiations and approved the draft Second Additional Protocol on enhanced co-operation on cybercrime and electronic evidence. The draft Protocol is the result of an inclusive process involving over 600 experts from 75 countries, 91 negotiation sessions and six rounds of stakeholder consultations.

The Protocol will be of operational value for practitioners in that it provides for:

- a legal basis for disclosure of domain name registration information;
- a basis for direct co-operation with service providers for subscriber information (“direct disclosure”);
- effective means to obtain subscriber information and traffic data (“giving effect”);
- immediate co-operation in emergencies (“expedited disclosure” and “emergency MLA”);
- mutual assistance tools (“video-conferencing”, “JITs”);
- data protection safeguards to permit the flow of personal data under the Protocol.

It will also be of policy value in that, with this Protocol the Convention on Cybercrime will remain relevant and effective, as it demonstrates that effective co-operation with rule of law and data protection safeguards is feasible, and that the Convention will continue to stand for a free and open internet where restrictions are limited to cases of criminal misuse.

[14] See the surveys prepared by C-PROC on the global state of cybercrime legislation

[15] See the T-CY report on “The Budapest Convention on Cybercrime. Benefits and impact in practice”.

Once adopted by the Committee of Ministers it could be opened for signature in March 2022.

C-PROC facilitated this work under the Cybercrime@Octopus and Octopus projects and supported meetings of the Protocol Drafting Plenaries and Drafting Group and subgroup meetings.

Information on the forthcoming Protocol has already been provided in a number of C-PROC activities. Once the Protocol will be opened for signature, more capacity building will be needed to support its implementation. Such support can be provided without delay as it is already foreseen under current C-PROC projects.

UN Ad Hoc Committee on countering the use of information and communications technologies for criminal purposes

In December 2019, through Resolution 74/247, the United Nations General Assembly decided to establish an "open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes". The Ad Hoc Committee, *inter alia* shall take "into full consideration existing international instruments".

In May 2021, the General Assembly adopted Resolution 75/282, entitled "Countering the use of information and communications technologies for criminal purposes" regarding the modalities of the treaty process. The first substantive session is scheduled for 17 to 28 January 2022 in New York.

Completion of the Second Additional Protocol to the Convention on Cybercrime in 2021 will provide State parties to the Budapest Convention with benchmarks regarding the substance as well as the necessary human rights, rule of law and data protection safeguards to be upheld in the context of a future UN treaty.

C-PROC may support the participation of experts from project priority countries in UN meetings related to this process.

Covid-19 and capacity building

The Covid-19 pandemic has led to a massive increase in cybercrime, underlining the relevance of the Budapest Convention and related capacity building by C-PROC. However, it also continued to shape the way in which C-PROC carried out capacity-building activities. Almost all of the 395 activities – with the exception of research and desk studies – were held online, either through open or restricted webinars, advisory workshops on cybercrime legislation, country-specific meetings for the development of standard operating procedures for electronic evidence, table-top exercises for policy makers, law enforcement training workshops or other types of activities.

A number of online tools were developed or further improved, such as the "country wikis" and "legal profiles" on the Octopus Platform, the Cyberviolence resource, or the resource on Cybercrime and Covid-19.

C-PROC staff have acquired additional competencies for the delivery of online activities, and the technical infrastructure of the Office was further improved.

Anticipating that online events will also take place post-Covid, a new C-PROC platform for e-learning and the delivery of judicial training online is being developed under the Octopus Project that is expected to become operational in 2022.

3. Overview of projects and achievements between October 2020 and September 2021

Current projects

In the period October 2020 to September 2021, C-PROC supported approximately 395 activities under the following projects:

List of projects (October 2020 – September 2021)			
Project title	**Duration**	**Budget**	**Funding**
Cybercrime@Octopus	Jan 2014 – Dec 2020	EUR 4 million	Voluntary contributions (Estonia, Hungary, Monaco, Netherlands, Romania, Slovakia, UK, Japan, USA and Microsoft)
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2024	EUR 18.9 million	EU/CoE JP (including 10% Council of Europe Ordinary Budget, OB)
OCTOPUS Project	Jan 2020 – Dec 2024	EUR 5 million	Voluntary contributions (Hungary, UK, Canada, Japan and USA)
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 – Dec 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 is available online.

By September 2021, the combined budgets of projects underway amounted to some EUR 38 million.[16]

The Office relies to a broad extent 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, and Hungary, the United Kingdom, Canada and Japan contributed as well. The Office also relies on the support of the Government of Romania, which continues to provide rent-free office space.

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

Achievements

Criminal justice capacities

Over the reference period, C-PROC implemented activities to strengthen criminal justice capacities in particular in the currently 35 priority countries that are eligible for a broad range of assistance. Over 80 other countries participated in at least some of the activities.

[16] 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.

These activities focused typically on:

- domestic legislation on cybercrime and electronic evidence as well as on data protection;
- 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;
- mainstreaming of judicial training on cybercrime and e-evidence;
- public/private co-operation, in particular between service providers and criminal justice authorities;
- international co-operation, including on streamlining mutual assistance procedures, request templates and other tools, and strengthening of 24/7 points of contact.

By nature, such activities contribute to 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").

Examples of specific activities are:

- **CyberEast**: The development of policies and legislative reforms featured strongly in all Eastern Partnership states (except Belarus). This is complemented by the launch of public opinion surveys on cybercrime and cybersecurity. The project reinforced capacities of criminal authorities and interagency co-operation via a series of online discussions on data protection, development of standard operating procedures, numerous training sessions and practical exercises. Some 68 activities were supported by this project in the past year.

- **CyberSouth**: The legal frameworks for the protection of personal data in priority countries (Algeria, Jordan, Lebanon, Morocco and Tunisia) were assessed and further recommendations were prepared with the support of the project. Materials for judicial training were developed in Algeria, Lebanon and Tunisia. Capacities for police-to-police co-operation and judicial co-operation on cybercrime and e-evidence were reinforced and the development of strategies against cybercrime was promoted in priority countries. Some 62 activities were supported by this project in the past year.

- **GLACY+**: Legislative reforms and policy reviews on cybercrime, electronic evidence and data protection were supported with a focus on countries of Africa, Asia, Pacific and Caribbean (examples are Belize, Botswana, Burkina Faso, Côte D'Ivoire, the Gambia, Fiji, Kiribati, Maldives, Mauritius, Mozambique, Namibia, Nigeria, Papua New Guinea, Sierra Leone, Sudan and Tonga). Regional co-operation in Africa was enhanced through the organisation of the Second African Forum. This Forum also further promoted the use of the Budapest Convention in Africa. GLACY+ contributed significantly to the consolidation of the community of judicial trainers and to the creation of an International Network of Judicial Trainers on cybercrime and electronic evidence. Some 128 activities were supported by this project in the past year.

- **iPROCEEDS-2**: A Guide on seizing cryptocurrencies was produced and quickly became a "toolbox" for investigators internationally. The knowledge of magistrates on investigating online child sexual exploitation was increased through online training courses. The mutual legal assistance process was improved through a regional specialised judicial training course on international co-operation and follow-up through regional and domestic workshops. The project supported over 90 activities in the past year.

- **EndOCSEA@Europe**: The knowledge and capacities of criminal justice authorities were increased through a Pilot training on online child sexual abuse and exploitation for judges, prosecutors and the national police in the Republic of Moldova. The regional conference on improving operational capacities to tackle online child sexual exploitation and abuse (OCSEA) presented the training module for law enforcement, judges and prosecutors; it was translated into 11 languages and is made available upon request. Some 25 activities were supported by this project in the past year. The project ended in June 2021.

- **Cybercrime@Octopus** and the follow-up **Octopus project:** These supported the expansion of capacity-building activities and legislative amendments to the Caribbean region (Barbados, Guyana, Montserrat, Jamaica, Saint Lucia, Suriname and Trinidad and Tobago), as well as additional countries of Africa and Asia. A series of webinars was launched along with other activities on Covid-19 related cybercrime in Asia. Action against online child sexual exploitation and abuse was promoted through the preparation of country profiles and a regional workshop for Asia. Particular attention was paid to raising awareness of cybercrime threats among policy makers through joint activities with other partners (Parliamentary webinars). Some 72 activities were supported by these projects in the past year.

Guides and tools

C-PROC, also in partnership with other international organisations (for example INTERPOL), developed a number of guides and tools on matters related to cybercrime and electronic evidence (recent examples include a "guide on criminal justice statistics on cybercrime", the above-mentioned "guide on cryptocurrencies" and a "guide for first responders to cybercrime investigations"). These guides were then used in domestic workshops or as reference documents, for example, when developing domestic standard operating procedures.

The guides provide practitioners with practical tools for cybercrime investigations and prosecutions and for the handling of electronic evidence based on international good practices. They also permit C-PROC to provide more consistent support to criminal justice authorities in different countries.

Cybercrime and related legislation

The strengthening of domestic legislation on cybercrime and electronic evidence is an important component of all projects. As a result, numerous countries either adopted such legislation or advanced with their reforms between October 2020 and September 2021. C-PROC maintains a database of legislation on cybercrime in countries worldwide. For example, the latest cursory overview of the "Global state of cybercrime legislation" shows that by June 2021, 124 states (or 64% of UN members) had substantive criminal law provisions in place broadly corresponding to those of the Budapest Convention. This represents an increase of 18 states since February 2020. Examples include Belize, Congo, Fiji, Mozambique, South Africa, Vanuatu or Zambia. Most of these had benefitted from C-PROC assistance.

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

Moreover, C-PROC in co-operation with the Council of Europe's Data Protection Unit supported reforms of legislation on data protection in line with Convention "108+" in a number of countries (see below).

Synergies

Capacity building creates synergies and C-PROC activities continued to be carried out in partnership with multiple organisations, among them the European Union, EUROJUST, EUROPOL, the European Cybercrime Training and Education Group (ECTEG), 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 (IAP), INTERPOL, the Organization of American States, the Pacific Island Law Officers Network (PILON), the United Nations, the US Department of Justice, the US Department of State, 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 European Union (El PAcCTO, SIRIUS, OCWAR_C) that have cybercrime and e-evidence among their topics for ensuring the promotion of the similar international policies on cybercrime. C-PROC is thus well connected to large networks of experts and institutions in all regions of the world and recognised as key partner.

Synergies are also created with other Council of Europe instruments. GLACY+, CyberEast and CyberSouth assisted several countries in the implementation of capacity-building activities on data protection in line with Convention “108+”, such as in Armenia, Georgia, Republic of Moldova and Algeria, Colombia, Ethiopia, the Gambia, Jordan, Lebanon, Morocco, Namibia, Peru, Thailand, Tunisia and others.

EndOCSEA@Europe was implemented by the Children’s Rights Division with the support of C-PROC and is an illustration of the synergies between the Budapest and Lanzarote Conventions. The online resource on “cyberviolence” is an example of synergies of the Budapest, Lanzarote and Istanbul Conventions.

4. Conclusions

Impact

The Cybercrime Programme Office of the Council of Europe, between October 2020 and September 2021, continued to produce an impact on criminal justice capacities and legislation on cybercrime and electronic evidence based on the Budapest Convention, in countries in all regions of the world.

C-PROC responded to Covid-19 related restrictions by improving its technical and human resources and its competencies for the online delivery of activities, and was thus able to implement nearly 400 activities in this period.

Through the Cybercrime Programme Office, the Council of Europe continues to play a leading role for capacity building on cybercrime and electronic evidence. Synergies with relevant organisations and projects further increased during the past 12 months.

Numerous activities focused on the strengthening of data protection legislation and systems to ensure that effective responses to cybercrime will be accompanied by human rights and rule of law safeguards.

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 be successful to ensure impact and innovation. With the forthcoming Second Additional Protocol, the Budapest Convention is likely to remain the most relevant international standard on cybercrime for years to come. Capacity building has been and will remain a major factor for increased membership in the Convention and its Protocols.

Priorities

Specific priorities for the forthcoming 12 months include:

- To support the opening for signature and subsequent implementation of the Second Additional Protocol to the Convention on Cybercrime. A conference on “enhanced co-operation on cybercrime and electronic evidence” is to be organised under the Octopus Project in Strasbourg on 29 and 30 March 2022. It would permit the opening for signature of the Protocol.

- To support the strengthening of human rights, rule of law and data protection safeguards in countries participating in project activities. This includes in particular support to the implementation of Convention “108+”.

- To further improve capabilities for the online delivery of activities. Priorities in 2022 include the launch of the C-PROC platform for e-learning and the delivery of judicial training online.

- To further promote synergies of the Budapest Convention with relevant Council of Europe instruments, including its first Protocol on Xenophobia and Racism (CETS 189) as well as the Data Protection (CETS 223), Lanzarote (CETS 201) and Istanbul (CETS 210) Conventions, the Convention on Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198) and MONEYVAL regarding cryptocurrencies. Further synergies with other organisations will also be sought.

- To prepare the extension of current projects and to mobilise additional resources. The current portfolio of projects covers priority regions in Europe as well as countries committed to implementing the Budapest Convention in other parts of the world. Some projects will come to an end in the near future, and follow-up will be required:

    - an extension of the GLACY+ project by 42 months with a top-up of EUR 5.5 million is in preparation;
    - the extension of the CyberEast project by 18 months with a top-up of EUR 1.08 million Euros has been prepared and is expected to be approved soon;
    - the project CyberSouth was scheduled to end in December 2021 but a no-cost extension of 24 months has been agreed in principle;
    - new project proposals will be developed in the course of 2022.