COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Information Documents

SG/Inf(2023)1

9 January 2023

Council of Europe Office on Cybercrime in Bucharest:

C-PROC activity report for the period October 2021 – December 2022

Contents

Executive summary

The Cybercrime Programme Office of the Council of Europe (hereinafter “C-PROC” or “the Office”) in Bucharest, Romania, is responsible for ensuring 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 present report is to inform the Committee of Ministers of the activities of the Office from October 2021 to December 2022.

In this period, C-PROC operated, *inter alia,* against the background of increasing challenges of cybercrime and e-evidence, including the proliferation of ransomware attacks. The Russian aggression against Ukraine raised further challenges related to cybercrime and e-evidence. The United Nations (UN) process aimed at a new international treaty on “countering the use of information and communications technologies for criminal purposes” commenced (February 2022). During this period, the Convention on Cybercrime completed 20 years of global impact (20th anniversary of the Convention in November 2021) and the new Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) was opened for signature (May 2022).

By December 2022, C-PROC was one of the largest external offices of the Council of Europe, with a cumulative budget of over EUR 39 million for active projects and 38 staff. The Office continues to rely on external funding. More than 90% of its budget is covered by voluntary contributions or European Union (EU) contributions to joint projects. The EU remained the main donor through joint projects co-funded by the Council of Europe. The United States of America also made major financing available. Other donors during this period were Hungary, Italy, the Netherlands, the United Kingdom, Canada and Japan. The Office benefits from the support of the Government of Romania which provides rent-free office space.

C-PROC supported some 420 activities under five projects involving more than 130 countries between October 2021 and December 2022 focusing on:

- domestic legislation in line with the Convention on Cybercrime and its protocols, as well as related standards (data protection, the protection of children);
- criminal justice capacities (for the investigation, prosecution and adjudication of cybercrime and the use of e-evidence) for financial investigations, for addressing ransomware attacks, for interagency and international co-operation;
- guides, online resources and other tools and exercises for practitioners;
- public/private co-operation and co-operation between criminal justice and cybersecurity institutions;
- participation of experts from Parties to the Convention in the UN treaty process;
- specific support to Ukraine.

The Office maintained its reputation as a centre of excellence on cybercrime and further consolidated the Council of Europe’s position as a global leader for capacity building on cybercrime and e-evidence.

Support by C-PROC is a major factor ensuring the success of the Convention. The accessions to the Convention by Nigeria and Brazil and the invitations to accede to Côte d’Ivoire, Ecuador, Fiji, Timor Leste, Trinidad and Tobago as well as Vanuatu during this period are also a result of C-PROC activities.

The formula of the Convention on Cybercrime and its protocols as the common standard backed up by the Cybercrime Convention Committee (T-CY) and capacity building through C-PROC continues to ensure impact, synergies and innovation. With its new Second Additional Protocol, the Convention on Cybercrime is likely to remain the most relevant international mechanism on cybercrime for years to come.

With several projects coming to an end in 2023, new projects need to be designed and funding secured to ensure the continued success of this formula beyond next year.

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 (hereinafter "C-PROC" or "the Office") in Bucharest, Romania, during the period October 2021 to December 2022.[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 on 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 Convention on Cybercrime (ETS No. 185) and related standards, (b) follow-up and assessments by the Cybercrime Convention Committee (T-CY) and (c) capacity building.

2. Context

Challenges of cybercrime and electronic evidence

Cybercrime – that is, offences against and by means of computer systems – represents a significant threat to fundamental rights, democracy and the rule of law, as well as to international peace and stability, and it has major social and economic impact. The Covid-19 pandemic has accelerated since early 2020 the digital transformation of societies, thus offering more opportunities for criminal exploitation.

Current challenges include:

- *A proliferation of ransomware offences*: these typically consist of the encryption of computer data or systems, thus locking out users, followed by requests for ransom against the (promise of) access to be restored. Offenders may also threaten to release sensitive or personal information to extract payments from victims. The "WannaCry" and "NotPetya" attacks of 2016/2017 affected computers and attracted major attention worldwide. During the Covid-19 pandemic in 2020 and 2021, healthcare institutions, including research facilities developing vaccines, were victims of ransomware attacks. Businesses of all sizes, individuals, as well as the public sector are targeted by ransomware. In April and May 2022, the government of Costa Rica had to declare a national emergency following ransomware attacks. Public institutions in Montenegro were targeted in August 2022 and in Albania in September 2022.

- In response:

  - C-PROC supported a number of activities to assist criminal justice authorities through workshops during the Octopus Conference in November 2021, an international training course on ransomware investigations for authorities

[1] The decision setting up the Office requested the Secretary General to present such annual reports.
Note: in order to align reporting periods with calendar years, the present report covers the period October 2021 to December 2022.
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.

[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.

from 34 countries in May 2022, an international exercise on ransomware investigations and prosecutions in Türkiye in July 2022, the development of a guide on ransomware investigations and a joint international conference with EUROJUST on this topic in November 2022.

- Furthermore, the T-CY decided in May 2022 to prepare a Guidance Note to explain how the provisions of the Convention on Cybercrime and its Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) can be used to criminalise, investigate, prosecute and co-operate against ransomware-related offences. This Guidance Note was adopted in November 2022. The tools of the Convention and its new Second Additional Protocol are thus available to counter ransomware offences.[4]

- *The use of virtual currencies to obfuscate criminal money flows, including for the payment of ransom*. In response:

  - a guide on seizing cryptocurrencies was developed in 2021 by C-PROC under the iPROCEEDS-2 project;
  - a series of training courses on cryptocurrency and dark net investigations was delivered in South-Eastern Europe and Türkiye between January and May 2022 under the iPROCEEDS-2 project;
  - C-PROC is co-operating with MONEYVAL[5] in a typology exercise on practices related to virtual assets and virtual asset service providers.

- *Obtaining e-evidence for use in criminal proceedings*: all types of crime, not only cybercrime, may entail evidence on computer systems. Such evidence may be in foreign, multiple or unknown jurisdictions, and obtaining such volatile evidence is a complex challenge. In response:

  - the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence was finalised and opened for signature in May 2022;
  - synergies were sought with other Council of Europe treaties and mechanisms related to criminal matters, so that these may benefit from the procedural and co-operation tools of the Convention on Cybercrime and the new Protocol[6];
  - numerous capacity building activities on e-evidence, including the tools of the new Protocol, were organised.

---

[4] Costa Rica signed the Second Additional Protocol to the Convention in June 2022 while making specific reference to the ransomware attacks that it had suffered in the previous months.

[5] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

[6] 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 Convention on Cybercrime and its Second Additional Protocol at their disposal. Examples range from the Criminal Law Convention on Corruption (ETS No. 174) to the conventions and/or protocols on money laundering and financing of terrorism (CETS No. 198), trafficking in human beings (CETS No. 197), terrorism (ETS No. 190, CETS No. 196 and CETS No. 217), protection of children against sexual exploitation and abuse (CETS No. 201), violence against women (CETS No. 210), counterfeiting of medical products (CETS No. 211), manipulation of sports competitions (CETS No. 215) and trafficking in organs (CETS No. 216).
Regarding synergies, see the studies on:
- Online and technology-facilitated trafficking in human beings
- Protecting women and girls from violence in the digital age – The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women.

See also the online resource on “cyberviolence”.

The Russian aggression against Ukraine

The Russian aggression against Ukraine has been preceded and is accompanied by cyberattacks against the critical infrastructure of Ukraine and other forms of cybercrime.[7] Evidence not only of such offences, but also of war crimes may take the form of e-evidence.[8]

In response, C-PROC under the CyberEast joint project with the European Union (EU):

- assisted in amendments to the domestic criminal law to increase the effectiveness of criminal justice action against cyberattacks;
- supported training on the use of open source intelligence (OSINT) and e-evidence in war crime proceedings;
- reviewed legislation on the admissibility of OSINT in criminal proceedings;
- provided training on ransomware offences;
- provided advanced training on cybercrime and e-evidence to Ukrainian judges.

Following the onset of the Russian aggression, C-PROC also assisted in the evacuation of Council of Europe staff and their families, as well as of counterparts from Ukraine to or via Romania.

20 years of the Convention on Cybercrime

The Convention on Cybercrime was opened for signature in Budapest, Hungary, on 23 November 2001. On the occasion of the 20th anniversary of the Convention, an Octopus Conference and special event were organised from 16 to 18 November 2021 in co-operation with the Hungarian Chairmanship of the Committee of Ministers.[9] More than 30 ministers and other senior officials intervened in the special event. About 1,200 cybercrime experts from some 120 countries – including from public sector, but also international and private sector organisations, civil society organisations and academia – participated in the conference.

The special event and the Octopus Conference confirmed the impact of the Convention worldwide over the past 20 years.[10] The updated survey on the "Global state of cybercrime legislation" published in December 2022 showed how the Convention has shaped the criminal law of over 80% of all states.[11]

By December 2022, 68 states had become Parties to the Convention (the most recent ones being Brazil and Nigeria). A further 15 states had signed it or been invited to accede to the Convention. During the past year – also as a result of C-PROC activities on domestic legislation – Côte d'Ivoire, Ecuador, Fiji, Timor Leste Trinidad and Tobago, as well as Vanuatu were invited to accede. By the end of 2022, additional requests for accession were being processed.

---

[7] See for example:
https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[8] See for example:
https://www.justiceinfo.net/en/93111-insights-digital-revolution-war-crimes-probes-ukraine.html
https://www.euronews.com/next/2022/04/06/how-digital-evidence-of-war-crimes-in-ukraine-is-being-collected-verified-and-stored
https://www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/

[9] Octopus conference 2021 (coe.int) The meetings were held online due to the Covid-19 pandemic.

[10] https://rm.coe.int/octopus-conference-2021-key-messages-v18nov2021/1680a494e6

[11] https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan-2023-public-v1/1680a99137
See also the "country wikis" and legal profiles at the Octopus Platform
https://www.coe.int/en/web/octopus/home

The first Additional Protocol to the Convention on Acts of Xenophobia and Racism Committed via Computer Systems (ETS No. 189)[12] had 33 Parties by the end of 2022. A further 12 had signed it. In January 2023, this Protocol will celebrate its 20th anniversary.

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence[13]

Considering the proliferation of cybercrime and the increasing complexity of obtaining e-evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, additional tools are needed for a more effective criminal justice response and to permit governments to meet their positive obligation to protect individuals against crime.

Therefore, the T-CY negotiated a new Protocol to the Convention on Cybercrime between 2017 and 2021. On 12 May 2022, this Second Additional Protocol was opened for signature. 22 states signed on that occasion, two others in May and June 2022, and a further six on 30 November 2022.[14]

The Protocol provides for effective tools for enhanced co-operation and disclosure of e-evidence with a strong system of rule of law and data protection safeguards:

- 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 mutual assistance");
- mutual assistance tools ("video-conferencing", "joint investigation teams and joint investigations");
- data protection safeguards to permit the flow of personal data under the Protocol.

With this Protocol, the Convention on Cybercrime will remain relevant and effective. 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.

C-PROC facilitated the preparation of the Protocol under the project Cybercrime@Octopus and the subsequent Octopus Project.[15] Following the opening for signature, C-PROC projects organised numerous activities to share information on the tools of this new treaty, and are now assisting countries in the implementation of the Protocol.

It was important that the Protocol was completed prior to the UN treaty process.

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

By adopting Resolution 74/247[16] in December 2019, the United Nations General Assembly (UNGA) established the "open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of

[12] Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of racist and xenophobic nature committed through computer systems.
[13] The Protocol can be found here.
[14] The chart of signatures and ratifications can be found here.
[15] Support to the T-CY, including co-funding, is (was) part of these projects.
[16] The Resolution had been proposed by the Russian Federation.

information and communications technologies for criminal purposes". In May 2021, the UNGA adopted the modalities of this treaty process through Resolution 75/282. In total, six negotiation sessions of two weeks each are foreseen to take place in New York and Vienna and to finalise the draft treaty by February 2024.

Following a first session in New York (February/March 2022)[17], the second one was held in Vienna (May/June) and the third one in New York (August/September 2022).

C-PROC supported the participation of experts from Parties to the Convention on Cybercrime and Observers to the TC-Y in these sessions in order to ensure consistency of a future treaty with the provisions of the Convention and observance of human rights and rule of law requirements.

One insight from the three sessions so far is that the Convention on Cybercrime serves as the standard of reference and that proposals for provisions of the future UN treaty which are based on those of the Convention on Cybercrime are most likely to find agreement. A second insight is that the UN treaty process appears to enhance the attraction of and interest in accession to the Convention on Cybercrime.

3. Overview of projects and achievements between October 2021 and December 2022

Current projects

In the period from October 2021 to December 2022, C-PROC supported approximately 420 activities under the following projects:

Project title	Duration	Budget	Funding
GLACY+ project on Global Action on Cybercrime Extended[18]	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 (Canada, Hungary, 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 – June 2023[19]	EUR 4.95 million	EU/CoE JP (10% OB)
CyberSouth on capacity building in the Southern Neighbourhood	July 2017 – Dec 2023	EUR 5 million	EU/CoE JP (10% OB)
CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region	June 2019 – Dec 2023	EUR 5.33 million	EU/CoE JP (10% OB)

From March 2022 onwards, with the gradual lifting of Covid-19-related restrictions, these were held either as in-person, hybrid or online formats.

[17] This first session started on 28 February 2022, that is, four days after the start of the Russian aggression against Ukraine.
[18] Note: In November 2022, the EU Commission and the Council of Europe signed an additional contribution agreement for a new project Global Action on Cybercrime Enhanced (GLACY-e) with a budget of EUR 5.56 million starting in August 2023 and scheduled to end in February 2026.
[19] Note: no-cost extension to December 2023 agreed in principle by the European Commission.

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

By December 2022, the combined budgets of projects underway amounted to some EUR 39.2 million (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).

The Office relies on external funding. During the past year, more than 90% of its budget was funded by extra-budgetary resources, i.e. voluntary contributions and EU contributions to joint projects. The EU remained the main donor through joint projects co-funded by the Council of Europe. The United States of America also made major funding available. Hungary, Italy, the Netherlands, 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 the Octopus Project is fully funded by voluntary contributions, joint projects with the EU include 10% co-funding from the budget of the Council of Europe.

While funding available for 2023 seems to be appropriate, major additional resources will need to be mobilised in the coming months:

- the return to in-person activities (in combination with online and hybrid formats) means that cost of activities is increasing; this is compounded by current economic trends (rising cost for travel, inflation, fall-out from the Russian aggression against Ukraine);
- the number of states reaching out for support by projects implemented by C-PROC has been and will keep increasing considerably;
- several projects will come to an end in 2023.

Proposals for possible follow-up projects are made in the “conclusions” below.

Achievements

Criminal justice capacities

Between October 2021 and December 2022, C-PROC contributed significantly to the strengthening of criminal justice capacities, in particular in the currently 40 priority countries that are eligible for a broad range of assistance. Over 90 other countries participated in at least some of the activities.

Capacity building support generated by the Office is based on the Convention on Cybercrime and also reinforces the work of the T-CY. Project activities focused typically on:

- domestic legislation on cybercrime and e-evidence, as well as on data protection and 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;
- mainstreaming of 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 on streamlining mutual assistance procedures, request templates and other tools, and strengthening of 24/7 points of contact.

Such activities contribute 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").

Examples of specific activities are:

- **CyberEast**: Policies on cybercrime in all Eastern Partnership states (except Belarus) were reinforced by findings of public opinion surveys (Cyber Barometer). Work on legislation with project countries continued in view of the requirements of the Second Additional Protocol to the Convention, with Moldova and Ukraine signing it in November 2022. The project reinforced capacities of criminal justice authorities and interagency co-operation via series of trainings on financial investigations, advanced e-evidence and forensics, and co-operative Regional Cyber Exercises, with dedicated sessions on cybercrime reporting and access to data in the private sector. Targeted support to Ukraine included work to ensure the admissibility of evidence, support to legal reforms, developing practical skills on combating ransomware and use of open-source intelligence for investigations. 72 activities were supported by this project in this period.

- **iPROCEEDS-2**: Capacities of law enforcement authorities were enhanced through specialised training on investigation of cyberattacks, ransomware, virtual currencies, darknet, paralleled with financial investigations exercises. Closer links between magistrates, investigators, the cybersecurity community and the private sector were achieved by supporting public/private meetings at domestic level, with a focus on co-operation between criminal justice authorities and service providers. The capabilities of judges and prosecutors to handle complex cybercrime cases were strengthened through sustainable judicial training on cybercrime, e-evidence, international co-operation, online crime proceeds and the certification of training skills. The thirrd edition of the Underground Economy Conference, in co-operation with Team CYMRU, capped around 500 representatives from law enforcement agencies, the cyber security community, private industry and academia across the globe to share case studies and new tools to handle cybercrime threats. The project supported some 84 activities in this period.

- **CyberSouth**: Sustainable judicial capacities to address cybercrime in all priority countries (Algeria, Jordan, Lebanon, Morocco, Tunisia) were reinforced through the finalisation of a series of training courses on international co-operation and e-evidence, and the delivery of the training of trainers course to magistrates, with the aim to establish a pool of national experts that can be involved in future educational activities on cybercrime. Support to national judicial training institutions was also provided to integrate educational programmes on cybercrime and e-evidence into their curricula. The promotion of domestic toolkits for first responders in law enforcement agencies contributed to improve the quality and efficiency of cybercrime investigations (Algeria, Jordan, Lebanon, Morocco and Tunisia). Strategic approaches to address cybercrime continued to be supported through online discussions and recommendations on the collection and analysis of statistical data on cybercrime. Advice was provided to Jordan in view of aligning domestic legislation more closely with the Convention on Cybercrime. The project supported some 76 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 (Colombia, Ecuador, Fiji, Nauru, Panama, Philippines, Uganda and Uruguay) and data protection (Chile, Ecuador, The Gambia, Vanuatu). Series of webinars on the universality and implementation of the Convention on Cybercrime (with Parliamentarians for Global Action), and on the Second Additional Protocol to the Convention (with the International Association of Prosecutors) served to promote knowledge and use of the Convention and cement the project's partnerships with regional and international organisations. Dedicated activities in Colombia, Brazil, Belize and Uruguay enhanced dialogue between policymakers and practitioners. Continuing the focus on building technical capacities of law enforcement authorities, advisory workshops on the search, seizure and confiscation of online crime proceeds implemented by the project partner INTERPOL in Nigeria, Ghana, Chile, Paraguay and the Philippines increased countries' knowledge on parallel financial investigations. International cooperation was strengthened though series of annual events focused on scenario-based exercises on data preservation, mutual legal assistance, parallel financial investigation, and other cooperative mechanisms for Africa and Latin America. Two new courses were piloted in Africa and Latin America: train the trainers for ECTEG first responders course and FOSI training, with plans to expand the delivery to other regions in 2023. GLACY+ further deepened its focus on judicial training through national training workshops in Benin, Cabo Verde, Ghana, Mauritius, Panama, Paraguay, Senegal, Sierra Leone and Sri Lanka, and a series of practitioner-to-practitioner workshops organised within the framework of C-PROC's International Network of National Judicial Trainers. Two major events were held in Costa Rica in November 2022 in co-operation with the Octopus Project, notably the Americas Forum on Cybercrime and the international Conference on Women and Cybercrime. Some 180 activities were supported by the project in this period.

- **Octopus Project:** The opening for signature of the Second Additional Protocol to the Convention on Cybercrime supported by the Octopus Project in co-operation with other C-PROC projects in May 2022 provided parties to the Convention on Cybercrime with new opportunities for enhanced co-operation and disclosure of e-evidence. A series of dedicated webinars, including multistakeholder roundtables in Latin America, raised awareness and acceptance of the protocol in view of its prospective accession by states. Improved policy dialogue and digital partnerships on cybercrime were fostered through the exchange of views with the diplomatic community, a series of parliamentary webinars and other activities underlining the importance of the free, open and global internet and respect of human rights and rule of law requirements. Legislation and capacities of countries to address the challenge of cybercrime and e-evidence, Covid-19 related cybercrime, cyber-violence (including online child sexual exploitation and abuse and gender-based cyberviolence) were the focus of activities with Barbados, Nauru and other Caribbean, Latin American and Asian countries. Translated training materials were made available through the Octopus Platform, and the newly launched HELP course on Cybercrime and Electronic Evidence became an important tool enabling criminal justice authorities and legal practitioners worldwide to increase their knowledge on the topic. A dedicated online training platform envisaged to be fully operational in early 2023 is meant to add to the toolkit at the disposal of countries worldwide. Dialogue was fostered within the Cybercrime Convention community: support to T-CY plenaries, the Working Group on undercover investigations and extension of searches, the celebration of the 20th Anniversary of the Convention on Cybercrime and the Octopus conference further strengthened the membership, reach and impact of this treaty. 112 activities were supported by this project in this period.

Guides for practitioners

C-PROC, also in partnership with other international organisations, develops guides and tools on matters related to cybercrime and e-evidence. Such guides provide practitioners with practical tools for cybercrime investigations and prosecutions and for the handling of e-evidence based on international good practices. They also permit C-PROC to provide more consistent support to criminal justice authorities in different countries. Between October 2021 and December 2022, the following additional guides were developed under C-PROC projects:

- Version 3.0 of the Council of Europe Electronic Evidence Guide provides guidance to criminal justice professionals on how to identify, handle, seize and secure e-evidence, with an update on new technologies and devices such as drones and cryptocurrencies.

- C-PROC published the Guide on Law Enforcement Training Strategies on Cybercrime and E-evidence that was prepared in co-operation with INTERPOL.

- A Guide for the investigation of ransomware offences was finalised in December 2022.

Online training platform on cybercrime and e-evidence

Prior to the Covid-19 pandemic, most capacity building efforts supported by C-PROC involved classic on-site activities. Following the onset of the pandemic, C-PROC turned to delivering activities online. It has become clear that even with the lifting of Covid-19-related restrictions and the return to onsite activities, digital learning formats are here to stay.

C-PROC is therefore preparing an online training platform on cybercrime and e-evidence, which is to be launched by early 2023 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.

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 is maintaining information on developments regarding legislation in “country wikis” and “legal profiles” at the Octopus Platform and is carrying out a regular survey on the global state of cybercrime legislation.[20] For example, by January 2022, 128 states (or two-thirds of UN members) had substantive criminal law provisions in place broadly corresponding to those of the Convention on Cybercrime. This represents an increase of 22 states within two years (i.e. since February 2020).

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 Cooperation (EUROJUST), the EU Agency for Law Enforcement Cooperation (EUROPOL), the EU Agency for Law Enforcement Training (CEPOL), the EU Institute for Security Studies, the African Union Commission, the

[20] https://rm.coe.int/3148-1-3-4-cyberleg-global-state-jan2022-p/1680a564bb
https://www.coe.int/en/web/octopus/home

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[21], Parliamentarians for Global Action (PGA), the Organisation of American States (OAS), the Pacific Island Law Officers Network (PILON), the United Nations, the United States Department of Justice, the United States 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 EU (CyberNet, El PAcCTO, SIRIUS, OCWAR-C) that have cybercrime and e-evidence among their topics for ensuring the promotion of similar international policies on cybercrime. C-PROC remains 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 and actions, for example by supporting capacity building activities on data protection in line with the modernised Convention for the protection of individuals with regard to the processing of personal data (hereinafter "Convention 108+")[22], or on the protection of children against the sexual exploitation and sexual abuse in line with the Lanzarote Convention, the creation of the online resource on cyberviolence, or support to typology studies on money laundering.

4. Conclusions

Impact

C-PROC produced again important impact on criminal justice capacities and legislation on cybercrime and e-evidence based on the Convention on Cybercrime in all regions of the world through some 420 activities, involving over 130 countries between October 2021 and December 2022. With the work of the C-PROC, the Council of Europe remains a global leader for capacity building in this field.

Partnership and synergies with other stakeholders and drawing on related Council of Europe standards (for example on data protection or the protection of children) helped multiply the impact.

While C-PROC projects have a clear focus on an effective criminal justice response based on the Convention on Cybercrime and its protocols and with the necessary human rights, rule of law and data protection safeguards, the approach proved to be sufficiently pragmatic and flexible to address emerging challenges. In the past year, for example, this included support to Ukraine, addressing ransomware attacks, or reinforcing links between cybersecurity and criminal justice responses.

The number of countries aligning their domestic legislation with and seeking accession to the Convention on Cybercrime kept increasing during this period.

By ensuring participation of experts from parties to the Convention on Cybercrime in the UN treaty process, more UN member states have become aware of the benefits of the Convention, thus generating more interest in it.

The opening for signature of the Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence further increased the attraction of the Convention

[21] 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.
[22] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

on Cybercrime. With this new instrument, the Convention will remain the most relevant international agreement on cybercrime in the foreseeable future. The Convention with its protocols, explanatory reports and guidance notes is available in a single compilation. Furthermore, special editions have been prepared to document the process of the negotiation of the Convention on Cybercrime and of the Second Additional Protocol.

The formula of the Convention on Cybercrime as the common standard, backed up by the T-CY and capacity building through C-PROC, continued to be a successful algorithm to ensure impact and innovation.

The demands on C-PROC for capacity building keep increasing:

- The growing number of countries requesting accession to the Convention on Cybercrime means that more countries will require support to ensure that their legislation meets the requirements of the Convention (including safeguards), that they have the capacity to apply such legislation and that they are able to co-operate with other parties.

- The opening for signature of the Second Additional Protocol means that signatories need to be supported in the implementation of this instrument in terms of legislation and capacities.

- Support is required to address emerging challenges (for example, related to ransomware, virtual currencies, cyberviolence, war crime and cybersecurity).

The return to in-person activities (in combination with online and hybrid formats) means that cost of activities is increasing. This is further compounded by current economic trends.

At the same time, three projects are scheduled to end in 2023 (projects iPROCEEDS-2, CyberSouth and CyberEast). Additional resources need to be secured to sustain the current approach.

Priorities

Specific priorities for the forthcoming 12 months therefore include:

- To ensure that countries invited to accede to the Convention on Cybercrime have the necessary legislation and capacities in place, in line with the provisions of this treaty prior to actual accession.

- To support signature, ratification and implementation of the Second Additional Protocol to the Convention on Cybercrime.

- To promote the first Additional Protocol to the Convention on Cybercrime on Xenophobia and Racism Committed via Computer Systems. Its 20th anniversary in January 2023 will provide an opportunity.

- To assist criminal justice authorities to address current challenges related to ransomware attacks, cryptocurrencies, use of open source intelligence and e-evidence in proceedings related to war crimes (Ukraine) and to enhance their co-operation with bodies responsible for cybersecurity.

- 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 promote synergies of the Convention on Cybercrime with relevant Council of Europe instruments, including its first Additional Protocol to the Convention on Xenophobia and Racism Committed via Computer Systems as well as the Data Protection[23], Lanzarote[24] and Istanbul[25] Conventions, the Convention on Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism[26] and MONEYVAL (regarding cryptocurrencies). Further partnerships and synergies with other organisations will also be sought.

- To prepare new projects, or the extension of ongoingprojects, and to mobilise the necessary resources. The current portfolio of projects covers priority regions in Europe, as well as countries committed to implementing the Convention on Cybercrime in other parts of the world. Some projects will come to an end in the near future, and follow-up will be required to ensure impact beyond 2023:

  - Prepare for launch in January 2024:

    - a new project on cybercrime, financial investigations and the Second Additional Protocol covering South-eastern Europe and Türkiye (as follow up to iPROCEEDS-2 or in the form of a cost extension of this project);
    - a new project CyberEast (or cost-extension) covering Armenia, Azerbaijan, Georgia, Moldova and Ukraine (as follow-up to the current CyberEast project);
    - a new project to follow up to the CyberSouth project (currently covering Algeria, Jordan, Lebanon, Morocco and Tunisia).

  - Further expand the Octopus Project and mobilise additional resources.

[23] Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS No. 223).
[24] Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).
[25] Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210).
[26] Convention on Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).