Information Documents

SG/Inf(2019)38

Strasbourg, 19 November 2019

The Council of Europe Office on Cybercrime in Bucharest

C-PROC activity report for the period October 2018 – September 2019

Contents

1. Background and purpose of this report 3
2. Cybercrime – the approach of the Council of Europe 4
3. Summary of projects and results in the period October 2018 – September 2019 5
3.1 Overview of current projects 5
3.2 Cybercrime@Octopus 6
3.3 Cybercrime@EAP 2018 – International and public/ private co-operation 8
3.4 CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region 8
3.5 iPROCEEDS project targeting proceeds from crime on the Internet in South-eastern Europe 9
3.6 CyberSouth project on cybercrime and e-evidence in the Southern Neighbourhood region 11
3.7 GLACY+ Project on Global Action on Cybercrime Extended 12
3.8 EndOCSEA@Europe project to End Online Child Sexual Exploitation and Abuse in Europe 15
4. Impact 17
5. Conclusions and priorities 19
6. Appendix: Inventory of activities supported by C-PROC (October 2018 – September 2019) 22

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) in Bucharest, Romania, during the period October 2018 to September 2019.[1]

In October 2013, the Committee of Ministers[2] decided to establish a Programme Office on Cybercrime in Bucharest, Romania, as the Council of Europe's response to the need for capacity-building on cybercrime and electronic evidence. In the same decision, it invited the Secretary General to report annually on the activities of this Office and its costs, including a proposal regarding the continuation of its functioning.

This decision followed an offer by the Government of Romania and a proposal by the Secretary General in spring 2013.[3] The Cybercrime Programme Office of the Council of Europe (C-PROC) became operational in April 2014.

The objective of the Office is to ensure the implementation of the capacity-building projects on cybercrime of the Council of Europe in all regions of the world.[4] This includes:

- identification of needs for capacity-building in the area of cybercrime;
- advice, support and co-ordination in planning, negotiation and timely implementation of targeted Council of Europe activities on cybercrime, including joint programmes with the European Union and other donors;
- establishment of partnerships against cybercrime with public and private sector organisations;
- co-operation with the authorities of Romania in matters regarding cybercrime;
- fund-raising activities for specific projects and programmes.

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 the Memorandum of Understanding signed in October 2013.

The Secretariat of the Cybercrime Convention Committee (T-CY) – and thus the intergovernmental part of the Council of Europe's work on cybercrime – remains in Strasbourg.

[1] For the report covering April 2014 to September 2015 see https://rm.coe.int/168047d1b8
For the period October 2015 to September 2016 see https://rm.coe.int/16806b8a87
For the period October 2016 to September 2017 see this report
For the period October 2017 to September 2018 see this report
[2] On 9 October 2013, at their 1180th meeting.
[3] SG/Inf(2013)29
[4] See SG/Inf(2013)29 and MoU between the Council of Europe and the Government of Romania, signed on 15 October 2013.

By September 2019, C-PROC had 30 staff funded from project budgets, with the exception of the Head of Office, who is also the Executive Secretary of the T-CY and divides his time between Strasbourg and Bucharest. This arrangement ensures that activities of the T-CY and C-PROC remain closely linked.

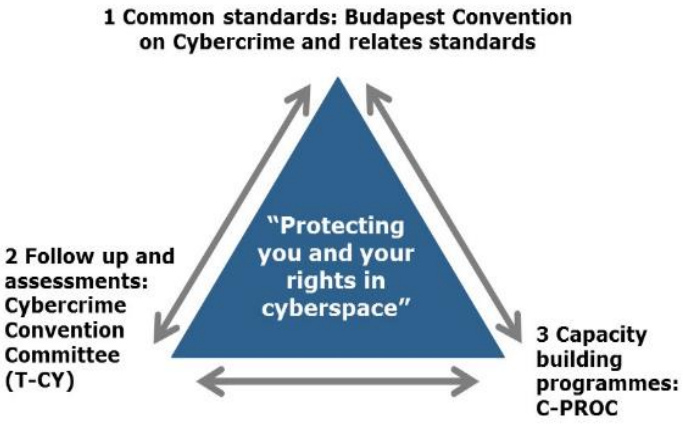
The 5th Anniversary of C-PROC was celebrated in conjunction with the international conference on "Criminal Justice in Cyberspace" – jointly organised by the Council of Europe and the Romanian Presidency of the Council of the EU – in Bucharest from 25 to 27 February 2019, with the participation of the Deputy Secretary General. It confirmed the impact made by the Office in terms of membership and level of implementation of the Budapest Convention on Cybercrime, the strengthening of legislation worldwide on the basis of this treaty, sustainable judicial and law enforcement training programmes on cybercrime and electronic evidence, improved international co-operation, including through 24/7 points of contact, as well as partnerships and synergies with a large number of organisations.

2. Cybercrime – the approach of the Council of Europe

Cybercrime – as offences against and by means of computer systems – has evolved into a major threat to fundamental rights, democracy and the rule of law, as well as international peace and stability and has a major economic impact. Along with this, the question of evidence on computer systems ("electronic evidence") has gained in significance and complexity.

Any crime – be it fraud, attacks against media, parliaments, election systems or public infrastructure, child abuse or other forms of sexual exploitation, the theft of personal data, racism and xenophobia, money laundering or terrorism – is likely to entail cybercrime or electronic evidence.

This issue is thus closely linked to the core objectives of the Council of Europe, that is, the promotion of human rights, democracy and the rule of law.



The Council of Europe's approach to these challenges consists of a "dynamic" triangle of three interrelated elements:

- The Budapest Convention on Cybercrime (ETS 185), which was opened for signature in 2001[5], remains the most relevant international agreement on this issue. By September 2019, 64 states were Parties and a further eight had signed or been invited to accede. The Budapest Convention is thus one of the most successful treaties of the Council of Europe in terms of membership;

[5] Complemented by the Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of 2003.

- The Cybercrime Convention Committee (T-CY) carries out assessments of the implementation of the Convention by the Parties, adopts Guidance Notes and maintains working groups to identify responses to emerging challenges. With currently 73 member and observer states[6] as well as 12 observer organisations, the T-CY is one of the main intergovernmental bodies on cybercrime internationally. Its current main focus is the preparation of an Additional Protocol to the Convention on Cybercrime on enhanced international co-operation and access to evidence in the cloud;

- Capacity-building on cybercrime has been an essential element of the approach of the Council of Europe from 2006 onwards. Discussions at the level of the United Nations in early 2013[7] confirmed broad international agreement on capacity-building as an effective way ahead to help societies meet the challenges of cybercrime and electronic evidence. This argument – which in 2013 led to establishment of C-PROC – remains valid today. It was further confirmed in a recent report of the UN Secretary General to the 74th Session of the United Nations General Assembly.

3. Summary of projects and results in the period October 2018 – September 2019

Since its establishment, C-PROC's primary objective has been "to ensure the implementation of capacity-building projects on cybercrime of the Council of Europe"[8]. Concretely, it assists, through capacity-building projects, countries worldwide in the strengthening of their criminal justice capacities on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime and related standards.[9]

3.1 Overview of current projects

In the period October 2018 to September 2019, C-PROC supported approximately 240 activities[10] under the projects listed below.

By September 2019, the combined budget of projects underway amounted to EUR 32.3 million. This represents a further increase compared to previous years.[11]

While Cybercrime@Octopus and EndOCSEA@EUROPE are fully funded by voluntary contributions, joint projects with the European Union have 10% co-funding from the budget of the Council of Europe (approximately EUR 2.7 million).

---

[6] 64 Parties, 8 signatories or states invited to accede as well as the Russian Federation.

[7] Meeting of the UN Intergovernmental Expert Group on Cybercrime, Vienna, February 2013.

[8] SG/Inf(2013)29 and CM decision from 9 October 2013, at their 1180th meeting.

[9] Such as the Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), and others.

[10] See Appendix for the list of activities.

[11] September 2015: EUR 6 million, September 2016: EUR 22 million, September 2017: EUR 24.4 million, September 2018: EUR 26.7 million.

List of projects (October 2018 – September 2019)

Project title	Duration	Budget	Funding
Cybercrime@Octopus	Jan 2014 – Dec 2020	EUR 4 million	Voluntary contributions (Estonia, Hungary, Monaco, Netherlands, Romania, Slovak Republic, UK, Japan, USA and Microsoft)
Cybercrime@EAP 2018 on international and public/ private co-operation in the Eastern Partnership region	Jan 2018 – Dec 2018	EUR 0.98 million	EU/CoE JP (Partnership for Good Governance)
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2021	EUR 13.35 million	EU/CoE JP
iPROCEEDS project targeting proceeds from crime on the Internet in South-eastern Europe and Turkey	Jan 2016 – Dec 2019	EUR 5.56 million	EU/CoE JP
EndOCSEA@EUROPE project against Online Child Sexual Exploitation and Abuse	July 2018 – Dec 2020	EUR 0.85 million	End Violence against Children Fund
CyberSouth on capacity-building in the Southern Neighbourhood	July 2017 – June 2020	EUR 3.33 million	EU/CoE JP
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

3.2 Cybercrime@Octopus

Cybercrime@Octopus is a global project funded by voluntary contributions. It is designed to assist any country requiring support in a pragmatic manner, in particular with regard to the preparation of legislation.

Activities between October 2018 and September 2019 included, for example:

- Ghana – a series of workshops for senior judges and members of Parliament in October 2018. This facilitated the accession of Ghana to the Budapest Convention in December 2018.
- Niger – Advisory mission on legislation in December 2018. This resulted in the adoption of domestic legislation in line with the Budapest Convention and a decision to accede to this treaty in 2019.

- Mauritania – Review of legal framework and analysis of capacity-building needs in December 2018.
- Kazakhstan – Workshop (December 2018) followed by a review of domestic legislation on cybercrime and e-evidence.
- Guatemala – Advisory mission on legislation in January 2019. This resulted in the submission of draft legislation in line with the Budapest Convention to Congress in August 2019 and a decision to accede to this treaty.
- Georgia – Support to an integrated strategy on cybercrime and cybersecurity in February 2019.
- Ivory Coast – T-CY visit to review domestic legislation against the Budapest Convention in March 2019. This resulted in a political decision to seek accession to the Budapest Convention.
- Guinea (Conakry) – Review of domestic legislation against the Budapest Convention in April 2019. This confirmed the need to reform domestic legislation.
- Benin – T-CY visit to review domestic legislation against the Budapest Convention in April 2019. This resulted in a request for accession during the visit and a subsequent invitation to accede to the Budapest Convention.
- The Gambia – Workshop on data protection legislation in line with Convention 108 in May 2019.
- Qatar – Review of domestic legislation (Doha, June 2019). This resulted in a set of proposals for reform of legislation in line with the Budapest Convention.
- Judicial and law enforcement training, *inter alia*, in Nigeria (December 2018, February 2019), Chile (November 2018) or Costa Rica (February 2019).

These examples illustrate the impact that capacity-building projects can make in terms of legislation, rule of law safeguards and skills of criminal justice authorities.

The objectives of Cybercrime@Octopus include support to the Cybercrime Convention Committee (T-CY).

A major event, in this respect, was the international conference on "Criminal Justice in Cyberspace" – jointly organised by the Council of Europe and the Romanian Presidency of the Council of the EU in Bucharest from 25 to 27 February 2019, which resulted in a set of key messages and which provided a better understanding of the work on the 2nd additional Protocol to the Budapest Convention.

In addition, the project co-funded meetings of the T-CY and in particular of the Protocol Drafting Groups (November 2018, February 2019, March 2019, May 2019, July 2019 and September 2019). This meant that the work on the 2nd Additional Protocol could proceed without delay in spite of the financial difficulties of the Organisation during this period.

The project has so far been funded by Estonia, Hungary, Monaco, Netherlands, Romania (in-kind), Slovak Republic, United Kingdom, Japan, USA and Microsoft, with the USA being the main contributor.

Overall, Cybercrime@Octopus is a flexible tool to respond to needs, strengthen legislation, promote multi-stakeholder partnerships and support the T-CY in a pragmatic manner. It

remains a resource to which donors can contribute to action against cybercrime and support the T-CY at any time without lengthy lead time for project design and approval.

3.3 Cybercrime@EAP 2018 – International and public/ private co-operation

Cybercrime@EaP 2018 was a one-year project that built on previous activities in the Eastern Partnership region. It ended in December 2018.

Between October and December 2018, Cybercrime@EaP 2018 focused on the development of practical skills for investigators, mutual legal assistance authorities and 24/7 points of contact. Technical courses on Network Investigations and Live Data Forensics, held regionally in co-operation with the European Cybercrime Training and Education Group (ECTEG), were highlights in October.

A series of practical table-top exercises on international co-operation, testing practical tools (such as Octopus Cybercrime Community) and ("Article 29-31") templates for co-operation in real-life case scenarios were also competed in this period.

Regional Cyber Drills at the Cyber Week Republic of Moldova 2018 further improved practical skills of co-operation between law enforcement officers working on cybercrime and CSIRT/CERT members working on cybersecurity on a number of issues, such as incident handling, malware analysis and protection of critical infrastructure.

The Closing Conference of the project adopted two regional reports on Threats and Challenges of Cybercrime in the Eastern Partnership and an updated Study on Cybercrime and Cybersecurity Strategies in the Eastern Partnership region.

The six-month gap between the end of the project Cybercrime@EAP 2018 and the new project CyberEast was partially filled by the project Cybercrime@Octopus.

3.4 CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region

The joint EU/Council of Europe project CyberEast ("Action on Cybercrime for Cyber Resilience in the Eastern Partnership region") formally commenced on 20 June 2019 and the Launching Conference was held in Brussels in September 2019.

The project covers Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine. The objective is "to increase and enhance cyber-resilience and criminal justice capacities of the Eastern Partnership countries to better address the challenges of cyber threats and improve their overall security".

This 3-year project reinforces previous achievements such as legislative frameworks implementing the Budapest Convention on Cybercrime, enabling efficient regional and international co-operation, and improving public/ private co-operation regarding cybercrime and electronic evidence in the Eastern Partnership region.

However, it also features enhancing the operational capacities of cybercrime units, increasing accountability, oversight and public visibility of law enforcement action on cybercrime, as well as strengthening interagency co-operation on cybercrime and electronic evidence, in particular by improving information-sharing by Computer Security Incident Response Teams (CSIRTs) with relevant authorities.

During the inception phase of CyberEast a series of assessment visits to each Eastern Partnership country on the institutional setup, capacities, competencies and training needs of cybercrime units as well as interagency co-operation commenced in September 2019.

3.5 iPROCEEDS project targeting proceeds from crime on the Internet in South-eastern Europe

The iPROCEEDS joint project of the Council of Europe and the European Union covers Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Turkey and Kosovo*[12] and is aimed at strengthening the capacity to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet. It has a budget of EUR 5.56 million and lasts from January 2016 to December 2019. Components include:

- Public reporting systems;
- Legislation;
- Co-operation between cybercrime, financial investigation and financial intelligence units;
- Guidelines and indicators for detection of online fraud and money laundering on the Internet;
- Public/ private information sharing;
- Judicial training;
- International co-operation.

iPROCEEDS thus follows up on recommendations of a joint MONEYVAL/Global Project on Cybercrime typology study of 2012.

Between October 2018 and September 2019, iPROCEEDS further increased the skills and capacity of cybercrime and financial investigators, digital forensics specialists, prosecutors and representatives of Financial Intelligence Units (FIUs) in the search, seizure and confiscation of the proceeds of online crime. The project delivered a number of specialised training sessions and workshops such as Network Investigations, Online Financial Fraud and Credit Card Fraud, Online Undercover Investigations. Moreover, to adequately equip law enforcement officers with tools to investigate cybercrime offences, access to Free Forensic Tools for the Law Enforcement Community (FREETOOL) was facilitated. On the basis of an agreement of the Council of Europe with University College Dublin (UCD), the tools were provided to the Parties of the Convention on Cybercrime for further distribution and use within their respective agencies.

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

The Project supported the studies of law enforcement officers in a long-distance Master programme on Forensic Computing and Cybercrime Investigation, offered by University College Dublin, Ireland. Ten students have successfully graduated the programme. It ran for 24 months and covered modules such as Computer Forensics, Financial Investigation Techniques – Following the Money, Network Investigations, Mobile Devices Investigation, Live Data Forensics, VoIP and Wireless Investigations and others.

Strengthening criminal justice authorities' capacities with respect to inter-agency and international co-operation for the search, seizure and confiscation of the proceeds of online crime remained the main objective of the Project. Three simulation exercises on cybercrime and financial investigations were organised in Tirana, Albania (4-7 March 2019), Belgrade, Serbia (8-11 April 2019) and Ankara, Turkey (6-9 May 2019). Cybercrime and financial investigators, digital forensics specialists, prosecutors and money laundering analysts from the FIUs undertook investigations on the Darknet, virtual currencies and co-operated within the framework of joint investigation teams (JITs). Participants established closer links between various professional communities in a real-time environment at both national and international levels for the investigation of cybercrime and its financial gains.

iPROCEEDS worked towards strengthening international co-operation between cybercrime units as well as between competent authorities for judicial co-operation by testing international co-operation in the framework of a table-top exercise and acquiring solid understanding on how to use formal and informal co-operation channels in cybercrime investigations. This led to a better understanding of direct judicial co-operation, the need to use templates and online tools, and increased coordination between judicial and police-to-police co-operation processes. An important result of these efforts was the translation by the project countries of the standard templates approved by the T-CY for requests under Articles 29 (data preservation) and Article 31 (access to stored data) under the Budapest Convention. Their use will increase the efficiency of the 24/7 points of contact and mutual legal assistance authorities in their corresponding proceedings under these provisions.

iPROCEEDS took the lead in organising the Underground Economy Conference 2019 which was co-hosted in September 2019 by the Council of Europe at its premises in Strasbourg, France. This prominent international information security event brought together around 450 representatives from law enforcement agencies, the cyber security community, private industry and academia from across the globe. It was opened by the Deputy Secretary General.

In 2019, the Project continued supporting judicial training programmes on cybercrime, electronic evidence and the proceeds of online crime. National delivery of the judicial introductory training courses on cybercrime, electronic evidence and the proceeds of online crime took place in Kosovo* (19-22 February 2019), Montenegro (11-12 March 2019 and 15-16 April 2019), Bosnia and Herzegovina (22-25 April 2019), Albania (11-12 March 2019 and 13-14 May 2019 and 12-13 June), Turkey (14-17 May 2019) and North Macedonia (17-18 and 28-29 October 2019). Around 150 judges, prosecutors, legal associates and candidates increased their skills and knowledge required to fulfil their respective roles and functions in cases of cybercrime, electronic evidence and search, seizure and confiscation

of the proceeds of online crime. The training module was delivered by national trainers and organised in co-operation with national training institutions. Moreover, in co-operation with other projects the first International Conference of National Judicial Trainers Network on Cybercrime and Electronic Evidence was organised, which brought together training institutions and national trainers from around the world to determine the needs and priorities related to training on cybercrime and electronic evidence and reflect on the benefits, feasibility and steps to be taken regarding the set-up of a network of national judicial trainers on cybercrime and electronic evidence.

3.6 CyberSouth project on cybercrime and e-evidence in the Southern Neighbourhood region

The CyberSouth joint project of the Council of Europe and the European Union covers the Southern Neighbourhood region with Algeria, Jordan, Lebanon, Morocco and Tunisia as initial priority countries. It has a duration of 36 months (July 2017 – June 2020) with a budget of EUR 3.33 million.

The objective is to strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements. It focuses on cybercrime legislation, specialised police services and interagency co-operation, judicial training, 24/7 points of contact and international co-operation, as well as cybercrime policies. The launching conference was held in Tunis in March 2018.

In Year Two of its implementation, CyberSouth has emerged as a major partner supporting the five priority countries in the co-operation on cybercrime and electronic evidence.

Project actions ranged from regional reflections on the elaboration of national situation reports on cybercrime and electronic evidence, to dedicated legislative advice workshops, judicial and law enforcement training and finally participation of countries in international fora related to cybercrime, which in turn led to changes with a long-term impact on international co-operation.

CyberSouth organised 52 activities (domestic/ regional/ international) targeting priority countries from October 2018 to September 2019. The project had started with an inception phase of eight months, without any history of co-operation with four out of the five countries, (the exception being Morocco). This marks an important achievement: the trust and commitment of countries to co-operate with the Council of Europe not only to benefit from activities but also to contribute and gain the same standards and capabilities in the co-operation on cybercrime and e-evidence as other European States.

A hundred reference magistrates were trained on the topic and working groups were established to develop domestic courses on cybercrime and electronic evidence for initial and in-service training.

Law enforcement agencies of priority countries were given the opportunity to update their working procedures and practices by taking part in workshops and training activities, *inter*

alia on business email compromise and credit card fraud, live data forensics, darkweb and cryptocurrencies, undercover online investigation, OSINT (open source intelligence) investigations and malware analysis.

These agencies contributed to the adaptation of the E-First course (developed by the European Cybercrime Training and Education Group, ECTEG), an e-learning first responder course on cybercrime and e-evidence in Arabic. This was complemented by support to a strategic approach to law enforcement capacity-building on cybercrime and e-evidence aimed at making competencies and skills available at national and regional levels.

While Morocco is already a Party to the Convention and Tunisia has been invited to accede, Lebanon and Jordan also made major progress in aligning their legislation with the standards of the Budapest Convention. Most importantly, the competent authorities in Lebanon and Jordan show that they have understood the importance of becoming a party to such an international agreement, which provides a legal basis for the expedited exchange of information crucial for investigations on cybercrime and e-evidence.

3.7 GLACY+ Project on Global Action on Cybercrime Extended

Building on the experience of GLACY, the Council of Europe and the European Union agreed to follow up through the GLACY+ project on "Global Action on Cybercrime Extended". The project technically commenced in March 2016 with an initial duration of four years and a budget of EUR 10 million.

Given its impact and expanding needs following accession requests or accessions to the Budapest Convention (Cabo Verde, Nigeria, Chile, Costa Rica), interest in accession and needs for assistance by other countries (Burkina Faso, the Gambia, Nepal, Samoa, Uganda, Vanuatu and others), the budget was increased to EUR 13.35 million in March 2018 and its duration extended to February 2021. By September 2019 a further increase and extension was under consideration.

GLACY+ comprises three components:

1. To promote the adoption and implementation of consistent cybercrime legislation, policies and strategies;

2. To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police co-operation with each other as well as internationally with cybercrime units in Europe and other regions;

3. To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international co-operation.

INTERPOL – under an agreement with the Council of Europe – is a partner and is leading the implementation of the law enforcement component of the project. Other project partners

include Estonia (Ministry of Justice), France (Ministry of Interior), Romania (National Police, Prosecution Service (DIICOT) and Ministry of Justice), United Kingdom (National Crime Agency) and the USA (Department of Justice) as well as Europol (European Cybercrime Centre – EC3).

Between October 2018 and September 2019, GLACY+ supported some 96 activities involving more than 80 countries worldwide.

During this period a strong focus was put on the strengthening of legislation. Advisory missions on legislation were carried out to Costa Rica, Guatemala, Kenya, Mexico, Namibia, Sierra Leone, and The Gambia.

A feature of GLACY+ is to seek synergies with other international organisations and programmes:

- A major event to this effect was the first African Forum on Cybercrime with the participation of 300 delegates from 52 African countries. It was co-organised with the African Union Commission and a number of regional and international organisations, including UNODC, INTERPOL, the Commonwealth Secretariat, the World Bank, as well as the United Kingdom's Foreign and Commonwealth Office, the United States Department of Justice and the US Department of State.

- Co-organisation of the 3rd meeting of the Cybercrime Working Group of the Pacific Island Law Officers Network (PILON) in Vanuatu May 2019 in co-operation with the PILON Secretariat and Australia. This contributed to reforms of domestic legislation in six Pacific Island States.

- Co-operation was developed with FOPREL (Forum of Presidents of the Legislative Powers of Central America and the Caribbean Basin) through a regional workshop and an exchange of letters. This permitted to reach out to national Parliaments of the region and to raise awareness on aligning domestic legislations on cybercrime and electronic evidence with the Budapest Convention.

- Joint international conference of Eurojust and the Council of Europe in Investigation of online Child Abuse in the Darknet at the end of September 2019.

- Synergies with other EU-funded projects active in complementary subject areas and similar geographies (namely OCWAR-C, Cyber4D and EL PAcCTO), through coordination meetings with relevant project management units and European Commission counterparts. Coordination with Europol's project SIRIUS was also ensured.

- Other activities in this line were participation in the EU Cyber Forum by all GLACY+ priority countries, work on a joint Council of Europe – EU Fundamental Rights Agency Handbook on Cybercrime and Fundamental Rights, contributions to GFCE (Global Forum on Cybercrime Expertise) and the ICANN Public Safety Working Group.

International co-operation and the sharing of good practices was fostered through a number of regional and international meetings. For example, the Dominican Republic hosted events for Caribbean countries, Cabo Verde for the Prosecutors' Offices of all Portuguese-speaking countries, Chile hosted the Ibero-American Network of Cyber Prosecutors ("CiberRede") meeting, and Nigeria was the host of the African Regional Workshop on Cybercrime, National Cybersecurity and Internet Piracy.

In addition, international events were held to enhance the technical skills of cybercrime investigators of GLACY+ countries:

- the INTERPOL Workshop on channels and avenues for international co-operation in cybercrime;
- Training of trainers on cybercrime and electronic evidence for first responders from African Gendarmeries;
- the INTERPOL Malware analysis training.

Capacities of the judiciary and the prosecution services were reinforced through introductory and advanced judicial courses in Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Indonesia, Mauritius, Nigeria and Sri Lanka. In several events, the pool of trainers consisted partially or fully of judges, magistrates or prosecutors previously trained under GLACY and GLACY+ activities. Some of the trainers also introduced the Council of Europe training programme to their peers from neighbouring countries, with judicial courses being organised in the Philippines for the ASEAN region and in Senegal for French and Portuguese speaking countries of the ECOWAS region.

With the aim of creating a network of such trainers, an international meeting of national and international judicial trainers on cybercrime and electronic evidence, trained under Council of Europe's programmes, was held in Strasbourg. Training needs and new courses, certification programs and the feasibility of an international network of judicial trainers were discussed.

Moreover, the integration of training modules in the curricula of judicial training institutions and the mainstreaming of mutual legal assistance procedures was facilitated in Costa Rica, the Dominican Republic and Ghana.

Finally, law enforcement capacities were reinforced with the support of INTERPOL, as implementing partner of the project, through workshops/ training on cybercrime investigations, electronic evidence and international co-operation in Singapore (with participation of all GLACY+ countries), Dominican Republic, Philippines and Tonga.

Operational advice was provided through technical missions on the development of cybercrime investigation units and data forensics units in Nigeria and Cabo Verde and on the integration of ECTEG training materials into the law enforcement training plan in Tonga. Other law enforcement capacities were reinforced by technical trainings and courses on INTERPOL tools and services in Cabo Verde, Colombia, Ghana, Hong Kong, Mauritius, Morocco, Nigeria, Senegal and Sri Lanka.

In conclusion, during this period the GLACY+ project made an impact in terms of:

- Implementation of provisions of and awareness of the advantages of the Budapest Convention;
- International co-operation and synergies with a wide range of relevant organisations and projects;
- Reinforcement of capacities worldwide through judicial and law enforcement training on cybercrime and electronic evidence.

3.8 EndOCSEA@Europe project to End Online Child Sexual Exploitation and Abuse in Europe

The project End Online Child Sexual Exploitation and Abuse @ Europe (EndOCSEA@Europe) is implemented by the Council of Europe's Children's Rights Division with the support of the C-PROC programme office. The project benefits all of the 47 Council of Europe member states, with a focus on Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Republic of Moldova, Montenegro, Serbia, Turkey and Ukraine. The project is financed by the Fund to End Violence Against Children (EVAC), has a duration of 30 months (July 2018 – December 2020) and a budget of EUR 849,041.

The aims of the project are to:

- strengthen multidisciplinary collaboration at national and regional levels, through national governance structures and situation analyses of OCSEA risks and responses;
- support legislative and procedural reforms, training and capacities building for law enforcement officials, judges and prosecutors for end to end victims' support;
- address societal capabilities through awareness-raising, education of key target groups and the empowerment of children.

This project is implemented in the framework of the Council of Europe's Strategy for the Rights of the Child (2016 - 2021), contributing to the implementation of two priority areas: the right of the child to a life free from violence and the rights of the child in the digital environment.

During the period October 2018 to September 2019, the project, among other things:

- Provided support to signatory states to the Lanzarote Convention to facilitate participation in the Lanzarote Committee meeting, 5 - 7 March 2019.

- Endorsed[13] Armenia, Azerbaijan and Ukraine as pilot countries for project activities including gap analyses and training module development.

- Analysed responses to prevent and combat online child sexual exploitation and abuse at national and regional level, a baseline mapping of Council of Europe member states responses and a comparative review of collective mechanisms available at pan-European level are due for publication in November 2019.

- Undertook research into legislation, policies and practices to prevent and combat online child sexual exploitation in Armenia, Azerbaijan and Ukraine. Fact-finding visits and workshops with relevant ministries and authorities took place in Azerbaijan, Armenia and Ukraine between June and September. The findings and recommendations of the Gap analysis will be published in November 2019.

- Engaged in a dialogue with civil society organisations with a view to strengthening their capacities and contributions to the implementation and monitoring mechanism set out by the *Lanzarote Convention*. 35 civil society organisations active in 20 member states took part in an international conference on 8 - 9 April 2019 in Strasbourg, France.

- Adopted strategic priorities to strengthen multi-sectorial co-operation to prevent and combat online child sexual exploitation and abuse at an International conference held on 16 - 17 May 2019, in Strasbourg, which gathered over 70 participants from 22 countries.

- Awarded grants to civil society organisations in the Republic of Moldova, Serbia, and Ukraine and Human Rights Defender's Office in Montenegro, to develop awareness raising tools and activities. Over 5,000 children and 42 schools will participate in workshops and campaigns, while five information and advocacy tools will be developed by July 2020.

- Developed a child-friendly version of the *Lanzarote Convention*, through child participation, due for publication in November 2019.

- Raised awareness about project activities and participation of experts from focus countries in other relevant events such as OECD conference on the Protection of Children in a Connected World (Zurich, October 2018), Regional Conference on Cybercrime Strategies (Tbilisi, December 2018), Eurojust joint conference on online investigations: Dark web and online child abuse (The Hague, September 2019), ENOC 23rd Annual Conference on Children's rights in the digital environment (Belfast, September 2019).

[13] by the project steering group, including representatives from each of the 10 countries in focus.

4. Impact

C-PROC has supported some 850 activities in the five and a half years since April 2014, when it became operational, and some 240 between October 2018 and September 2019.

Some 40 priority countries have benefitted from a large menu of support, and an additional approximately 100 countries participated in regional or international activities or benefited from specific assistance such as advice on legislation.

It would be beyond the scope of the present report to analyse the impact of all these activities, for example, in terms of investigations, prosecutions, adjudications or levels of international co-operation.

However, a few points may illustrate the impact of C-PROC:

- Increased membership of the Budapest Convention: Since 2014, 23 additional States became Parties to this treaty (Andorra, Argentina, Cabo Verde, Canada, Chile, Costa Rica, Ghana, Greece, Israel, Liechtenstein, Mauritius, Monaco, Morocco, Panama, Paraguay, Peru, Philippines, Poland, San Marino, Senegal, Sri Lanka, Tonga, Turkey), others have been invited to accede (Benin, Nigeria, Tunisia), and further requests for accession were in the process of consultation by September 2019. While European States would have joined sooner or later anyway, C-PROC capacity-building was a primary factor for additional membership by most non-European countries.

- Impact on legislation: C-PROC, under several projects, closely follows developments regarding legislation on cybercrime and electronic evidence worldwide since 2013. The latest update was prepared in June 2019. Results indicate that by June 2019, more than half of all UN member states had their substantive criminal law largely in line with the Budapest Convention. Good progress was also made in terms of procedural powers. By June 2019, 152 States (79% of UN members) seemed to have used the Budapest Convention as a guideline or at least as a source when developing domestic legislation. In Africa, Asia-Pacific and Latin America this is largely due to capacity-building activities.

Substantive criminal law provisions in line with Budapest Convention

	States	Largely in place by January 2013		Largely in place by June 2019	
All Africa	54	6	*11%*	18	*33%*
All Americas	35	10	*29%*	15	*43%*
All Asia	42	13	*31%*	18	*43%*
All Europe	48	38	*79%*	45	*94%*
All Oceania	14	3	*21%*	4	*29%*
All	**193**	**70**	***36%***	**100**	***52%***

Specific procedural powers to secure electronic evidence

	States	Largely in place by January 2013		Largely in place by June 2019	
All Africa	54	5	*9%*	15	*28%*
All Americas	35	5	*14%*	12	*34%*
All Asia	42	8	*19%*	13	*31%*
All Europe	48	31	*65%*	40	*83%*
All Oceania	14	1	*7%*	3	*21%*
All	**193**	**50**	***26%***	**82**	***43%***

- Safeguards strengthened: Given the need to reconcile effective criminal justice with rule of law safeguards, C-PROC is not only supporting reforms of criminal law but also data protection legislation with the Data Protection Convention 108 and its Protocols. To this effect, C-PROC is drawing on the expertise of the Data Protection Unit at the Council of Europe. Examples are Kenya, Nigeria, Sri Lanka and the Dominican Republic. It is therefore no coincidence that currently 49 of the 64 Parties to the Budapest Convention are also Parties to Convention 108.

- Synergies increased: A major concern for many years has been that organisations carrying out capacity-building lacked coordination and coherence, or that they were competing against each other.[14] Seeking partnerships and synergies is thus a feature of C-PROC and is reflected in joint projects with the European Union, co-operation with Eurojust and Europol, agreements with INTERPOL, the African Union Commission, ECOWAS or FOPREL, with institutions in Parties to the Budapest Convention such as Estonia, France, Romania, United Kingdom and USA, participation in ICANN or the Global Forum on Cyber Expertise, and many others. The Forum for Africa (Ethiopia, October 2018), the PILON meeting for Pacific Island States (May 2019) or the Eurojust/Council of Europe Conference on child abuse in the Darknet (September 2019) are examples of how such co-operation is of benefit to criminal justice authorities on the ground.

- Sustainable training: C-PROC is supporting sustainable training programmes that can produce lasting impact. With regard to judicial training, in numerous priority countries the sequencing consisted of:

  1. Training the trainers of domestic training academies;
  2. Adapting training modules to domestic needs;
  3. Assisting trained trainers in the delivery of pilot courses;
  4. Inserting modules into the regular curricula of training academies;

  In July 2019, an additional element was initiated, that is, the creation of a network of trained judicial trainers on cybercrime and e-evidence.

[14] This was raised, *inter alia* in multiple Octopus Conferences (see for example Octopus 2011)

In short, experience from the past five and a half years since the establishment of C-PROC confirms that capacity-building is an effective way to help societies in any part of the world address the key challenges of cybercrime. Capacity-building on cybercrime and e-evidence:

- works, responds to needs and makes an impact in terms of criminal justice action on cybercrime and e-evidence with rule of law safeguards;
- facilitates multi-stakeholder co-operation;
- has human development benefits and feeds into UN Sustainable Development Goals;
- helps reduce the digital divide;
- is based on broad international support and may help overcome political divisions.

5. Conclusions and priorities

The following conclusions can be drawn:

- Between October 2018 and September 2019, the Office supported approximately 240 activities under seven projects covering priority regions in Europe as well as countries in other regions of the world committed to implementing the Budapest Convention. Officials from more than 120 countries were involved in project activities during this period.

- During these twelve months, the Office further improved its performance in terms of quality, effectiveness, outcome and impact. Activities supported by C-PROC made an impact in terms of membership and level of implementation of the Budapest Convention, the strengthening of legislation worldwide on the basis of this treaty, sustainable judicial and law enforcement training programmes on cybercrime and electronic evidence, improved international co-operation including through 24/7 points of contact as well as partnerships and synergies with a large number of organisations.

- Through the Cybercrime Programme Office, the Council of Europe remains a global leader for capacity-building on cybercrime and electronic evidence. C-PROC is a confirmation that capacity-building is producing impact and is an effective way to help societies in any part of the world address the key challenges of cybercrime.

- The “dynamic triangle” combining agreed-upon standards (Budapest Convention), with follow up through the T-CY and capacity-building through C-PROC is a distinctive feature of the Council of Europe and remains highly effective. C-PROC projects are supporting implementation of the Budapest Convention and follow up or contribute to the work of the Cybercrime Convention Committee. Given the recent budgetary challenges of the Council of Europe, it was most valuable that the T-CY could rely on voluntary contributions through the project Cybercrime@Octopus. The T-CY and the preparation of the 2nd Additional Protocol to the Budapest Convention were thus not affected by the financial difficulties that the Council of Europe encountered during this period.

- The Budapest Convention is among the Council of Europe treaties with broadest membership and global reach. With each new Party, the Budapest Convention and international co-operation on cybercrime will become more effective. As all but one member state are Parties or Signatories, additional Parties will be non-member states of the Council of Europe. Between October 2018 and September 2019, Argentina, Cabo Verde, Ghana, Morocco, Paraguay and Peru became Parties. The Office contributes to ensuring that prospective and actual Parties have the capacity to apply the Budapest Convention.

- C-PROC remains one of the most successful external offices of the Council of Europe with regard to resource mobilisation. Large numbers of activities are being carried out by C-PROC and are generating impact in an efficient and cost-effective manner. This makes the Office attractive to donors. By September 2019, projects with a volume of more than EUR 32 million were underway.

- The European Union remains the main donor through joint projects co-funded by the Council of Europe. Between October 2018 and September 2019 voluntary contributions have also been received from Netherlands, United Kingdom, Japan and the USA to the project Cybercrime@Octopus.

- The Government of Romania not only makes office premises available rent free, but also provides support through expertise. The Ministry of Justice, the National Police, the Prosecution Service (DIICOT), the National Institute of Magistracy and the Computer Emergency Response Team contribute in substance to project activities.

- Several other States (Estonia, France, Germany, United Kingdom and the USA) as well as the European Cybercrime Centre at Europol (EC3) and INTERPOL are also partners in one or more projects. Numerous project activities are carried out in partnership with or involving a wide range of public and private sector organisations.

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

- Feeding the dynamic triangle of Budapest Convention, T-CY and capacity-building: C-PROC to facilitate accession by additional States to the Budapest Convention and to support the T-CY in the preparation of the 2nd Additional Protocol. Once the Protocol is adopted, to support implementation by Parties to the Convention.

- Emphasis on human rights and rule of law safeguards: C-PROC projects to support the development of specific legislation with safeguards, standardised procedures and a strong emphasis on the training of judges. Continue to support the development of data protection legislation in line with the modernised Data Protection Convention 108 in co-operation with the Data Protection Unit of the Council of Europe.

- Enhancing the expertise of the Office: the role of C-PROC as a centre of subject-matter knowledge to be further increased through training materials, tools and online resources as well as monitoring of legislative developments worldwide.

- Resource mobilisation: 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 of these projects will come to an end within a few months and follow up will be required:

  - follow up to iPROCEEDS on online criminal money flows in South-eastern Europe as the current project is scheduled to end in December 2019;

  - follow up project to Cybercrime@Octopus (ending in December 2020) to be funded by voluntary contributions. This is to include support to the work of the Cybercrime Convention Committee;

  - GLACY+ expansion in terms of budget and duration to respond to growing requests for assistance and accessions to the Budapest Convention;

  - extension of CyberSouth for the Southern Neighbourhood as the current project is scheduled to end in June 2020;

  - new project on Xenophobia and Racism (CybercrimeXR) to support implementation of the Protocol to the Budapest Convention on Cybercrime;

  - follow up to EndOCSEA@Europe to provide for a broader range of capacity-building measures for the protection of children against sexual violence online (the current project is ending in December 2020).

- Synergies and partnerships: these features will be further enhanced through co-operation with external organisations (for example by adding a component to GLACY+ in support of regional training institutions) but also within the Council of Europe (for example through activities related to Lanzarote, Istanbul or Trafficking Conventions).

In sum, the aim is for C-PROC to further continue to evolve in terms of quality, expertise, impact and synergies for global co-operation on cybercrime and e-evidence.

6. Appendix: Inventory of activities supported by C-PROC (October 2018 – September 2019)

October 2018

iPROCEEDS	Second National Delivery of the Introductory Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Bihać, Bosnia and Herzegovina, 1-4 October 2018
CyberCrime@EAP 2018	ECTEG Course on Network Investigations, Yerevan, Armenia, 1-5 October 2018
CyberSouth	Advanced training of magistrates on cybercrime and electronic evidence, Rabat, Morocco, 1-5 October 2018
GLACY+ Cybercrime@Octopus	Data Protection Legislation Workshop, Nairobi, Kenya, 2-5 October 2018
iPROCEEDS Cybercrime@Octopus	Regional Forum on Online Fraud, Zagreb, Croatia, 4-5 October 2018
GLACY+	Advisory mission on cybercrime legislation & Advisory mission on national policies and strategies on Cybercrime, San Jose, Costa Rica, 8-11 October 2018
CyberSouth	Workshop on the Budapest Convention in Jordan, Amman, Jordan, 8-9 October 2018
CyberCrime@EAP 2018	OSCE Conference on Preventing and Countering Terrorism in the Digital Age, Minsk, Belarus, 9-10 October 2018
CyberCrime@EAP 2018	Table-top exercise on international co-operation on cybercrime, Minsk, Belarus, 11-12 October 2018
CyberCrime@EAP 2018	Meeting on further capacity-building on cybercrime in the Eastern Partnership region, Bucharest, Romania, 12 October 2018
CyberCrime@EAP 2018	Table-top exercise on international co-operation on cybercrime, Tbilisi, Georgia, 15–16 October 2018
GLACY+	INTERPOL Cybercrime Investigation Training for African Region, Nairobi, Kenya, 15-19 October 2018
iPROCEEDS	ECTEG regional training on Malware Investigations in co-operation with the Department of Cybercrime, Turkish National Police, Ankara, Turkey, 15-19 October 2018
GLACY+ CyberSouth Cybercrime@Octopus	African Forum on Cybercrime: Policies and Legislation, International Co-operation and Capacity-building, Addis Ababa, Ethiopia, 16-18 October 2018
iPROCEEDS	Meeting of the working group to elaborate/ improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment, Sarajevo, Bosnia and Herzegovina 18 October 2018
CyberCrime@EAP 2018	Table-top exercise on international co-operation on cybercrime, Kyiv, Ukraine, 18-19 October 2018
CyberCrime@EAP 2018	ECTEG Course on Live Data Forensics, Baku, Azerbaijan, 22-26 October 2018
GLACY+ Cybercrime@Octopus	Workshop on Cybercrime and Electronic Evidence for Supreme Court Judges, Accra, Ghana, 23 October 2018

GLACY+	Workshop on Cybercrime and Electronic Evidence for Judges of the Court of Appeal, Accra, Ghana, 24 October 2018
GLACY+ Cybercrime@Octopus	Workshop on Cybercrime & Cybersecurity for Selected Members of Parliament, Accra, Ghana, 25 October 2018
GLACY+ Cybercrime@Octopus	Participation in the Criminal Justice Sector Forum on Cybercrime, Accra, Ghana, 23 October 2018
GLACY+	International conference on Cybercrime organised by the Judicial School of the Dominican Republic, Santo Domingo, Dominican Republic, 25-26 October 2018
CyberCrime@EAP 2018	Support to Regional Cyber Week & Expo 2018 in Republic of Moldova, Kishinev, Republic of Moldova, 29 October - 2 November 2018
GLACY+	ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers, Colombo, Sri Lanka, 29 October – 2 November 2018
EndOCSEA@Europe	OECD workshop on the Protection of Children in the Digital Environment, Zurich, Switzerland, 15-16 October 2018.
EndOCSEA@Europe	ERA conference on Cyberbullying, sexting and sextortion - legal responses to the risks and dangers for children in cyberspace, Barcelona, Spain, 29-30 October 2018.

November 2018

CyberCrime@EAP 2018	Advisory Mission on international co-operation through 24/7 points of contact and mutual legal assistance, Kyiv, Ukraine, 1-2 November 2018
iPROCEEDS	Training Course on Cryptocurrencies, Budapest, Hungary, 5-7 November 2018
GLACY+ Cybercrime@Octopus	Basic Judicial Training on Cybercrime for Trainers/Judges, Prosecutors and Lawyers and Adaptation of Materials to the Local Context, Santiago, Chile, 5-9 November 2018
CyberCrime@EAP 2018	Advisory Mission on international co-operation through 24/7 points of contact and mutual legal assistance, Kyiv, Ukraine, 6-8 November 2018
CyberSouth	Study visit of the Gendarmerie – Centre for the prevention of and fight against information crime and cybercrime (CPLCIC), Algiers, Algeria, 7-8 November 2018
CyberCrime@EAP 2018	Support to Georgian Cyber Security Forum 2018, Kvareli, Georgia, 9 November 2018
CyberSouth	Workshop on online fraud and electronic payment frauds, Bucharest, Romania, 12-14 November 2018
CyberSouth	Initial training of magistrates on cybercrime and electronic evidence, Tunis, Tunisia, 12-14 November 2018
iPROCEEDS	Regional case simulation exercise on cybercrime and financial investigations, Bucharest, Romania, 12-15 November 2018
GLACY+	Advanced judicial training on cybercrime and electronic evidence for judges, prosecutors and other judicial personnel of French- and Portuguese-speaking countries of ECOWAS and Mauritania, Dakar, Senegal 12-15 November 2018

GLACY+	Conference on Cybercrime organised by FIIAPP, management of the joint EU-FIIAPP project EL PAcCTO, San Salvador, El Salvador, 13-14 November 2018
GLACY+	Presentation on Budapest Convention and Additional Protocols at the ENISA-EC3 Workshop on CSIRT and international law enforcement co-operation, Netherlands, 13 November 2018
GLACY+	Participation in the seminar "Investigating Web 2.0 - The Collection of Evidence Located Abroad and the Challenges of Transborder Access to Data", organised by ERA and NIM (National Institute for Magistracy), Bucharest, Romania, 13-14 November 2018
GLACY+	In-country Workshop on Data Protection and INTERPOL Tools and Services and support on how to set-up and on how to strengthen the 24/7 Points of Contact for Cybercrime and Electronic Evidence, Sri Lanka, 14-16 November 2018
CyberSouth	Round table on cybersecurity, Beirut, Lebanon, 15 November 2018
GLACY+	Cybercrime and Fundamental Rights – Expert meeting, Bucharest, Romania, 15-16 November 2018
CyberSouth	Workshop on the Budapest Convention, Beirut, Lebanon, 16 November 2018
CyberSouth	Awareness raising and GAP analysis on the Budapest Convention, Amman, Jordan, 18 November 2018
CyberSouth	Initial training on cybercrime and electronic evidence for magistrates, Amman, Jordan, 19- 22 November 2018
GLACY+	In-country Workshop on Data Protection and INTERPOL Tools and Services and support on how to set-up and on how to strengthen the 24/7 Points of Contact for Cybercrime and Electronic Evidence, Port Louis, Mauritius, 19-21 November 2018
GLACY+	Introductory Training of Trainers Course on Cybercrime and Electronic Evidence for Prosecutors and State Attorneys of the ASEAN Region, Manila, Philippines, 20-23 November 2018
CyberSouth	Study visit of the National Garde, Tunis, Tunisia, 19 and 21 November 2018
iPROCEEDS	Second National Delivery of the Introductory Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Ankara, Turkey 21-24 November 2018
CyberCrime@EAP 2018	Meeting on Cybersecurity Capacity Maturity Model for Nations (CMM), Tbilisi, Georgia, 22 November 2018
CyberSouth	2nd Steering Committee, Strasbourg, France, 26 November 2018
CyberCrime@EAP 2018 GLACY+ iPROCEEDS CyberSouth	20th Plenary Meeting of the Cybercrime Convention Committee And 3rd Protocol Drafting Plenary, Strasbourg, France, 27-30 November 2018
CyberSouth	The 4th Anti-Cybercrime Forum on Cybercrime and Cyber Security Regime - Risks and Opportunities, Beirut, Lebanon, 29 November 2018
EndOCSEA@Europe	Planning meeting with WePROTECT Global Alliance and other actors, London, UK, 8-9 November 2018.

December 2018

iPROCEEDS	Workshop on online financial fraud and credit card fraud, Skopje, North Macedonia, 3 December 2018
CyberSouth	Advanced Judicial Training, Algiers, Algeria, 2-6 December 2018
GLACY+	5th African Working Group Meeting on Cybercrime for Heads of Cybercrime Units, Accra, Ghana, 4-6 December 2018
GLACY+	Meeting of the Interparliamentary Commission on public security and the administration of justice (CISCAJ), Guatemala, 6 December 2018
iPROCEEDS	MSc in Forensic Computing and Cybercrime Investigation University College Dublin - 4th Semester, Dublin, Ireland, 8–12 December 2018
CyberSouth	Study visit of General Directorate of National Security (DGSN), Rabat, Morocco, 10-11 December 2018
iPROCEEDS	International Workshop on Cybercrime, Ankara, Turkey, 10 December 2018
GLACY+ Cybercrime@Octopus	First responders' training of trainers for Law Enforcement Officials, Abuja, Nigeria, 10–13 December 2018
Cybercrime@Octopus	Advisory mission on the preparation of legislation on cybercrime and electronic evidence, Niamey, Niger, 10-13 December 2018
GLACY+	Advisory Mission on Harmonisation of Legislation on Cybercrime and Electronic Evidence, Freetown, Sierra Leone, 11–14 December 2018
CyberCrime@EAP 2018	Regional Meeting: Conference on Cybercrime Strategies and Closing Event for Cybercrime@EaP projects (2015-2018), Tbilisi, Georgia, 11-13 December 2018
CyberSouth	Training on electronic evidence for Lebanese magistrates, Beirut, Lebanon, 14 December 2018
GLACY+	ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers, Dakar, Senegal, 17-21 December 2018
Cybercrime@Octopus	Advisory mission on the legal framework on cybercrime and electronic evidence and assessment of capacity building needs, Nouakchott, Mauritania, 17-19 December 2018
Cybercrime@Octopus	Workshop on legislation related to cybercrime and electronic evidence, Astana, Kazakhstan, 20-21 December 2018

January 2019

CyberSouth	E- FIRST Course, European Cybercrime Training Education Group (ECTEG), Bucharest, Romania, 14-18 January 2019
GLACY+	Coordination meeting with other EU-funded projects with components on cybercrime, Brussels, Belgium, 16 January 2019
CyberSouth	Advanced Judicial Training on cybercrime and electronic evidence, Beirut, Lebanon, 16-19 January 2019
Cybercrime@Octopus	First working meeting on National Strategy of Cyber Security 2019-2020 and its Action Plan, Tbilisi, Georgia, 17 January 2019
GLACY+ Cybercrime@Octopus	Advisory mission on legislation on Cybercrime and Electronic Evidence, Guatemala City, Guatemala, 21-24 January 2019

GLACY+	Workshop on Cybercrime and Electronic evidence for Judges, Magistrates and Prosecutors of Indonesia, Jakarta, Indonesia, 21-25 January 2019
CyberSouth	International Forum on Cybersecurity and intergovernmental meetings on cybersecurity, Lille, France, 22-25 January 2019
CyberSouth	Regional Workshop on Judicial Training Strategy, Beirut, Lebanon, 23-25 January 2019
GLACY+ Cybercrime@Octopus	Introductory Judicial Training of Trainers on Cybercrime and Electronic Evidence for Judges, Prosecutors and Lawyers and adaptation of materials to the local context, Abuja, Nigeria, 28 January – 01 February 2019
iPROCEEDS	Meeting on Public-private co-operation for fighting cybercrime and online crime proceeds, Tirana, Albania, 29 January 2019

February 2019

GLACY+	Advisory mission and workshop on the collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, Rabat, Morocco, 4–6 February 2019
GLACY+	Participation in the advisory mission on cybercrime legislation in the framework of the Cyber Resilience Program of the Commonwealth Secretariat, Nairobi, Kenya, 4-8 February 2019
CyberSouth	Advanced Judicial Training on cybercrime and electronic evidence, Tunis, Tunisia, 4-8 February 2019
Cybercrime@Octopus	Contribute to the 2nd meeting related to drafting of the new integrated (cybercrime and cybersecurity) Strategy for Georgia 2019-2020, Tbilisi, Georgia, 5-7 February 2019
CyberSouth	Support to UNODC meeting “Challenges and Best Practices in the Treatment and Use of Digital Evidence in Terrorism Cases”, Vienna, 5-7 February 2019
iPROCEEDS	ECTEG Training Course on Network Investigations, Bucharest, Romania, 11-15 February 2019
Cybercrime@Octopus	T-CY Protocol Drafting Group meeting, Strasbourg, France, 11-13 February 2019
GLACY+ Cybercrime@Octopus	Introductory Judicial Training of Trainers (TOT) on Cybercrime and Electronic Evidence for Judges, Prosecutors and Lawyers, San Jose, Costa Rica, 11-15 February 2019
GLACY+	ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers, Rabat, Morocco, 11-15 February 2019
CyberSouth	Briefing meeting with the Embassies regarding cybercrime and electronic evidence, Bucharest, Romania, 15 February 2019
CyberSouth	ECTEG Live Data Forensics Training, Bucharest, Romania, 18–22 February 2019
CyberSouth	Integration of judicial training material in Morocco, Rabat, Morocco, 18-22 February 2019
Cybercrime@Octopus	Participation at the 22nd European Police Congress, 19-20 February 2019

iPROCEEDS	Second Delivery of the Introductory training module on cybercrime, electronic evidence and online crime proceeds, Pristina, Kosovo*, 19-22 February 2019
GLACY+ iPROCEEDS Cybercrime@Octopus	Conference on Criminal Justice in Cyberspace, Bucharest, Romania, 25-27 February 2019
CyberSouth	Support to UNODC meeting "Drafting a legislation on the admissibility of digital evidence before terrorism courts", Egypt, 24-28 February 2019
GLACY+	INTERPOL Instructor Development Course for Spanish and Portuguese speaking countries, Bogota, Colombia, 25 February - 1 March 2019
GLACY+	Lecture on the Budapest Convention for the Cybersecurity Master program, LUISS, Rome, Italy, 28 February 2019
Cybercrime@Octopus	Drafting the 2nd Additional Protocol to the Budapest Convention, Feb-Dec 2019

March 2019

GLACY+	Coordination meeting at Europol with the PMU of the SIRIUS Project to assess possible co-operation GLACY+, The Hague, Netherlands, 1 March 2019
GLACY+	Workshop on Cybercrime and Electronic Evidence for Intake of New Judges, Colombo, Sri Lanka, 2-3 March 2019
EndOCSEA@Europe	First meeting of the Steering Committee for the Project EndOCSEA@Europe, Strasbourg, France, 4 March 2019
iPROCEEDS	Case simulation exercise on cybercrime and financial investigations, Tirana, Albania, 4–7 March 2019
CyberSouth	ECTEG Course on Darkweb and Crypto Currencies, Bucharest, Romania, 4-8 March 2019
GLACY+	Coordination meeting with EU-funded Cybercrime projects (OCWAR-C, GLACY+, Cyber4Dev), Brussels, Belgium, 5 March 2019
GLACY+	Coordination meeting with Eurojust for the preparation of a joint international conference, The Hague, Netherlands, 8 March 2019
iPROCEEDS	Assessment mission on harmonisation of legislation of Serbia on cybercrime and electronic evidence with EU and Council of Europe standards, Belgrade, Serbia, 11-12 March 2019
iPROCEEDS	Third delivery of the Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Podgorica, Montenegro, 11-12 March 2019
Cybercrime@Octopus	Awareness-raising workshop on the Budapest Convention on Cybercrime, Abidjan, Ivory Coast, 12 March 2019
iPROCEEDS	Meeting on update ECTEG Training on Darkweb and virtual currencies investigations, Bucharest, Romania, 11-13 March 2019
GLACY+	Participation in the Empact OA 3.6, 11-13 March 2019
GLACY+	Advanced Judicial Training of Trainers on Cybercrime and Electronic Evidence for Judges, Prosecutors and Public Defenders, Santo Domingo, Dominican Republic, 11–14 March 2019
CyberSouth	Advanced Training on Cybercrime and Electronic Evidence for Magistrates, Amman, Jordan, 17-19 March and 20-23 March 2019

GLACY+	National Conference on the Technical Implementation of the Budapest Convention, Accra, Ghana, 18-19 March 2019
GLACY+	Participation in the Cyber Command Course organised by the Hong Kong Police, Hong Kong, 18-22 March 2019
GLACY+ Cybercrime@Octopus	Advisory Mission on Integration/Mainstreaming of Training Modules in curricula of Judicial Training Institutions, Accra, Ghana, 20–22 March 2019
iPROCEEDS	6th meeting of the T-CY Protocol Drafting Group (T-CY PDG), Vienna, Austria, 25-26 March, 2019
CyberSouth	Law Enforcement Training in the area of undercover online operations in combatting cybercrime, Bucharest, Romania, 25-29 March 2019
GLACY+	Legislation on cybercrime and electronic evidence in The Gambia - Drafting Exercise, Banjul, The Gambia, 25–27 March 2019
iPROCEEDS	4th Edition of the Critical Infrastructure Protection Forum, Bucharest, Romania, 25-29 March 2019
CyberSouth GLACY+ iPROCEEDS Cybercrime@Octopus	The Fifth meeting of the United Nations Intergovernmental Expert Group on Cybercrime (UNIEG), Vienna, Austria, 27-30 March 2019
iPROCEEDS	6th Meeting of the Project Steering Committee, Bucharest, Romania, 29 March 2019

April 2019

Cybercrime@Octopus	Awareness workshop on the Budapest Convention, Conakry, Guinea, 1-2 April 2019
CyberSouth	ECTEG online First responder Course meeting, Bucharest, Romania, 2-4 April 2019
GLACY+	Advisory mission on the streamlining of procedures for Mutual Legal Assistance related to Cybercrime and Electronic Evidence, Santo Domingo, Dominican Republic, 2-5 April 2019
iPROCEEDS	Training of trainers on delivery of the basic training module on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors for North Macedonia and Turkey, Skopje, North Macedonia, 2-6 April 2019
GLACY+	GFCE Working Group Meetings 2019, The Hague, Netherlands, 3-4 April 2019
GLACY+	In-country workshop on Data Protection and INTERPOL tools and services, combined with support on how to set up and strengthen the 24/7 points of contact for cybercrime and electronic evidence, Manila, Philippines, 3-5 April 2019
iPROCEEDS	Workshop on online financial fraud and credit card fraud, Ankara, Turkey, 4 April 2019
Cybercrime@Octopus	Awareness Workshop on the Budapest Convention, Cotonou, Benin, 4-5 April 2019
GLACY+	Advisory mission on the integration of cybercrime and electronic evidence in the training curricula of judicial training institutions, Santo Domingo, Dominican Republic, 4-5 April 2019

EndOCSEA@Europe	Civil Society Conference: Strengthening civil society participation in the implementation and monitoring of the Lanzarote Convention, Strasbourg, France, 8-9 April 2019
CyberSouth	Regional workshop towards the elaboration of national reports on the evaluation of cyberthreats, Rabat, Morocco, 8-10 April 2019
GLACY+	Advanced Judicial Training Course on Cybercrime and Electronic Evidence for Judges, Prosecutors and other Judicial Officers, Santiago, Chile, 8-11 April 2019
iPROCEEDS	Case simulation exercise on cybercrime and financial investigations for Bosnia and Herzegovina, Montenegro and Serbia, Belgrade, Serbia, 8-11 April 2019
CyberSouth	Workshop on cybersecurity CEPOL, Beirut, Lebanon, 9-11 April 2019
GLACY+	International Conference on Cybercrime and Electronic Evidence and 2nd Meeting of the Cybercrime Forum for CPLP countries, Praia, Cabo Verde, 11-12 April 2019
iPROCEEDS	Legal Reflections on 24/7 Points of Contact and Preservation Requests, Istanbul, Turkey, 15-16 April 2019
iPROCEEDS	Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds for judges and prosecutors (2nd part), Podgorica, Montenegro, 15-16 April 2019
GLACY+	Participation in the EU Cyber Forum, Brussels, Belgium, 15-16 April 2019
CyberSouth	Study visit to the specialised cybercrime unit of the French National Police, Nanterre, France, 15-16 April 2019
GLACY+	GLACY+ Steering Committee, Brussels, Belgium, 16 April 2019
iPROCEEDS	Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Vlasic, Bosnia and Herzegovina, 22-25 April 2019
GLACY+	4th meeting of the INTERPOL Global Cybercrime Expert Group, Lyon, France, 24-26 April 2019
iPROCEEDS	Support participation in the International Conference on digital forensics and digital evidence - DataFocus 2019, Zagreb, Croatia, 30 April 2019
iPROCEEDS	Support participation in long-distance master programme at UCD (Summer examination), Dublin, Ireland, 30 April - 2 May 2019
EndOCSEA@Europe	Desk research for Baseline Mapping on OCSEA in COE member states, April-October 2019
EndOCSEA@Europe	Desk research for Comparative Review of international mechanisms to prevent and combat OCSEA, April-September 2019

May 2019

Cybercrime@Octopus	Internet and Jurisdiction Conference, Berlin, Germany, 3-5 May 2019
iPROCEEDS	Case simulation exercises on cybercrime and financial investigations (for North Macedonia and Turkey), Ankara, Turkey, 6-9 May 2019
Cybercrime@Octopus	Data protection legislation workshop, Banjul, Gambia, 6-10 May 2019
GLACY+	Introductory Judicial Training of Trainers on Cybercrime and Electronic Evidence for Judges, Prosecutors and Lawyers and adaptation of materials to the local context, Praia, Cabo Verde, 6-10 May 2019

iPROCEEDS	Table-top exercise on international co-operation in cybercrime cases, Bucharest, Romania, 8-9 May 2019
GLACY+	Advanced Judicial Training Course on Cybercrime and Electronic Evidence for Judges, Prosecutors and other Judicial Officers, San Jose, Costa Rica, 13-16 May 2019
iPROCEEDS	Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (1st part), Tirana, Albania, 13-14 May 2019
Cybercrime@Octopus	7th T-CY Protocol Drafting Group meeting, Strasbourg, France, 13-15 May 2019
GLACY+	Second Expert Meeting on the Joint CoE/ FRA Handbook on Cybercrime and Fundamental Rights, Vienna, Austria, 14-15 May 2019
iPROCEEDS	Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors, Ankara, Turkey, 14-17 May 2019
CyberSouth, GLACY+ Cybercrime@Octopus	Free Forensic Tools for the Law Enforcement Community (FREETOOL) – Open Source Tools for Cybercrime Investigation and Digital Forensics, Bucharest, Romania, 15-17 May 2019
GLACY+	In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and strengthen the 24/7 points of contact for cybercrime and electronic evidence, Nuku'alofa, Tonga, 15-17 May 2019
EndOCSEA@Europe	Council of Europe Conference: Multi-sectorial co-operation to prevent and combat Online Child Sexual Exploitation and Abuse - International Conference, Strasbourg, France, 16-17 May 2019
GLACY+	Advisory mission on Procedural Legislation on Cybercrime and Electronic Evidence, San Jose, Costa Rica 16-17 May 2019
GLACY+	Advisory mission and workshop on cybercrime and cyber security policies and strategies, Manila, Philippines, 20-22 May 2019
CyberSouth	ECTEG online First responder Course meeting, Lisbon, Portugal, 20-24 May 2019
Cybercrime@Octopus	Pompidou Group – Annual meeting on Drugs Online and request for nominations Criminal Intelligence Service, Vienna, Austria, 21-23 May 2019
GLACY+ Cybercrime@Octopus	Participation in the 20th International Symposium on Cybercrime Response (ISCR 2019), Seoul, Korea, 22-24 May 2019
GLACY+	Participation in the Cybersecurity Maturity Model assessment mission and advisory mission on cybercrime legislation, in coordination with the World Bank, the UK FCO and the Commonwealth Secretariat, Windhoek, Namibia, 22-24 May 2019
GLACY+	Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, Manila, Philippines, 23-24 May 2019
iPROCEEDS	Conference on Crime in the Digital Age: Enhancing Capacities of Criminal Justice Institutions across the OSCE Area, Vienna, Austria, 24 May 2019

GLACY+ Cybercrime@Octopus	PILON Regional Workshop on cybercrime and electronic evidence in the Pacific. International Co-operation to Share Electronic Evidence to Combat Cybercrime, Port Vila, Vanuatu, 27-31 May 2019
GLACY+	Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, Port Louis, Mauritius, 28-29 May 2019
iPROCEEDS	Support participation in the Conference on ISS World Europe - Intelligence Support Systems for Electronic Surveillance, Social Media/ DarkNet Monitoring and Cyber Crime Investigations, Prague, Czech Republic, 28-30 May 2019
GLACY+	Workshop on the Development of Cybercrime Investigations; National Workshop and Advice on Interagency Co-operation and Public Private Collaboration to Fight Cybercrime, Santo Domingo, Dominican Republic, 28-30 May 2019

June 2019

CyberSouth	CEPOL training event on electronic evidence-Contribution of the Council of Europe, Budapest, Hungary, 3-6 June 2019
GLACY+	Regional training of trainers for First Responders on Cybercrime and Electronic Evidence for African gendarmeries, Dakar, Senegal, 3-7 June 2019
GLACY+	Cryptocurrency Investigations Training to police cyber-units, Santo Domingo, Dominican Republic, 3-7 June 2019
CyberSouth	Adaptation of Judicial training material to Tunisian judicial training course, Tunis, Tunisia, 10-14 June 2019
Cybercrime@Octopus	The 8th Annual Summit on Human Rights in the Digital Age, Tunis, Tunisia, 11-14 June 2019
CyberSouth	Euromed police and Justice Regional Workshop for Euro-Mediterranean Cybercrime and Digital Evidence Contact Points, Bucharest, Romania, 12-14 June 2019
iPROCEEDS	Introductory training course on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors (2nd part), Tirana, Albania, 12-13 June 2019
GLACY+	Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community, Santo Domingo, Dominican Republic, 12-14 June 2019
CyberSouth	Integration judicial training on cybercrime and electronic evidence, Algiers, Algeria, 16-20 June 2019
CyberSouth	ECTEG Pilot course Online Investigators course (OSINT), Tunis, Tunisia, 17-21 June 2019
GLACY+	Participation in the launching event of the HELP online course on Data Protection, Bucharest, Romania, 18-19 June 2019
EndOCSEA@Europe	Gap analysis of legislation, policy and practices on OCSEA in Azerbaijan, Baku, Azerbaijan, 18-21 June 2019
Cybercrime@Octopus	Workshop on legislation on cybercrime and electronic evidence, Doha, Qatar, 18-28 June 2019

Cybercrime@Octopus	European Dialogue on Internet Governance, The Hague, Netherlands, 19-20 June 2019
GLACY+	Participation in ICANN 65 - Policy Meeting, Marrakech, Morocco, 24-27 June 2019
CyberSouth	Malware Analysis Training, Tunis, Tunisia, 24-28 June 2019
GLACY+	International Data Protection Conference for the African Region, Accra, Ghana, 24-27 June 2019
GLACY+	Second Annual meeting and International Conference of the Ibero-American Network of Cyber Prosecutors, Santiago, Chile, 25-26 June 2019
GLACY+ iPROCEEDS	Joint International Workshop for Cybercrime Investigation Units and MLA Central Authorities, Singapore, 25-27 June 2019
iPROCEEDS	Fourth annual Symposium on Cybersecurity Awareness organised by the Anti-Phishing Working Group, Bucharest, Romania, 26 - 27 June 2019

July 2019

GLACY+	Advisory mission and workshop on legislation to FOPREL, San Salvador, El Salvador, 1-2 July 2019
GLACY+, CyberSouth CyberEast iPROCEEDS Cybercrime@Octopus	21st T-CY Plenary and 4th Protocol Drafting Plenary, Strasbourg, France, 8-11 July 2019
GLACY+	Study visit of Sri Lankan judges to Belgium and workshop on cybercrime and electronic evidence, Brussels, Belgium, 8 July 2019
CyberSouth	CyberSouth Third steering Committee, Strasbourg, France, 9 July 2019
GLACY+ CyberSouth CyberEast iPROCEEDS	International Conference of National Judicial Trainers Network on Cybercrime and Electronic Evidence, Strasbourg, France, 10-12 July 2019
CyberSouth	12th Middle East and North Africa Working Group Meeting on Cybercrime for Heads of Units in co-operation with Interpol, Amman, Jordan, 16-17 July 2019
GLACY+	Development of Cybercrime Investigation Unit and Data Forensics Unit, Abuja, Nigeria 16-19 July 2019
GLACY+	Participation in the Cybersecurity Summer Boot Camp 2019, Leon, Spain, 16-27 July
CyberSouth	ECTEG workshop for Digital Forensics Trainers, Budapest, Hungary, 22-26 July 2019
GLACY+	Development of Cybercrime Investigation Unit and Data Forensics Unit, Praia, Cabo Verde, 22-25 July 2019
EndOCSEA@Europe	Desk research for gap analysis regarding legislation, policy and procedures on OCSEA in Armenia, July-September 2019
EndOCSEA@Europe	Desk research for gap analysis regarding legislation, policy and procedures on OCSEA in Azerbaijan, July-September 2019
EndOCSEA@Europe	Desk research for gap analysis regarding legislation, policy and procedures on OCSEA in Ukraine, July-September 2019

EndOCSEA@Europe	Civil Society Grants to raise awareness on OCSEA through child participation and development of tools, July 2019 - July 2020
EndOCSEA@Europe	Child consultations to develop a child-friendly version of the Lanzarote Convention, July-October 2019

August 2019

GLACY+	Follow-up meeting with FOPREL and bilateral meetings with Mexican authorities in view of adoption/ reviewing legislation and accession to the Budapest Convention, Mexico City, Mexico, 19-21 August 2019
GLACY+	Introductory Training of Trainers on Cybercrime and Electronic Evidence for Magistrates and Prosecutors, Port Louis, Mauritius, 19-23 August 2019
GLACY+	Preparatory meeting with Eurojust for the joint conference, 23 August 2019

September 2019

GLACY+	INTERPOL Malware Analysis Training, Manila, Philippines, 2-6 September 2019
CyberSouth CyberEast iPROCEEDS GLACY+	2019 Underground Economy Conference, Strasbourg, France, 3-6 September 2019
CyberEast	Assessment of EaP countries institutional setup, capacities, competencies, training needs as well as interagency co-operation gaps and opportunities, Kyiv, Ukraine, 3-5 September 2019
CyberEast	Assessment of EaP countries institutional setup, capacities, competencies, training needs as well as interagency co-operation gaps and opportunities, Yerevan, Armenia, 9-10 September 2019
CyberEast	Assessment of EaP countries institutional set-up, capacities, competencies, training needs as well as interagency co-operation gaps and opportunities, Baku, Azerbaijan, 12-13 September 2019
CyberSouth	Participation in the Cybersecurity Dialogues Congress and delivering a presentation on the role of the Council Europe in the cyber environment, Sibiu, Romania 12-13 September 2019
CyberSouth	Adaptation of Judicial training material, Amman, Jordan, 15-19 September 2019
Cybercrime@Octopus	8th meeting of the Protocol Drafting Group, Paris, France, 16-18 September 2019
CyberEast	Assessment of EaP countries institutional setup, capacities, competencies, training needs as well as interagency co-operation gaps and opportunities, Tbilisi, Georgia, 16-17 September 2019
EndOCSEA@Europe	Fact finding visit and gap analysis workshop regarding legislation, policy and procedures on OCSEA, Yerevan, Armenia, 16-20 September 2019
EndOCSEA@Europe	Fact finding visit and gap analysis workshop regarding legislation, policy and procedures on OCSEA, Kyiv, Ukraine, 17-19 September 2019
iPROCEEDS	Regional training on Undercover Online Investigations in co-operation with SELEC, Bucharest, Romania, 17-20 September 2019

CyberEast	Launching Event of CyberEast Project, Brussels, Belgium, 19-20 September 2019
CyberSouth	Meeting on legislation, Amman, Jordan, 23 September 2019
GLACY+	In-country advisory mission on integration/ mainstreaming of training modules in curricula of judicial training institutions and prosecutors' training institution, San Jose, Costa Rica, 23-24 September 2019
GLACY+ Cybercrime@Octopus	African Regional Conference on Cybercrime, National Cyber Security and Internet Piracy, Lagos, Nigeria, 23-27 September 2019
CyberEast	Support to EAP Internet Governance Summer School, Tbilisi, Georgia, 23-27 September 2019
CyberSouth	Regional workshop on law enforcement training strategies, Amman, Jordan, 24-25 September 2019
CyberEast	Assessment of EaP countries' institutional setup, capacities, competencies, training needs and interagency co-operation gaps and opportunities, Minsk, Belarus, 24-25 September 2019
Cybercrime@Octopus	Hosting a panel on Cybercrime and Data Protection Legislation in Africa at FIFAfrica 2019, in collaboration with the Data protection Unit of the Council of Europe, Addis Ababa, Ethiopia, 25-26 September 2019
GLACY+	Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, Nuku'alofa, Tonga, 25-27 September 2019
iPROCEEDS	Trust Services Forum-CA Day, Berlin, Germany, 25-26 September 2019
GLACY+ CyberEast iPROCEEDS EndOCSEA@Europe	International Joint Conference Eurojust/CoE on Internet Investigations: Dark web and online child abuse, The Hague, Netherlands, 30 September - 1 October 2019
EndOCSEA@Europe	Desk research to analyses OCSEA training strategies and materials for Law enforcement officers in Armenia, Azerbaijan, Republic of Moldova and Ukraine, September-December 2019
EndOCSEA@Europe	ENOC annual conference - Awareness raising among Ombudspersons for children, Belfast, Ireland, September 2019