COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

## Information Documents

**SG/Inf(2018)32**

Strasbourg, 14 November 2018

# The Council of Europe Office on Cybercrime in Bucharest

# C-PROC activity report for the period October 2017 – September 2018

# Contents

# Executive summary

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, in the period October 2017 to September 2018.[1]

In response to the need for enhanced capacity-building on cybercrime worldwide, on 9 October 2013 (at their 1180th meeting), the Committee of Ministers decided that the Council of Europe establish a Programme Office on Cybercrime in Bucharest. The Office became operational on 7 April 2014, and all capacity-building projects on cybercrime are being implemented by this Office. Since then, C-PROC carried out or supported some 620 activities involving more than 150 countries.

Between October 2017 and September 2018 the Office supported approximately 220 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. These were aimed at improving legislation, training of judges, prosecutors and investigators, public/private and international co-operation, and other measures to strengthen the criminal justice response to cybercrime and electronic evidence.

The Office is broadly funded from extra-budgetary resources. By September 2018, the Office managed ongoing projects with a combined budget of more than EUR 26 million and with 29 staff (from nine different member states). It is headed by the Head of Cybercrime Division (DGI) who divides his time between Strasbourg and Bucharest. He is supported by an experienced Head of Operations. All staff – with the exception of the Head of Office – is funded from the budgets of projects for which they are responsible. C-PROC premises are located at the UN House in Bucharest, and are provided rent free by the Government of Romania.

The experience during the past year confirms that the expectations linked with the establishment of the Office have been met:

- The Council of Europe remains a global leader for capacity-building on cybercrime and electronic evidence.

- The relevance and impact of the Office is not solely due to the volume of projects and activities but also to strong synergies between the Budapest Convention, follow up and assessments by the Cybercrime Convention Committee (T-CY) and capacity-building by C-PROC. Between October 2017 and September 2018, C-PROC in particular provided back up and resources to the T-CY in the face of challenges related to the Ordinary Budget of the Council of Europe.

[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

- Capacity-building activities of C-PROC enable non-member states to join the Budapest Convention. During the last twelve months, six states from Africa, Asia and Latin America became Parties.

- Activities are designed to strengthen human rights, democracy and the rule of law through legislation, targeted training as well as data protection and other safeguards.

- The Office is attractive to donors. The Office had started in April 2014 with projects with a volume of approximately EUR 4 million and by September 2018 the volume had increased to more than EUR 26 million. Additional projects are in preparation.

- Relevant authorities of the Government of Romania, but also of other Parties to the Budapest Convention (currently Estonia, France, Germany, United Kingdom and USA), as well as the European Cybercrime Centre at EUROPOL and INTERPOL are partners in C-PROC projects and contribute their expertise. The Office and its projects have established strong relations with numerous other organisations.

While the Office will continue along the same path, specific targets for the forthcoming twelve months include:

- Emphasis on human rights and rule of law safeguards;

- Protecting children against online sexual violence and other measures against cyberviolence;

- Fund-raising for follow up projects in the Eastern Partnership region and South-eastern Europe;

- Further enhancing the subject-matter expertise of the Office.

The expectations linked with the establishment of the Office have been met and the conditions for its further development are in place.

It is proposed that the Office continue to operate under the current arrangement.

# 1 Background and purpose of this report

The purpose of the present report is to inform the Committee of Ministers of the Council of Europe of the activities of the Council of Europe Programme Office on Cybercrime (C-PROC) in Bucharest, Romania, during the period October 2017 to September 2018.

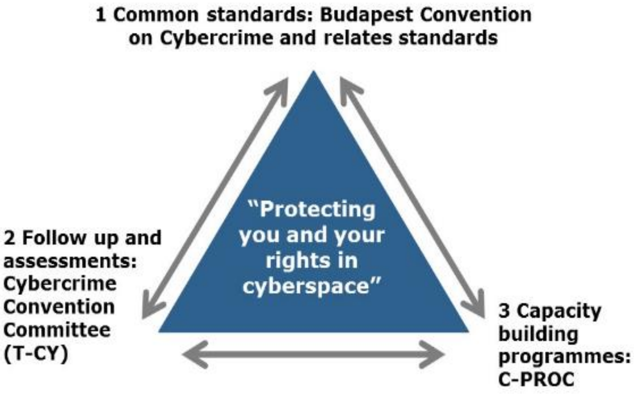
Cybercrime – as offences against and by means of computer systems – has evolved into a major threat to fundamental rights, democracy and the rule of law, as well as international peace and stability. Along with this, the question of electronic evidence has gained in significance and complexity.

Today 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.

The question of cybercrime and electronic evidence 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[2] and remains the most relevant international agreement on this issue. By September 2018, 61 states were Parties and a further 10 had signed it 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;


1 Common standards: Budapest Convention on Cybercrime and relates standards
"Protecting you and your rights in cyberspace"
2 Follow up and assessments: Cybercrime Convention Committee (T-CY)
3 Capacity building programmes: C-PROC

- 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 72 member and observer states[3] and eleven observer organisations, the T-CY is one of the main intergovernmental bodies on cybercrime internationally. Its main focus currently is the preparation of an Additional

[2] 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.

[3] 61 Parties, 10 signatories or states invited to accede as well as the Russian Federation.

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. However, discussions at the level of the United Nations in early 2013[4] confirmed broad international agreement on capacity-building as an effective way ahead to help societies meet the challenge of cybercrime and electronic evidence.

The decision by the Committee of Ministers in October 2013,[5] following an offer of the Government of Romania and a proposal by the Secretary General (SG/Inf(2013)29), to establish a Programme Office on Cybercrime in Bucharest, Romania, represents the Council of Europe's response to this need for worldwide capacity-building.

The Office became operational on 7 April 2014 once the respective Memorandum of Understanding (MoU) – signed by the Council of Europe and the Ministry of Foreign Affairs – had entered into force.

The decision was linked with the expectation that:

- A specialised Office would allow the Council of Europe to respond to the growing need for capacity-building on cybercrime worldwide in a visible and credible manner;

- A dedicated Programme Office for cost-effective project implementation would facilitate fund-raising;

- Capacity-building activities by the Office would complement the intergovernmental activities of the Cybercrime Convention Committee (T-CY), which would continue to be managed from Strasbourg;

- The Office would be funded mainly by extra-budgetary resources.

Experience after 54 months of operations confirms that these expectations have been more than met.

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

[5] On 9 October 2013, at their 1180th meeting.

## 2 Mandate of the Office[6]

The objective of the Office is to ensure the implementation of the capacity-building projects on cybercrime of the Council of Europe worldwide.

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;
- establishing 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.

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.

## 3 Projects and results in the period October 2017 – September 2018

C-PROC is responsible for assisting 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.[7] The Office meets its purpose through capacity-building projects.

[6] SG/Inf(2013)29 and MoU between the Council of Europe and the Government of Romania, signed on 15 October 2013.

[7] 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.

### 3.1 Overview of current projects

In the period October 2017 to September 2018, C-PROC supported approximately 220 activities[8] under the following projects:

| Project title | Duration | Budget | Funding |
|---|---|---|---|
| Cybercrime@Octopus (number 3021) | Jan 2014 – Dec 2019 | EUR 3.5 million | Voluntary contributions (Estonia, Hungary, Japan, Monaco, Romania, Slovak Republic, UK, USA and Microsoft) |
| Cybercrime@EAP II on international co-operation in the Eastern Partnership region (number 3271) | May 2015 – Dec 2017 | EUR 800,000 | EU/CoE JP (Partnership for Good Governance) |
| Cybercrime@EAP III on public/private co-operation in the Eastern Partnership region (number 3608) | Dec 2015 – Dec 2017 | EUR 1.2 million | EU/CoE JP (Partnership for Good Governance) |
| Cybercrime@EAP 2018 on international and public/private co-operation in the Eastern Partnership region (number 1963) | Jan 2018 – Dec 2018 | EUR 980,000 | EU/CoE JP (Partnership for Good Governance) |
| GLACY+ project on Global Action on Cybercrime Extended (number 3148) | 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 (3156) | Jan 2016 – June 2019 | EUR 5.56 million | EU/CoE JP |
| CyberSouth on capacity-building in the Southern Neighbourhood | July 2017 – June 2020 | EUR 3.33 million | EU/CoE JP |

By September 2018, projects with a combined volume of approximately EUR 26.7 million were being implemented by C-PROC. While Cybercrime@Octopus is 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 2.5million).

This represents a further increase compared to previous years (September 2015: EUR 6 million, September 2016: EUR 22 million, September 2017: EUR 24.4 million).

As foreseen in the mandate of the Office, C-PROC has identified, designed, negotiated and mobilised the funding for all these projects.

[8] See Appendix for the list of activities.

## 3.2 Cybercrime@Octopus

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

Activities between October 2017 and September 2018 include for example, a workshop for 24/7 contact points under the Budapest Convention (Strasbourg, July 2018), review of the legal framework or draft laws against the provisions of the Budapest Convention of Kuweit, Qatar, Samoa and Vanuatu, review of the legislation of Korea and dialogue with the Korean Government in view of accession to the Budapest Convention, review of the legislation of Malaysia and dialogue with Malaysian authorities, preparation – in co-operation with other projects – of a review on the global state of cybercrime legislation, support to a conference on cybercrime and public/private co-operation in India in August 2018, contribution to the training of judges from francophone countries in Paris in June 2018.

Furthermore, Cybercrime@Octopus facilitated the participation of Parties and observers to the Budapest Convention in important international events, such as the UN Intergovernmental Expert Group on Cybercrime in Vienna in April 2018, the UN Commission for Crime Prevention and Criminal Justice in May 2018 with its thematic focus on cybercrime, the Global Forum on Cyber Expertise, The Global Cyberspace Conference in New Dehli in November 2017 or the Internet Governance Forum in Geneva in December 2017.

The Octopus Conference – organised under this project – remains the flagship activity of the Council of Europe on Cybercrime. It is held every 18 months. The 2018 edition took place from 11 to 13 July 2018 in Strasbourg with some 360 experts from 95 countries and numerous public and private sector organisations. It offered, among other things, a platform for multi-stakeholder consultations on the 2nd Additional Protocol to the Budapest Convention.

Importantly, Cybercrime@Octopus is designed to support the Cybercrime Convention Committee (T-CY). For example, it funded participation of observer states in T-CY plenaries, and – with funding from the USA – interpretation to and from Spanish to facilitate participation by Latin American countries in the T-CY. In spring 2018, the United Kingdom made contributions available to support meetings of the T-CY aimed at the preparation of the 2nd additional Protocol to the Budapest Convention. Moreover, C-PROC staff provides logistical support to T-CY plenary meetings if necessary.

This is a reflection of the close links between the Budapest Convention, the T-CY and C-PROC.

The project has so far been funded by Estonia, Hungary, Monaco, 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 II – International co-operation

Cybercrime@EAP II, with a budget of EUR 800,000 and duration from May 2015 to December 2017, was aimed at strengthening the capacities of Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine) for international judicial and police co-operation on cybercrime and electronic evidence.

It ensured direct follow up to the recommendations on mutual legal assistance adopted by the Cybercrime Convention Committee (T-CY) in December 2014.

It provided targeted capacity-building in Eastern Partnership countries to improve skills of authorities as well as rules and procedures for international co-operation.

Participation of country teams in international events such as plenary sessions of the Cybercrime Convention Committee (T-CY) and Octopus Conference, Pompidou Group and UN expert group meetings on cybercrime, trainings and international meetings organised by EUROPOL/INTERPOL – and other regional and international events – provided opportunities to share good practices internationally. In-country activities targeted gaps in regulatory frameworks, institutional set up and capabilities and skills necessary to ensure effective international co-operation on cybercrime and electronic evidence.

Important progress was made in this period:

- A training programme on international co-operation and co-operation with multinational service providers was developed and delivered in all Eastern Partnership countries. A full set of materials developed for such specialised training is available for future capacity-building efforts;

- Templates for standardised requests for mutual legal assistance (Article 31 Budapest Convention) and data preservation (Article 29 and 30 of the Convention) were developed and an online resource on international co-operation in the Octopus Community was prepared and tested in this region. These templates were then further improved and adopted by the T-CY for use by all Parties to the Budapest Convention in July 2018;

- Reforms of procedural law were supported by the project in five Eastern Partnership countries, given that gaps in domestic criminal procedure law hinder international co-operation on cybercrime and e-evidence.

### 3.4 Cybercrime@EAP III – Public/private co-operation

The Cybercrime@EAP III project from 2016 to December 2017 was aimed at promoting co-operation between criminal justice authorities in the Eastern Partnership countries and service providers with a budget of EUR 1.2 million. This project was the first of its kind in the region and underlined the complexity of the matter.

The project focused on building trust as a prerequisite for public/private co-operation, by bringing relevant actors together and promoting dialogue, including with multinational service providers. Efforts were undertaken to support the conclusion or update of co-operation agreements in Armenia, Georgia, republic of Moldova and Ukraine.

Moreover, the project strongly focused on reforms of criminal procedure law as an important pre-condition for public/private co-operation in terms of clarity of applicable law and building trust with the private companies. Workshops and hearings to this effect were held in Azerbaijan, Armenia, Georgia and Ukraine. Written comments on draft laws were submitted to the authorities of these countries. In the Republic of Moldova, the project had co-operated with the Venice Commission resulting in an Opinion on proposed amendments to laws.

The strengthening of domestic legislation was also raised with Belarus in order to encourage reform of the procedural law in line with the Budapest Convention and rule of law requirements.

Keeping in mind the regional nature of the project, international and regional activities on the subject of public-private partnerships were used as platforms for sharing experience on such co-operation.

As a result of project efforts, the countries of the Eastern Partnership are engaged in continuous dialogue with national Internet service providers and other important national actors on improvement of co-operation between the government and the Internet industry in terms of access to data, while involvement in international discussions on co-operation with global service providers enables these countries to engage in more efficient co-operation with these companies in criminal investigations.

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

Designed as one-year extension of the Cybercrime@EAP II and Cybercrime@EAP III projects, the PGG 2018 – Cybercrime@EAP 2018 project maintains its focus on international co-operation and public/private partnerships on cybercrime and electronic evidence.

Capacities of state authorities responsible for mutual legal assistance and police-to-police co-operation were further enhanced through participation in

Cybercrime Convention Committee (T-CY) sessions, Octopus Conferences, Eurojust Joint Conference on Cybercrime, meetings of the 24/7 points of contact network under Article 35 Budapest Convention, INTERPOL/Europol Annual Conferences on Cybercrime and Pompidou Group meetings on cybercrime. The European Dialogue on Internet Governance (EuroDIG) continues to be the flagship discussion platform for the region on matters of public/private co-operation.

The second edition of the Regional Cybercrime Co-operation Exercise built on the success of the initial effort in 2017 and expanded the experience with direct participation of Internet service providers from the Eastern Partnership region in the exercise.

The Cybercrime@EAP 2018 project also added new elements and approaches.

Following adoption of the templates for preservation requests and mutual legal assistance requests for subscriber information by the T-CY in July 2018, the project designed and rolled out 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.

Practical skills of the 24/7 points of contact and cybercrime investigators concerning processing of traffic data are further strengthened through technical courses on Network Investigations and Live Data Forensics, held in co-operation with European Cybercrime Training and Education Group (ECTEG) and on the basis of ECTEG materials.

The focus on cybercrime strategies as enabling interagency co-operation and public-private dialogue is reinforced through a series of practical workshops in all EAP states. These workshops brought together major stakeholders in an effort to map and analyse tasks and responsibilities as well as perception of threats in cyberspace, and design possible strategic responses to these threats on the basis of the Declaration on Strategic Priorities for the Co-operation against Cybercrime in the Eastern Partnership region.

The project continues to sustain reforms of criminal procedure law as an important pre-condition for public/private co-operation in terms of clarity of applicable law and building trust with the private companies (Azerbaijan, Republic of Moldova, discussions through Regional Meetings). The institutional set up, regulations and responsibilities for international co-operation are targeted though advisory missions to individual countries of the region (Armenia, Azerbaijan and Ukraine).

Finally, to maximize impact and sustainability of efforts, the project is partnering with and supporting relevant national and regional fora of co-operation on public-private partnerships, such as Internet Governance Forums in Azerbaijan and Ukraine, OSCE Conference on Terrorism in Digital Age in Belarus, Georgian IT Innovations Conference (GITI) for Armenia and Georgia, and Cyber Week events in the Republic of Moldova.

### 3.6 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 a duration of four years (to February 2020) and a budget of EUR 10 million.

Given its impact and given additional needs following accession requests (Cabo Verde, Nigeria), accessions (Chile, Costa Rica), interest in accession and needs for assistance by other countries (Burkina Faso, Gambia, Nepal, Samoa, Uganda, Vanuatu and others), in March 2018, the budget was increased to EUR 13.35 million and its duration extended to February 2021.

GLACY+ comprises three components:

1. To promote consistent cybercrime and cybersecurity policies and strategies. This includes stronger co-operation with other international and regional organisations;

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 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 (DIICOT) and Ministry of Justice), United Kingdom (National Crime Agency) and the USA (Department of Justice) as well as EUROPOL (European Cybercrime Centre).

Between October 2017 and September 2018, GLACY+ supported some 95 activities.

These included a range of training courses carried out by INTERPOL in the Dominican Republic, Ghana, Mauritius, Philippines, Sri Lanka and Tonga.

In addition to a large number of in-country training events for judges, prosecutors and law enforcement, this period was marked by major regional and international activities. Examples are:

- Forum on cybercrime and electronic evidence for the Americas (Dominican Republic, December 2017) with more than 200 participants from 40 countries in partnership with the OAS, the US Department of Justice, INTERPOL and the participation of a number of other organisations;

- Regional basic and advanced training courses for judges and prosecutors of English-speaking countries of ECOWAS (Ghana, December 2017 and July 2018);

- Workshop on international co-operation organised in co-operation with EUROJUST (The Hague, March 2018) for some 100 experts from 37 countries;

- Regional training course for judges and prosecutors of ASEAN countries (Manila, Philippines, March 2018);

- Regional cybercrime workshop organised in co-operation with the Pacific Island Law Officers Network (PILON) (Tonga, June 2018) and advanced judicial training course for the Pacific Region (Tonga, August 2018).

GLACY+ is putting strong emphasis on the preparation of legislation and the training of judges and prosecutors in view of strengthening the rule of law, including safeguards. In line with this, the project is increasingly supporting the development of data protection legislation. For example, in September 2018, in co-operation with the Data Protection Unit of the Council of Europe, Nigeria was assisted in the drafting of its data protection bill. Similar activities are planned for other countries. Already in March 2018, GLACY+ provided support to Nigeria in the finalisation of the Digital Rights and Freedom Bill.

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

The iPROCEEDS joint project covers Albania, Bosnia and Herzegovina, Montenegro, Serbia, “the former Yugoslav Republic of Macedonia”, Turkey and Kosovo*[9] and is aimed at strengthening the capacity of authorities in the region 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 June 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 ML on the Internet;
- Public/private information sharing;
- Judicial training;
- International co-operation.

[9] *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.

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

iPROCEEDS supported the improvement of cybercrime reporting mechanisms and collection of cybercrime statistics. The project assessed reporting systems' effectiveness and put forward recommendations for the reform and improvement of interagency and private-public co-operation in exchanging cybercrime-related information by undertaking advisory missions and workshops in all seven project countries/areas. A sample methodology encouraging a more holistic approach to the collection, collation and use of statistics to support more efficient investigations and prosecutions and to better inform strategic decisions of policy-makers and regulators was presented at the Regional workshop on criminal justice statistics on cybercrime and electronic evidence.

With the aim to mitigate money laundering risks and control online fraud and criminal money flows on the Internet, the project continued supporting relevant authorities in improving and where necessary developing indicators for the prevention and control of online fraud and criminal money flows on the Internet for financial sector entities and their corresponding dissemination. During the reporting period, cybercrime indicators were developed in Montenegro, Kosovo*[10], “the former Yugoslav Republic of Macedonia” and Turkey.

The bulk of activities was organised with the view to increasing skills and capacity of cybercrime and financial investigators, prosecutors and representatives of Financial Intelligence Units (FIUs) in the search, seizure and confiscation of online crime proceeds through workshops on online financial fraud and credit card fraud, regional workshop on electronic evidence and assessment report on obtaining and using electronic evidence in criminal proceedings, specialised trainings for investigators and digital forensics specialists and Cybercrime Coordination and Partnership Exercises.

iPROCEEDS took the lead in organising the Underground Economy Conference 2018 which was co-hosted this year by the Council of Europe at its premises in Strasbourg, France. This prominent international information security event brought together around 400 representatives from law enforcement agencies, the cyber security community, private industry and academia from across the globe.

Sustainable Judicial Training programmes on cybercrime, electronic evidence and online crime proceeds are the only effective manner of ensuring that judges and prosecutors have sufficient knowledge to fulfil their roles effectively. The project supported the creation of a pool of national trainers in each judicial training institution of the IPA region, who during the reporting period successfully completed the first round of the national deliveries of the Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds in all seven project countries/areas. More than 200 judges and prosecutors

[10] *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.

benefited from the course and gained knowledge on cybercrime trends and threats, technology, electronic evidence, financial investigations of cybercrime proceeds, including the relevant substantive and procedural laws, money laundering typologies related to the online environment, as well as channels and avenues of international co-operation for the search, seizure and confiscation of online crime proceeds. The iPROCEEDS project also translated the Self-Guided Training Manual: Advanced Course on the Search, Seizure and Confiscation of Online Crime Proceeds for judges and prosecutors. Now the Manual is available in English, Albanian, Serbian, Macedonian and Turkish. It was disseminated to all judicial training institutions and published on the Octopus Community.

The materials developed by iPROCEEDS are also of benefit to other projects.

### 3.8 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 the period October 2017 to September 2018, among other things:

- country project teams were set up in Algeria, Lebanon, Morocco and Tunisia. These comprise the main counterpart institutions of the project and ensure ownership and effective project implementation;

- assessment visits were carried out to and initial situation reports were prepared for Algeria, Jordan, Lebanon and Tunisia with specific recommendations on legislation and other matters;[11]

- Tunisia was invited to accede to the Budapest Convention in February 2018 and Morocco completed the accession in June 2018;

- judicial training courses were carried out in Lebanon and Morocco and a judicial training manual was adapted for use in the project area. Other guides and materials were improved or translated into Arabic;

[11] This had already been completed for Morocco under the GLACY project earlier on.

- participation of experts from project countries in international training events and relevant meetings was supported, such as a EUROJUST conference in March 2018, the meeting of INTERPOL Heads of Cybercrime Units of the MENA region (Algiers, April 2018), the UN Intergovernmental Expert Group on Cybercrime (Vienna, April 2018), UN Crime Commission (Vienna, May 2018), the T-CY Plenary of November 2017 and the Octopus Conference in July 2018.

These activities in the initial year of the project implementation prepared the ground for the remaining two years of CyberSouth.

CyberSouth – like other projects managed by C-PROC – is promoting human rights, democracy and the rule of law through the training of judges, prosecutors and investigators, standardising procedures and safeguards, strengthening the independence of the judiciary and enabling law enforcement to follow international best practice when investigating cybercrime and securing electronic evidence.

## 4 Further funding priorities

With the projects underway, C-PROC has a solid basis and resources to make an impact over the next two to three years. Further priorities for projects and funding include:

- new project on “ending child online sexual exploitation and abuse”. Funding for this project (US$ 1 million) has been received. It will be implemented jointly by the Council of Europe’s Children Division and C-PROC as from October/November 2018;

- increased support to the Eastern Partnership region given that the current Cybercrime@EAP project is ending on 31 December 2018. Discussions with the European Union on a new project are at an advanced stage;

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

- additional voluntary contributions to the project Cybercrime@Octopus in view of support to the work of the Cybercrime Convention Committee;

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

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

## 5 Relationship with the Cybercrime Convention Committee (T-CY)

The Secretariat of the T-CY is serviced by Strasbourg-based staff while all capacity-building activities are managed by C-PROC. Close links are ensured in that the Executive Secretary of the T-CY is also the Head of C-PROC and divides his time between Strasbourg and Bucharest.

The past twelve months confirmed the experience since April 2014, namely that of strong synergies. The work of the T-CY feeds directly into the work of capacity-building activities and vice-versa.

Projects managed by C-PROC follow up to results of the T-CY. A considerable number of T-CY members share their expertise as trainers or speakers in capacity-building activities.

The Office in turn supports the T-CY in that the participation of additional experts of Parties and Observers in the T-CY is funded and organised under projects run by C-PROC.

Projects run by the Office also contribute to the T-CY in substance. One example is the templates for requests for subscriber information and for data preservation, adopted by the T-CY in July 2018, which had been developed and tested under an Eastern Partnership project on cybercrime.

Between October 2017 and September 2018, several T-CY activities were funded or co-funded from the budget of Cybercrime@Octopus, including T-CY plenary meetings in November 2017 and July 2018, and meetings of the T-CY Protocol Drafting Group in February, April, May and September 2018. The United Kingdom made voluntary contributions available specifically to the Protocol Drafting Process via the Cybercrime@Octopus project. Voluntary contributions by the USA allowed for Spanish interpretation in T-CY Plenaries.

The facilitation of common positions among the Parties to the Budapest Convention in international fora is one of the functions of the T-CY. C-PROC supported this on several occasions and funded participation in relevant meetings if necessary.

Moreover, the T-CY website and other online resources were maintained by staff funded under the Cybercrime@Octopus project.

## 6 Relations with the Government of Romania

The Government of Romania continues to honour its commitments under the Memorandum of Understanding signed in October 2013 and after fast-tracking the law ratifying the MoU by early April 2014.

Office space at the UN House, a prime location in Bucharest, is allocated to the Council of Europe rent free.

The Ministry of Justice, Directorate for Investigation of Organised Crime and Terrorism Offences within the Prosecution Office attached to the High Court of Cassation (DIICOT), the Romanian National Police, the National Institute of Magistracy and the Computer Emergency Response Team (CERT-RO) are seeking close co-operation with the Office regarding substantive matters and are contributing expertise to project activities or receiving study visits from project countries.

The Office is regularly invited to participate and speak in national, regional and international meetings on cybercrime, cybersecurity, organised crime and related matters taking place in Romania.

# 7 Administrative and financial matters

## 7.1 Staff

Between October 2017 and September 2018, the number of staff increased from 21 to 29.

The Office is headed by the Executive Secretary of the Cybercrime Convention Committee (Head of the Cybercrime Division) who divides his time between Strasbourg and Bucharest. This arrangement ensures that activities of the T-CY and C-PROC remain closely linked.

Given the increase in staff and resources managed at C-PROC, a Head of Operations (with Cost Centre Manager functions) was recruited in July 2017 who is also the Cost Centre Manager.

By September 2018, the Office thus had one internationally recruited Head of Operations (A2 level), five internationally recruited project managers (A1/2 level) and 14 locally recruited staff (ten project officers at B4/5 level, two finance assistants at B3 level, and ten project assistants at B2 level).

The staff originated from nine different member states. They were funded from project budgets and their exclusive responsibility is project implementation.

It is expected that four to five further positions will need to be filled in the coming months. This would then take the total number of staff to 34 which is the maximum capacity that the Office will be able to accommodate.

The level of expertise on cybercrime and electronic evidence within the Office has increased considerably during the past two years. This not only contributes to further improving the quality of project activities but also makes the Office a valuable source of subject-matter knowledge.

### 7.2 Financial matters

All costs of C-PROC, with the exception of the salary of the Head of Office, are covered by extra-budgetary resources:

- Office space is provided rent-free by the Government of Romania;
- All staff – with the exception of the Head of Office – is funded from the budgets of projects for which they are responsible;[12]
- Initial office furniture and IT equipment were funded by a voluntary contribution from the United Kingdom or are now funded from the budgets of the respective projects;
- Office running costs are directly funded by the lines for eligible local office costs and overheads of project budgets.

As projected, implementation of capacity-building projects from Bucharest is more cost effective and ensures a more favourable ratio of operational over staff and administrative cost when compared to Strasbourg. In the period April 2014 to September 2018, savings for staff amounted to approximately EUR 2.6 million and for office costs to EUR 1.2 million, that is, some EUR 3.8 million in total.

Implementation of projects by C-PROC is and will remain cost-effective and thus attractive for donors.

## 8 Visibility

C-PROC contributes to the visibility of the Council of Europe in cybercrime matters for example through the website (www.coe.int/cybercrime), by contributing to the Octopus Community and its tools, by disseminating twice per month a Cybercrime Digest and by publishing a quarterly Cybercrime@COE Update.

## 9 Conclusions and priorities

The following conclusions can be drawn:

- 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 an effective way to help societies in any part of the world address the key challenge of cybercrime;

- C-PROC projects are supporting implementation of the Budapest Convention and follow up, or contribute to the work of the Cybercrime Convention Committee. The “dynamic triangle” combining common standards (Budapest Convention), with follow-up through the T-CY and capacity-building through C-PROC, remains highly effective. Given the current budgetary challenges of

[12] The position is funded from overheads generated by projects implemented by C-PROC.

the Council of Europe, it is most valuable that the T-CY can rely on voluntary contributions through the project Cybercrime@Octopus to ensure that the preparation of the 2nd Additional Protocol to the Budapest Convention can proceed;

- The Budapest Convention is among the Council of Europe treaties with broadest membership and global reach.[13] With each new Party, the Budapest Convention and international co-operation on cybercrime will become more effective. As all but one member states are Parties or Signatories, additional Parties will be non-member states of the Council of Europe. Between October 2017 and September 2018, Argentina, Cabo Verde, Costa Rica, Morocco, Paraguay and Philippines became Parties. The Office contributes to ensuring that prospective and actual Parties have the capacity to apply the Budapest Convention;

- C-PROC is 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 2018, projects with a volume of more than EUR 26 million were underway;

- The European Union remains the main donor through joint projects co-funded by the Council of Europe. Between October 2017 and September 2018 voluntary contributions have also been received by Estonia, Japan, Monaco, the United Kingdom and in particular the USA to the project Cybercrime@Octopus;

- The Government of Romania is making office premises available rent free but is also supporting it through expertise. The Ministry of Justice, the National Police, the Prosecution Service (DIICOT), the National Institute of Magistracy and the Computer Emergency Response Team are seeking close co-operation with the Office, are project partners or 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 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 forthcoming twelve months are:

[13] Only surpassed by the joint Council of Europe /OECD Convention on Mutual Administrative Cooperation in Tax Matters (ETS 127) and the Convention on the Transfer of Sentenced Persons (ETS 112)

- Emphasis on human rights and rule of law safeguards: cybercrime undermines human rights, democracy and the rule of law. At the same time, the fight against cybercrime carries risks. C-PROC projects help address risks and strengthen these core values in all regions of the world, among other things, through the development of specific legislation with safeguards, standardised procedures and a strong emphasis on the training of judges. The Office will increasingly support the development of data protection legislation in line with the modernised Data Protection Convention 108 and in co-operation with the Data Protection Unit of the Council of Europe;

- Protecting children against online sexual violence and other measures against cyberviolence: a new project on ending child sexual exploitation "End Online Child Sexual Exploitation and Abuse @Europe" commenced in the second half of 2018, in co-operation with the Children's Rights Division of the Council of Europe and on the basis of the standards of the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. This is a further example of synergies within the Organisation. C-PROC will furthermore start to establish an online resource on cyberviolence as agreed by the T-CY in July 2018;[14]

- 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 implement the Budapest Convention. Some of these projects will come to an end within a few months. A new regional joint project on cybercrime for the Eastern Partnership will need to be prepared and negotiated. The same is true with regard to follow up to the iPROCEEDS project for South-eastern Europe. And further funding for global activities will be sought;

- Enhancing the expertise of the Office: the role of C-PROC as a centre of subject-matter knowledge will be further increased through the Octopus Community, training materials and technical reports. Already now, the Office is a unique source of information on cybercrime legislation worldwide. Steps will be taken for the further training of current and for attracting additional competent staff to achieve this objective.

The expectations linked with the establishment of the Office have been met and the conditions for its further development are in place.

It is proposed that the Office continue to operate under the current arrangement.

[14] See the recommendations of the T-CY Mapping Study on Cyberviolence.

# 10 Appendix: Inventory of activities supported by C-PROC (October 2017 – September 2018)

## October 2017

| | |
|---|---|
| Cybercrime@Octopus | CyFy 2017: The India Conference on Cyber Security and Internet Governance, New Delhi, India, 3-4 October 2017 |
| GLACY+ | Participation of 2 Philippines delegates in the Cybertipline Roundtable, Alexandria, Virginia, USA, 3-5 October 2017 |
| iPROCEEDS | Regional workshop on guidelines and indicators to prevent and detect online crime proceeds, Ljubljana, Slovenia, 4-5 October 2017 |
| CyberCrime@EAP III | Co-operation memorandum: Support to Internet Governance Forum 2017 Ukraine, Kyiv, Ukraine, 6 October 2017 |
| CyberCrime@EAP II,<br>iPROCEEDS | Regional Conference on Cybercrime, Baku, Azerbaijan, 9-11 October 2017 |
| GLACY+ | Support to the national delivery of Intro Course on cybercrime and electronic evidence for Judges and prosecutors, Santo Domingo, Dominican Republic, 10-13 October 2017 |
| CyberSouth | Scoping mission in Tunisia, Tunis, Tunisia, 11 October 2017 |
| GLACY+ | Meeting with cybercrime investigations heads of unit from the region to discuss operational activities and plan and organise a joint operation, Port Louis, Mauritius, 11-13 October 2017 |
| CyberSouth | Scoping mission in Algeria, Alger, Algeria, 12 October 2017 |
| CyberCrime@EAP III | Follow-up mission to Azerbaijan on various matters of public-private co-operation, Baku, Azerbaijan, 12-13 October 2017 |
| iPROCEEDS | Study visit on CSIRT/CERT Regulations and Operational Environment, Bucharest, Romania, 12-13 October 2017 |
| CyberCrime@EAP III | Support to participation of Belarus in COE/OSCE Conference on Internet Freedom, Vienna, Austria, 13 October 2017 |
| GLACY+ | Residential Workshop on Cybercrime and Electronic Evidence for District Judges and Magistrates, Kandy, Sri Lanka, 13-15 October 2017 |
| CyberCrime@EAP III | Follow-up mission to Armenia on various matters of public-private co-operation, Yerevan, Armenia, 16-17 October 2017 |
| GLACY+ | Advisory mission on cybercrime reporting and workshop on collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, Santo Domingo, Dominican Republic, 16-17 October 2017 |
| CyberSouth | Scoping mission in Lebanon, Beirut, Lebanon, 17-18 October 2017 |

| | |
|---|---|
| GLACY+ | UNODC Conference on Effective Responses to Online Child Sexual Exploitation in Southeast Asia, Bangkok, Thailand, 17-19 October 2017 |
| CyberCrime@EAP III | Follow-up mission to Georgia on various matters of public-private co-operation, Tbilisi, Georgia, 19-20 October 2017 |
| CyberCrime@EAP III | Follow-up mission to Belarus on various matters of public-private co-operation, Minsk, Belarus, 23-24 October 2017 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Tirana, Albania, 23-24 October 2017 (first part) |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Podgorica, Montenegro, 23-26 October 2017 |
| GLACY+ | Cybersecurity Week (to create public awareness and launch cyber security initiatives), Accra, Ghana, 23-27 October 2017 |
| CyberCrime@EAP II | Participation in ECTEG General Assembly on access to materials and planning of training for 24/7 in the EAP, Lisbon, Portugal, 26-27 October 2017 |
| iPROCEEDS | Workshop on inter-agency and international co-operation for search, seizure and confiscation of online crime proceeds, Podgorica, Montenegro, 26-27 October 2017 |
| GLACY+ | ICANN60 Annual General Meeting, Abu Dhabi, UAE, 28 October-3 November 2017 |
| iPROCEEDS | Advice and workshop on the preparation of interagency co-operation protocols, Podgorica, Montenegro, 26 October 2017 |
| iPROCEEDS | Workshop on domestic protocols for international sharing of intelligence and evidence, 27 October 2017 |
| CyberCrime@EAP III, iPROCEEDS | The 4th South East European Regional Forum on Cybersecurity and Cybercrime, Sofia, Bulgaria, 30-31 October 2017 |
| GLACY+ | GLACY+ Information session meetings with press and public sector, Bucharest, Romania, 31 October 2017 |

## November 2017

| | |
|---|---|
| CyberCrime@EAP III | Follow-up mission to Moldova on various matters of public-private co-operation, Kishinev, the Republic of Moldova, 2-3 November 2017 |
| iPROCEEDS | Regional workshop on obtaining and using electronic evidence, Bucharest, Romania, 2-3 November 2017 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Tirana, Albania, 6-7 November 2017 (second part) |

| | |
|---|---|
| CyberCrime@EAP III | Workshop on data retention and data preservation policy and practice, Baku, Republic of Azerbaijan, 6-7 November 2017 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Sarajevo, Bosnia and Herzegovina, 6-9 November 2017 |
| GLACY+ | Advanced Judicial Training for judges, magistrates and prosecutors, Accra, Ghana, 7-9 November 2017 |
| GLACY+ | Participation in the INTERPOL Cybercrime Training for the Pacific Region, Suva, Fiji, 6-10 November 2017 |
| GLACY+ | Advisory mission and workshop on Cybercrime Policies-Review of National Cybersecurity Policy & Strategy Document, Accra, Ghana, 9-10 November 2017 |
| CyberCrime@EAP III | Follow-up mission to Ukraine on various matters of public-private co-operation, 13-14 November 2017, Kyiv, Ukraine |
| iPROCEEDS | Cybercrime Coordination and Partnership Exercise, Pristina, Kosovo*[15], 13-16 November 2017 |
| CyberSouth | Assessment visit in Tunisia, Tunis, Tunisia, 13-17 November 2017 |
| CyberCrime@EAP III | Contribution to Georgian ICT Development and Cyber Security Event GITI 2017, Tbilisi, Georgia, 16-17 November 2017 |
| Cybercrime@Octopus | Participation in the 3rd National Cybersecurity Week, Mexico, 16-17 November 2017 |
| GLACY+ | INTERPOL Instructor Development Course, in SINGAPORE, with the participation of ALL GLACY+ countries, Singapore, 20-24 November 2017 |
| Cybercrime@Octopus | Global Forum on Cyber Expertise (GFCE), New Delhi, India, 21 November 2017 |
| GLACY+ | Participation in the second meeting of the Specialised Technical Committee on Communication and ICT formed by Ministers of Communication and Information Technologies from the African region, Addis Ababa, Ethiopia, 21 November 2017 |
| Cybercrime@Octopus,<br>GLACY+ | Participation in the Global Cyberspace Conference (GCCS2017), New Delhi, India, 23-24 November 2017 |

[15] *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.

| | |
|---|---|
| GLACY+, CyberCrime@EAP II, iPROCEEDS, Cybercrime@Octopus,<br>CyberSouth | 18th Plenary Meeting of the Cybercrime Convention Committee (T-CY) and the 1st Protocol Drafting Plenary, Strasbourg, France, 27-29 November 2017 |
| CyberSouth | Assessment visit in Lebanon, Beirut, Lebanon, 27-30 November 2017 |
| CyberSouth | Participation in the 3rd Anti-Cybercrime Forum, Beirut, Lebanon, 29 November 2017 |
| GLACY+ | GLACY+ Steering Committee, Strasbourg, France, 30 November 2017 |

### December 2017

| | |
|---|---|
| GLACY+ | Forum on the policies on cybercrime capacity-building by international/regional organisations – LATAM and CARIBBEAN, including Regional workshop on cybercrime and cybersecurity strategies with participation of Caribe/LATAM regional organisations combined with workshop on international co-operation for LATAM and Caribbean countries, Santo Domingo, Dominican Republic, 5-7 December 2017 |
| GLACY+ | Support to the regional delivery of Introductory Course on cybercrime and electronic evidence for Judges and Prosecutors of the Anglophone Countries of the ECOWAS REGION, Accra, Ghana, 5-8 December 2017 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Belgrade, Serbia, 4-7 December 2017 |
| iPROCEEDS | Cybercrime Coordination and Partnership Exercise, Belgrade, Serbia, 4-7 December 2017 |
| CyberSouth | Assessment visit in Algeria, Algiers, Algeria, 10-14 December 2017 |
| iPROCEEDS | 2nd semester Examination 2017, Master Programme in Forensic Computing and Cybercrime Investigation, Dublin, Ireland, 11-15 December 2017 |
| GLACY+ | International Workshop on Judicial Training Strategies, with the participation of all GLACY+ countries and all the ASEAN countries, Cebu, Philippines, 12-14 December 2017 |
| GLACY+ | The annual conference for all District Judges and Magistrates in Sri Lanka, Colombo, Sri Lanka, 18-19 December 2017 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds, Ankara, Turkey, 18-20 December 2017 |
| iPROCEEDS | Regional workshop on sharing good practices on reporting mechanisms in South-eastern Europe and Turkey, Skopje, “the former Yugoslav Republic of Macedonia”, 20 December 2017 |

| | |
|---|---|
| iPROCEEDS | The fourth meeting of the Project Steering Committee (PSC) of iPROCEEDS project, Skopje, "the former Yugoslav Republic of Macedonia", 21 December 2017 |
| Cybercrime@Octopus | Participation in the Workshop (WS149) on "Crime and jurisdiction in cyberspace – towards solutions" during IGF 2017, Geneva/Switzerland, 20 December 2017 |

## January 2018

| | |
|---|---|
| iPROCEEDS | Case simulation exercise on cybercrime and financial investigations, Sarajevo, Bosnia and Herzegovina, 15-18 January 2018 |
| GLACY+ | Advisory mission on harmonisation of legislation on cybercrime and electronic evidence, Kampala, Uganda, 16-18 January 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, Pristina, Kosovo*[16], 18 January 2018 |
| GLACY+ | Advisory mission on harmonisation of legislation on cybercrime and electronic evidence, Port-Louis, Mauritius, 22-24 January 2018 |
| GLACY+ | Advisory mission on the streamlining of procedures for mutual legal assistance (MLA) related to cybercrime and electronic evidence, Port-Louis, Mauritius, 25-26 January 2018 |
| iPROCEEDS | Meeting of MASAK with electronic money companies on guidelines and indicators for financial sector entities to prevent money laundering in the online environment, Ankara, Turkey, 30 January 2018 |

## February 2018

| | |
|---|---|
| GLACY+ | First Annual meeting and International Conference of the Ibero-American Cyber Network, with participation of Contact Points of the Cybercrime Forum of the PALOP countries, Lisbon, Portugal, 5-7 February 2018 |
| Cybercrime@Octopus | High Level Round Table Discussion on Budapest Convention in Malaysia, Kuala Lumpur, Malaysia, 6-7 February 2018 |
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies and update of the Online Resource, Yerevan, Armenia, 6 – 8 February 2018 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds to judges and prosecutors, Pristina, Kosovo*[16], 7-10 February 2018 |

[16] *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.

| | |
|---|---|
| Cybercrime@Octopus | Participation in the Expert Group Meeting (EGM) on Lawful Access to Digital Data Across Borders, Vienna, Austria, 12-13 February 2018 |
| GLACY+ | Participation in the Public Safety Working Group Inter-sessional Meeting, Brussels, Belgium, 12-13 February 2018 |
| iPROCEEDS | Meeting on Public-private co-operation for fighting cybercrime and online crime proceeds, Podgorica, Montenegro, 13 February 2018 |
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies and update of the Online Resource, Baku, Azerbaijan, 13-15 February 2018 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds (1st part), Skopje, “The former Yugoslav Republic of Macedonia”, 15-16 February 2018 |
| CyberSouth | Basic Training on Cybercrime and Electronic Evidence for Magistrates, Beirut, Lebanon, 16 February 2018 |
| GLACY+ | Advisory mission on the set up of the Cybercrime Division at the CID in Sri Lanka Police, Colombo, Sri Lanka, 19-21 February 2018 |
| Cybercrime@Octopus | Drug Online Course organised by the Central Directorate for Antidrug Services (C.D.A.S) and the Multiagency College of Advanced Studies for Law Enforcement Officials, Rome, Italy, 19-22 February 2018 |
| CyberSouth | Counter Terrorism Monitoring, Reporting and Support Mechanism (CT Morse) meeting, Brussels, Belgium, 20 February 2018 |
| iPROCEEDS | Meeting MASAK with virtual currency exchange on guidelines and indicators for financial sector entities to prevent money laundering in the online environment, Ankara, Turkey, 22 February 2018 |
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies and update of the Online Resource, Tbilisi, Georgia, 20-22 February 2018 |
| CyberCrime@EAP 2018 | Workshop on legal and practical aspects of co-operation between law enforcement and Internet service providers, Kishinev, Republic of Moldova, 26-27 February 2018 |
| Cybercrime@Octopus | Participation in the Global Internet and Jurisdiction Conference, Ottawa, Canada, 26-28 February 2018 |
| GLACY+ | Advisory mission on harmonisation of legislation on cybercrime and electronic evidence in Nepal, Kathmandu, Nepal, 26-28 February 2018 |
| GLACY+ | Basic judicial training on cybercrime and digital evidence for the Judicial Police, Kenitra, Morocco, 27 February-2 March 2018 |
| CyberSouth | EuroMed Justice Conference, Brussels, Belgium, 28 February 2018 |
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies and update of the Online Resource, Kishinev, Republic of Moldova, 28 February-2 March 2018 |

| | |
|---|---|
| Cybercrime@Octopus | Drafting of an Additional Protocol to the Budapest Convention, finalising and presenting the T-CY report on Cyberviolence, February-December 2018 |

## March 2018

| | |
|---|---|
| CyberSouth | Workshop on Responses to the challenge of cybercrime, Amman – Tareq, Jordan, 5 March 2018 |
| GLACY+ | Data Focus Conference, Jakarta and Surabaya, Indonesia, 5-8 March 2018 |
| iPROCEEDS | Introductory training module on cybercrime, electronic evidence and online crime proceeds (2nd part), Skopje, "The former Yugoslav Republic of Macedonia", 5-6 March 2018 |
| CyberSouth<br>CyberCrime@EAP 2018<br>GLACY+<br>iPROCEEDS | International conference on Judicial Co-operation in Cybercrime Matters, The Hague, Netherlands, 7-8 March 2018 |
| GLACY+ | Technical Review Meeting for the Digital Rights and Freedom Bill, Uyo, Akwa Ibom State, Nigeria, 8-10 March 2018 |
| iPROCEEDS | Meeting of MASAK with electronic money companies on guidelines and indicators for financial sector entities to prevent money laundering in the online environment, Ankara, Turkey, 9 March 2018 |
| GLACY+ | Participation in ICANN 61 Community Forum, San Juan, Puerto Rico, 10-15 March 2018 |
| GLACY+ | Meeting with cybercrime investigations heads of unit from the region to discuss operational activities and plan and organise a joint operation, Hong Kong, 12-16 March 2018 |
| GLACY+ | Advisory mission for the development of legislation on cybercrime and electronic evidence, Ouagadougou, Burkina Faso, 12-15 March 2018 |
| GLACY+ | Workshop on Cybercrime and Cybersecurity for The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Co-operation (BIMSTEC) Member Countries, Bangladesh, 13-15 March 2018 |
| iPROCEEDS | 2nd Western Balkans Integrative Internal Security Governance (IISG) Board Meeting, Ljubljana, Slovenia, 15-16 March 2018 |
| GLACY+ | Residential Workshop on Cybercrime and Electronic Evidence for District Judges and Magistrates, Colombo, Sri Lanka, 16-18 March 2018 |
| iPROCEEDS | Participation in the Second Cyber Security Conference, Sarajevo, Bosnia and Herzegovina, 20 March 2018 |

| | |
|---|---|
| GLACY+ | Participation in the ECTEG General Assembly and in the FREETOOL Showcase Event, The Hague, The Netherlands, 20-22 March 2018 |
| GLACY+ | Introductory Training of Trainers Course on Cybercrime and Electronic Evidence for Judges, Magistrates and Prosecutors of the ASEAN Region, Manila, Philippines, 20-23 March 2018 |
| CyberSouth | Project launching conference, Tunis, Tunisia, 21-23 March 2018 |
| iPROCEEDS | Workshop online financial fraud and credit card fraud, Sarajevo, Bosnia and Herzegovina, 21–22 March 2018 |
| Cybercrime@Octopus | Develop a study on legislation for Kuwait, 23 March 2018 |
| GLACY+ | Workshop on the streaming of MLA procedures related to cybercrime and electronic evidence, Dakar, Senegal, 26-27 March 2018 |
| CyberCrime@EAP 2018<br>GLACY+ | 2nd Regional Cybercrime Co-operation Exercise, Kishinev, Republic of Moldova, 27-30 March 2018 |

### April 2018

| | |
|---|---|
| GLACY+<br>CyberCrime@EAP 2018<br>iPROCEEDS<br>Cybercrime@Octopus<br>CyberSouth | Meeting of the United Nations Intergovernmental Expert Group on Cybercrime, Vienna, Austria, 3-7 April 2018 |
| iPROCEEDS<br>GLACY+<br>CyberCrime@EAP 2018<br>CyberSouth | T-CY Protocol Drafting Group meeting, Vienna, Austria, 6-7 April 2018 |
| CyberSouth | The 11th Middle East and North Africa Working Group Meeting on Cybercrime for Heads of Units, Algiers, Algeria, 4-5 April 2018 |
| GLACY+ | Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, Colombo, Sri Lanka, 4-6 April 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, Pristina, Kosovo*[17], 5 April 2018 |

[17] *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.

| | |
|---|---|
| iPROCEEDS | Meeting of the working group to elaborate/improve guidelines and indicators for financial sector entities to prevent money laundering in the online environment, Skopje, "The former Yugoslav Republic of Macedonia", 11 April 2018 |
| GLACY+ | Cyber Security and Cybercrime Policies for African Diplomats, Addis Ababa, Ethiopia, 11-13 April 2018 |
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies, Co-operation Memorandum and Online Resource, Kyiv, Ukraine, 11-13 April 2018 |
| GLACY+ | Initial Assessment Visit to Chile, Santiago, Chile, 16-19 April 2018 |
| iPROCEEDS | Case simulation exercise on cybercrime and financial investigations, Tirana, Albania, 16-19 April 2018 |
| GLACY+ | Integration of ECTEG materials in the training strategy for law enforcement officers, Accra, Ghana, 18-20 April 2018 |
| CyberCrime@EAP 2018 | Meeting of the Cybercrime Working Group at the Pompidou Group, Dublin, Ireland, 18-19 April 2018 |
| iPROCEEDS | Second national delivery of the introductory training module on cybercrime, electronic evidence and online crime proceeds, Podgorica, Montenegro, 19-20 April, 2018 (1st part) and 17-18 May 2018 (2nd part) |
| CyberCrime@EAP 2018 | Second Cyber Security Festival organised by Internet Development Initiative and University of Georgia, Tbilisi, Georgia, 20 April 2018 |
| CyberSouth | Participation in the 1st EuroMed Conference on Digital Evidence, Lisbon, Portugal, 23-25 April 2018 |
| GLACY+ | Initial Assessment Visit to Nigeria, Abuja, Nigeria, 24-27 April 2018 |
| CyberCrime@EAP 2018 | Advisory Mission on 24/7 Points of Contact – Functions and Institutional Setup, Yerevan, Armenia, 25-26 April 2018 |

### May 2018

| | |
|---|---|
| GLACY+ | Advisory mission on harmonisation of legislation on cybercrime and electronic evidence, Banjul, The Gambia, 2-4 May 2018 |
| iPROCEEDS<br>CyberCrime@EAP 2018 | Regional meeting on international co-operation on cybercrime and electronic evidence, Kyiv, Ukraine, 3-4 May 2018 |
| GLACY+ | Regional training of trainers on cybercrime and electronic evidence for first responders of the police forces, Dakar, Senegal, 7-11 May 2018 |
| Cybercrime@Octopus | Drug Online Course organised by the Central Directorate for Antidrug Services (C.D.A.S.) and the Multiagency College of Advanced Studies for Law Enforcement Officials, Rome, Italy, 7-11 May 2018 |

| | |
|---|---|
| CyberSouth | Study visit of specialised units on cybercrime in Lebanon, Beirut, Lebanon, 7-10 May 2018 |
| CyberSouth | Joint Advisory Mission to analyse ISF capabilities, Beirut, Lebanon, 8-11 May 2018 |
| GLACY+ | Residential Introductory Training on Cybercrime and Electronic Evidence for Prosecutors and Judges, Cebu, Philippines, 8-10 May |
| GLACY+ | INTERPOL meeting with cybercrime investigations heads of unit from the region to discuss operational activities and plan and organise a joint operation, Tehran, Iran, 8-10 May 2018 |
| iPROCEEDS | Support to participation at the MSc in Forensic Computing and Cybercrime Investigation University College Dublin - 3rd Semester Examination Session, Dublin, Ireland, 8-12 May 2018 |
| CyberSouth | CyFy 2018 Africa Conference, Tangier, Morocco, 10-12 May 2018 |
| GLACY+ | Lecture on the Budapest Convention, Cyber Security Master Programme LUISS University, Rome, Italy, 11 May 2018 |
| GLACY+ | GLACY+ Steering Committee, Vienna, Austria, 14 May 2018 |
| CyberSouth | Basic judicial training course on cybercrime and electronic evidence, Rabat, Morocco, 14-17 May 2018 |
| GLACY+<br>CyberCrime@EAP 2018<br>iPROCEEDS<br>Cybercrime@Octopus<br>CyberSouth | Participation in the 27th session of the UN Commission for Crime Prevention and Criminal Justice "Criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of co-operation at the national and international levels", Vienna, Austria, 14-18 May 2018.<br>Side-event on the state of cybercrime legislation (Council of Europe in partnership with the Governments of Argentina, Portugal, Romania, Sri Lanka and United Kingdom and the European Union), Vienna, Austria, 15 May 2018. |
| iPROCEEDS<br>GLACY+<br>CyberCrime@EAP 2018<br>CyberSouth | T-CY Protocol Drafting Group meeting, Vienna, Austria, 11-13 May 2018 |
| iPROCEEDS | Regional workshop on criminal justice statistics on cybercrime and electronic evidence, Bucharest, Romania, 14-15 May 2018 |
| iPROCEEDS | Case simulation exercise on cybercrime and financial investigations, Ankara, Turkey, 21-24 May 2018 |
| GLACY+ | Initial assessment visit to Costa Rica, San-José, Costa Rica, 21-24 May 2018 |

| | |
|---|---|
| CyberCrime@EAP 2018 | Workshop on Cybercrime Threats, Strategies and Online Resource, Minsk, Belarus, 22-24 May 2018 |
| iPROCEEDS | Second National Delivery of the Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Tirana, Albania, 30-31 May 2018 (1st part) |
| GLACY+ | DESK STUDY Analysis of the project of Cybercrime bill in Brazil, May – June 2018 |

### June 2018

| | |
|---|---|
| CyberCrime@EAP 2018 | Steering Committee and participation at EuroDIG 2018, Tbilisi, Georgia, 4-6 June 2018 |
| CyberSouth | Assessment visit in Jordan, Amman, Jordan, 4-6 June 2018 |
| GLACY+ | Initial assessment visit to Cape Verde, Praia, Cape Verde, 4-7 June 2018 |
| GLACY+ | Cybercrime Training organised by the Italian Police, Naples, Italy, 4-15 June 2018 |
| iPROCEEDS<br>CyberCrime@EAP 2018 | European Dialogue on Internet Governance (EuroDIG) 2018, Tbilisi, Georgia, 5-6 June 2018 |
| iPROCEEDS | Participation in the 3rd International Conference “Cyber Crime Trends and Threats: Europe and International Dimensions”, Nicosia, Cyprus, 11-12 June 2018 |
| GLACY+ | ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers (Live Data Forensics), Santo Domingo, Dominican Republic, 11-15 June 2018 |
| CyberCrime@EAP 2018 | Contribution to the Armenia Action Plan Steering Committee meeting, Yerevan, Armenia, 12 June 2018 |
| GLACY+ | Support regional meetings amongst relevant countries and international/regional organisation - Second Annual PILON Cybercrime Workshop: Combatting Online Child Abuse in the Pacific, Nuku’Alofa, Tonga, 12-15 June 2018 |
| iPROCEEDS | Second National Delivery of the Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Belgrade, Serbia, 12-15 June 2018 |
| GLACY+ | INTERPOL Instructor Development Course, Singapore, 18-22 June 2018 |
| Cybercrime@Octopus | Cybercriminality et Digital Evidence, Paris, 18-22 June 2018 |

| | |
|---|---|
| iPROCEEDS | Second National Delivery of the Introductory Judicial Training Module on Cybercrime, Electronic Evidence and Online Crime Proceeds, Tirana, Albania, 18-19 June 2018 (2nd part) |
| GLACY+ | Advanced Judicial Training Course on Cybercrime and Electronic Evidence for Judges, Magistrates and Prosecutors of the ASEAN Region, Cebu, Philippines, 19-22 June 2018 |
| CyberCrime@EAP 2018 | Advisory Mission on international co-operation through 24/7 points of contact and mutual legal assistance, Baku, Azerbaijan, 19-21 June 2018 |
| CyberSouth | CEPOL Co-ordination meeting, Budapest, Hungary, 26 June 2018 |
| GLACY+ | In-country workshop on Data Protection and INTERPOL tools and services, Santo Domingo, Dominican Republic, 26-28 June 2018 |
| GLACY+ | 3rd INTERPOL Digital Forensics Expert Group Meeting, Heathrow, United Kingdom, 27-29 June 2018 |
| GLACY+ | Participation in GFCE Working Group A Meeting - Cyber Security Policy & Strategy, The Hague, Netherlands, 28 June 2018 |
| Cybercrime@Octopus | Symposium at the Court of Cassation, International Criminal Law facing Cybercrime, Paris, 28 June, 2018 |

### July 2018

| | |
|---|---|
| Cybercrime@Octopus<br>GLACY+ | Advisory mission on cybercrime legislation in Samoa and Phase 1 – Stakeholders Training, Apia, Samoa, 2-3 July 2018 |
| GLACY+ | Workshop for Judges and Magistrates on cybercrime and electronic evidence, Apia, Samoa, 4-6 July 2018 |
| CyberCrime@EAP 2018<br>CyberSouth<br>GLACY+ | 19th Plenary Meeting of the Cybercrime Convention Committee and 2nd Protocol Drafting Plenary, Strasbourg, France, 9-11 July 2018 |
| iPROCEEDS | ECTEG Live Data Forensics Training, Pristina, Kosovo*[18] , 9-13 July 2018 |
| Cybercrime@Octopus<br>iPROCEEDS | Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime, Strasbourg, France, 11 July 2018 |
| Cybercrime@Octopus<br>iPROCEEDS<br>CyberSouth | Octopus Conference 2018 – Co-operation against Cybercrime, Strasbourg, France, 11-13 July 2018 |

[18] *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.

| | |
|---|---|
| GLACY+ | Visit of the AG of Nepal to Eurojust and Belgium, The Hague (The Netherlands), Brussels and Mechelen (Belgium), 16-20 July 2018 |
| GLACY+ | Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of Anglophone countries from the ECOWAS Region, Ghana, 17-20 July 2018 |
| GLACY+ | Annual CyberSecurity Bootcamp organised by OAS and INCIBE, in collaboration with Interpol, Europol and FIRST, Leon, Spain, 17-28 July 2018 |
| iPROCEEDS | First preparatory meeting to develop a Cybercrime Exercise Scenario (C-PROC and Consultants), Bucharest, Romania, 23-25 July 2018 |
| GLACY+ | Integration of ECTEG training materials into the law enforcement training academies and other professional law enforcement training bodies, Port Louis, Mauritius, 30 July - 1 August 2018 |
| CyberSouth | Adaptation of the judicial training course, Strasbourg, France, 30 July – 3 August 2018 |

### August 2018

| | |
|---|---|
| GLACY+ | Special Programme on Cybercrime and Electronic Evidence for Supreme Court Justices, Port Louis, Mauritius, 1-3 August 2018 |
| Cybercrime@Octopus | Comparative analysis of legal framework of Qatar, August 2018 |
| GLACY+ | ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers, Manila, Philippines, 13-18 August 2018 |
| GLACY+ | ECTEG Course, Cybercrime and Digital Forensics Specialised Training for Law Enforcement Officers, Nuku'alofa, Tonga, 20-24 August 2018 |
| GLACY+ | Advisory mission on cybercrime legislation in Vanuatu. Elaboration/revision of the legislative framework on Cybercrime and electronic evidence and Awareness workshop on the Budapest Convention, Vanuatu, 20-24 August 2018 |
| CyberSouth | Advisory mission on 24/7 contact point, Tunis, Tunisia, 27 August 2018 |
| GLACY+ | Advanced Judicial Training Course on Cybercrime and Electronic Evidence for Judges, Prosecutors and other Judicial Officers of the Pacific Region, Nuku'alofa, Kingdom of Tonga, 27-30 August 2018 |
| GLACY+ | Joint International Workshop for Cybercrime Investigation Units and MLA Central Authorities, Singapore, 27-31 August 2018 |
| Cybercrime@Octopus | International Symposium on Cybercrime Response, Seoul, Republic of Korea, 29-31 August 2018 |

| | |
|---|---|
| CyberSouth | Advisory mission for an expert's workshop to discuss the opportunities on adopting a cybersecurity strategy, Aramoun, Lebanon, 29-30 August 2018 |
| GLACY+ | Integration/mainstreaming of training modules on Cybercrime and Electronic Evidence into Judicial Training Curricula of training institutions, Nuku'alofa, Tonga, 30 August 2018 |
| Cybercrime@Octopus<br>GLACY+ | Support to the 11th India Security Summit, New Delhi, 31 August 2018 |

### September 2018

| | |
|---|---|
| CyberSouth | Awareness raising meeting on the Budapest Convention and its instruments, Alger, Algeria, 2 September 2018 |
| CyberCrime@EAP 2018<br>GLACY+<br>iPROCEEDS<br>CyberSouth | Underground Economy Conference 2018, Strasbourg, France, 4-7 September 2018 |
| GLACY+ | Participation in the 4th Americas INTERPOL Working Group Meeting on Cybercrime for Heads of Units, Rio de Janeiro, Brazil, 4-6 September 2018 |
| CyberSouth | Awareness-raising meeting on the Budapest Convention and its instruments, Tunis, Tunisia, 6-7 September 2018 |
| GLACY+ | Data Protection Legislation Drafting Residential Workshop, Calabar, Nigeria, 10-14 September 2018 |
| CyberCrime@EAP 2018 | Table-top exercise on international co-operation on cybercrime, Yerevan, Armenia, 10-11 September 2018 |
| iPROCEEDS | Meeting on public-private co-operation for fighting cybercrime and online crime proceeds, Brcko District, Bosnia and Herzegovina, 11 September 2018 |
| CyberSouth | Basic Judicial Training, Beirut, Lebanon, 11-15 September 2018 |
| Cybercrime@Octopus | Informal meeting on cybercrime of the G77 Group of States, Vienna, Austria, 11-12 September 2018 |
| iPROCEEDS | Meeting on public-private co-operation for fighting cybercrime and online crime proceeds, Banja Luka, Republika Srpska, Bosnia and Herzegovina, 12 September 2018 |
| CyberSouth | ECTEG meeting on first responders training, Brussels, Belgium, 13 September 2018 |

| | |
|---|---|
| CyberCrime@EAP 2018 | Table-top exercise on international co-operation on cybercrime, Baku, Azerbaijan, 13-14 September 2018 |
| Cybercrime@Octopus | T-CY Protocol Drafting Group, Strasbourg, France, 17-19 September 2018 |
| CyberSouth | Study visit cybercrime unit, forensic unit and CERT, Bucharest, Romania, 17-18 September 2018 |
| GLACY+<br>iPROCEEDS<br>CyberSouth<br>CyberCrime@EAP 2018 | Meetings of heads of cybercrime units and/or criminal investigation departments (CID) to share experience under the project with other countries. Participation in 6th INTERPOL – Europol Cybercrime Conference, Singapore, 18-20 September 2018 |
| iPROCEEDS | Participation in the Regional Ministerial Conference on High-Tech Crime and Information Security "Connect securely!", Belgrade, Serbia, 20-21 September 2018 |
| CyberSouth | Basic Judicial Training, Alger, Algeria 23-27 September 2018 |
| GLACY+ | Participation in the Pacific Judicial Conference, Apia, Samoa, 24 September 2018 |
| CyberCrime@EAP 2018 | Workshop on Law Enforcement and CSIRT/CERT Co-operation on Cybercrime, Kyiv, Ukraine, 24-26 September 2018 |
| iPROCEEDS | Second preparatory meeting to finalise the Cybercrime Exercise Scenario (C-PROC, consultants), Bucharest, Romania, 24-26 September 2018 |
| GLACY+ | Advisory mission on cybercrime legislation for Chile, in co-operation with the OAS, Washington DC, USA, 24-26 September 2018 |
| GLACY+ | Nigeria Conference on Cybercrime and Electronic Evidence<br>(NaCCEE 2018), Abuja, Nigeria, 26-28 September 2018 |
| GLACY+ | Participation in the bi-annual Policy Network Meeting in the Pacific, organised by the Australian Federal Police, Fiji, 26-28 September 2018 |
| GLACY+ | Forum on Internet Freedom in Africa (FIFAfrica), Accra, Ghana, 26-28 September 2018 |
| CyberCrime@EAP 2018 | Support to Internet Governance Forum and Youth IGF 2018 of Ukraine, Kyiv, Ukraine, 27-28 September 2018 |
| CyberSouth | OSCE meeting, Rome, Italy, 27-28 September 2018 |