COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 24 November 2017

**Information Documents**
**SG/Inf(2017)42**

# The Council of Europe Office on Cybercrime in Bucharest

## C-PROC activity report for the period October 2016 – September 2017

# 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 2016 to September 2017.[1]

In response to the need for enhanced capacity-building on cybercrime worldwide, on 9 October 2013 (at its 1180th meeting), the Committee of Ministers decided that the Council of Europe would establish a Programme Office on Cybercrime in Bucharest. The Office became operational on 7 April 2014, and all capacity-building activities on cybercrime since are being implemented by this Office. The Office is funded from extra-budgetary resources.

Between October 2016 and September 2017 the Office supported approximately 175 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.

By September 2017, the Office managed on-going projects with a combined budget of more than EUR 24 million and with 21 staff (from ten different member states). It was headed by the Head of Cybercrime Division (DG1) who divided his time between Strasbourg and Bucharest. He is supported as from July 2017 by a Head of Operations.

All staff – with the exception of the Head of Office – are funded from the budgets of projects for which they are responsible, and operational costs are covered through project budgets.

C-PROC is located at the UN House in Bucharest and is provided rent-free by the Government of Romania. The UN House was renovated in 2017.

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 and other relevant standards, follow up and assessments by the Cybercrime Convention Committee and capacity-building by C-PROC.

[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

- A large number of activities are being carried out in an efficient and cost-effective manner through the Office. Conditions are in place to further expand the Office and to absorb and manage additional resources.

- The Office is attractive to donors. The Office had started in April 2014 with projects with a volume of approximately EUR 4 million. By September 2016 the volume had increased to EUR 22 million and by September 2017 to more than EUR 24 million. Most of the funds come from Joint Projects with the European Union.

- 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.

With the projects currently underway, C-PROC has a solid basis to make an impact over the next two to three years. Additional funding would nevertheless be necessary, notably for projects in the Eastern Partnership region, for support to the Cybercrime Convention Committee, for support to implementation of the Protocol on Xenophobia and Racism and for the protection of children against online violence.

# 1 Background and purpose of this report

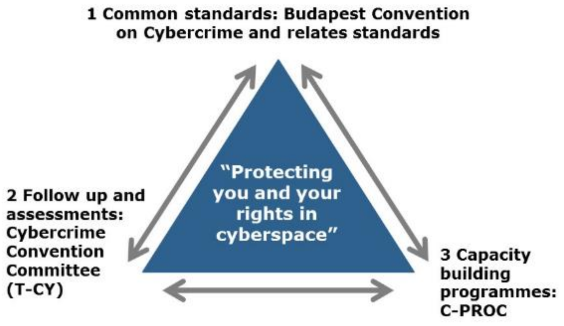
The purpose of the present report is to inform the Committee of Ministers of the Council of Europe of the activities of the Council of Europe Programme Office on Cybercrime (C-PROC) in Bucharest, Romania, during the period October 2016 to September 2017.

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 to 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 sexual exploitation, the theft of personal data, racism and xenophobia, money laundering or terrorism – is likely to entail cybercrime or electronic evidence.

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

- The Budapest Convention on Cybercrime (ETS 185) which was opened for signature in 2001[2] and which, sixteen years later, remains the most relevant international agreement on this issue. By September 2017, 56 States were Parties and a further 14 have signed it or been invited to accede.


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 71 member and observer states[3] and eleven observer organisations, the T-CY appears to have become the main intergovernmental body on cybercrime internationally.

[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] 56 Parties, 14 signatories or states invited to accede as well as the Russian Federation.

- Capacity-building on cybercrime has been an essential element of the approach of the Council of Europe from 2006 onwards, when the first phase of the Global Project on Cybercrime was launched. The international community has since reached broad 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,[4] 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, responded to the need for the Council of Europe to enhance its own capacities for supporting capacity-building worldwide.

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

The decision was linked to 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 by extra-budgetary resources.

Experience after 42 months of operations confirms that these expectations are being met.

[4] On 9 October 2013 at its 1180th meeting.

# 2 Mandate of the Office[5]

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 2016 – September 2017

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.[6] The Office meets its purpose through capacity-building projects.

## 3.1 Overview of current projects

In the period October 2016 to September 2017, C-PROC supported some 175 activities[7] under the following projects:

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

[6] 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.

[7] See Appendix for the list of activities.

| Project title | Duration | Budget | Funding |
|---|---|---|---|
| Cybercrime@Octopus | Jan 2014 – Dec 2019 | EUR 3.5 million | Voluntary contributions (Estonia, Hungary, Monaco, Romania, Slovakia, United Kingdom, Japan, United States of America and Microsoft) |
| Cybercrime@EAP II on international co-operation in the Eastern Partnership region | May 2015 – Dec 2017 | EUR 800,000<br>CoE 10% | EU/CoE JP (Partnership for Good Governance) |
| Cybercrime@EAP III on public/private co-operation in the Eastern Partnership region | Dec 2015 – Dec 2017 | EUR 1.2 million<br>CoE 10% | EU/CoE JP (Partnership for Good Governance) |
| GLACY project on Global Action on Cybercrime | Nov 2013 – Oct 2016 | EUR 3.35 million<br>CoE 10% | EU/CoE JP |
| GLACY+ project on Global Action on Cybercrime Extended | Mar 2016 – Feb 2020 | EUR 10 million<br>CoE 10% | EU/CoE JP |
| iPROCEEDS project targeting proceeds from crime on the Internet in South-Eastern Europe and Turkey | Jan 2016 – June 2019 | EUR 5.56 million<br>CoE 10% | EU/CoE JP |
| CyberSouth project on capacity-building in the Southern Neighbourhood | July 2017 – June 2020 | EUR 3.33 million<br>CoE 10% | EU/CoE JP |

By September 2017, projects with a combined volume of approximately EUR 24.4 million were being implemented by C-PROC.

This represents a sizeable increase compared to September 2015 (EUR 6 million), and a further increase compared to September 2016 (EUR 22 million).

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

## 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.

Under this project, the Office supported, for example, an assessment visit to Kazakhstan (June 2017), a meeting on cybercrime in India (August 2017), and a desk review of the draft law on cybercrime of Lebanon (May 2017). In September 2017, the project organised a meeting of the 24/7 network of contact points established under Article 35 Budapest Convention at EUROPOL in The Hague.

The project permits partnerships with other organisations. In co-operation with the Organization of American States (OAS), a workshop was conducted in Buenos Aires in June 2017 to strengthen networking among specialised cybercrime prosecutors from countries of Latin America, and in September 2017, a Cybersecurity Forum of the OAS in Uruguay was supported. In June 2017, the project contributed to an ECOWAS Cyber Strategy Workshop in Nigeria. In September 2017, the project supported the annual EUROPOL/INTERPOL conference on cybercrime in The Hague.

The project facilitates the design of new projects. For example, a planning workshop held in Bucharest for experts from Algeria, Jordan, Lebanon, Morocco and Tunisia in March 2017 resulted in the new project CyberSouth, which then commenced in July 2017.

The Octopus Conferences are also organised through this project. For example, from 16 - 18 November 2016, the Octopus Conference on Co-operation against Cybercrime was held in Strasbourg in conjunction with the 15th anniversary of the Budapest Convention on Cybercrime. The next Octopus Conference is scheduled for 11 – 13 July 2018.

Importantly, Cybercrime@Octopus is designed to support the Cybercrime Convention Committee (T-CY). For example, the project funded T-CY visits to Panama in December 2016 and to Argentina, Chile and Costa Rica in March 2017. These resulted in accession by Chile and Costa Rica, submission of the accession act to the Parliament of Argentina and submission of a new law on cybercrime to the Parliament of Panama.

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. 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.

Cybercrime@Octopus represents 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.

Overall, Cybercrime@Octopus remains a flexible tool to respond to needs, strengthen legislation, promote multi-stakeholder partnerships and support the T-CY in a pragmatic manner. The project has, therefore, been extended to December 2019 with an increased budget.[8]

### 3.3 Cybercrime@EAP II – International co-operation

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

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

Building on the results achieved in its first year of implementation, between October 2016 and September 2017, the project continued 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 setup and capabilities and skills necessary to ensure effective international co-operation on cybercrime and electronic evidence.

Important progress has been made:

- 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.

[8] It remains to be fully funded.

- Templates for standardised requests for mutual legal assistance (Article 31 Budapest Convention) and data preservation (Article 29/30 of the Convention) were developed and an online resource on international co-operation in the Octopus Community was prepared and tested in this region.

- 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.

Moreover, a detailed report on "Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play" was prepared and presented at the Eastern Partnership Rule of Law Panel in Brussels in June 2017. The report points at priorities for capacity-building in this region in the coming years.

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

The Cybercrime@EAP III project, launched in 2016 and lasting until December 2017, aims at promoting co-operation between criminal justice authorities in the Eastern Partnership countries and service providers.

This project is the first of its kind in the region and experience in 2016 underlined the complexity of the matter.

Considering the progress made, the budget of the project was increased from EUR 700,000 to EUR 1.2 million. This increase allowed the project to respond to common challenges at the regional level and address country-specific needs through domestic activities.

Much of the work between October 2016 and September 2017 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 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 Armenia, Azerbaijan, Georgia and Ukraine. Written comments on draft laws were submitted to the authorities of these countries. In the Republic of Moldova, the project co-operated with the Venice Commission, which resulted in an Opinion on proposed amendments to laws in December 2016 and a follow up workshop in September 2017.

The strengthening of domestic legislation was also discussed 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 discussion of outstanding issues of such co-operation.

Through participation in the first ever international Cybercrime Co-ordination and Partnership Exercise, attendance of the European Dialogue on Internet Governance 2017, and Regional meetings of the project dedicated to safeguards and guarantees and co-operation with providers, the countries involved are able to exchange best practices and experience both among themselves and with international partners.

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 GLACY Project on Global Action on Cybercrime

GLACY was a joint project of the Council of Europe and the European Union with a global scope, which started in November 2013 and ended on 31 October 2016 with a closing conference in Bucharest.

Priority countries were Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga, since these countries had committed to join the Budapest Convention on Cybercrime.

Project partners were France, Romania, Turkey and the European Cybercrime Centre at EUROPOL.

As a result of GLACY:

- Mauritius, Senegal, Sri Lanka and Tonga became Parties to the Budapest Convention on Cybercrime. GLACY moreover generated interest in other countries, and some of them have in the meantime been invited to accede, that is, Cape Verde, Ghana and Nigeria.

- All seven priority countries now have laws in force or draft laws in parliament bringing their criminal law regarding cybercrime and electronic evidence into line with international standards, that is, the Budapest Convention.

- Modules on cybercrime and electronic evidence have been mainstreamed into the curricula of judicial training academies. Training materials have been developed and adapted, and pilot introductory and advanced courses have been delivered to more than 900 judges and prosecutors, with the train-the-trainer methodology having a multiplier effect.

- Cybercrime units in priority countries have been strengthened through training (for example, delivery of first responders and live data forensic courses), access to training materials (such as those developed by the European Cybercrime Training and Education Group, ECTEG), as well as tools (such as an updated Electronic Evidence Guide and a guide on Standard Operating Procedures). Tools and materials are also available at the Octopus Community. Some 600 officers participated in training activities, including the training of trainers.

- The seven priority countries are now in a better position to co-operate internationally on cybercrime and electronic evidence. For example, their cybercrime units, prosecution services and 24/7 points of contact have been linked up with counterparts in other jurisdictions as well as EUROPOL and INTERPOL. This facilitated operational co-operation on actual cases.

- Governments have improved their ability to assess progress made in the investigation, prosecution and adjudication of cybercrime and other cases involving electronic evidence, even if reliable criminal justice statistics on cybercrime and electronic evidence remain a challenge. This was facilitated by GLACY, which started with analyses of the situation at the outset and ended with progress reviews.

- Engaging decision-makers was essential for the success of GLACY and will remain essential for the prevention and control of cybercrime. The results of progress reviews were fed back into the policy process and representatives of priority countries adopted a "Declaration on Strategic Priorities for Co-operation on Cybercrime and Electronic Evidence" at the GLACY Closing Conference (October 2016). These "Strategic Priorities" may serve as a blueprint to any country for comprehensive policies on cybercrime and e-evidence.

- The GLACY priority countries are now active members or observers in the Cybercrime Convention Committee.

The GLACY project is another example illustrating the functioning of the "dynamic triangle" of the Budapest Convention, the T-CY and capacity-building by C-PROC. It added credibility to the position of the Council of Europe and the European Union that capacity-building is one of the most effective ways ahead to address the problem of cybercrime at international levels.

At the meeting of the UN Intergovernmental Expert Group on Cybercrime (Vienna, April 2017), GLACY was presented as an example of good practice for capacity-building.

### 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 and will last until February 2020 with a budget of EUR 10 million. The launching conference was held in Bucharest in October 2016 back-to-back with the GLACY closing conference.

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).

Under GLACY+ most of the previous priority countries now serve as hubs to share their experience within their respective regions.[9] Additional priority countries

[9] Support to South Africa has been put on hold following communications by the authorities of South Africa.

committed to implementing the Budapest Convention have been added (such as Ghana and now also Cape Verde and Nigeria). Unlike GLACY, this project also supports Latin American countries. As the Dominican Republic is already a Party to the Budapest Convention, it is the first priority and hub country in this region.

In addition to priority countries, any country may benefit from support to the strengthening of legislation. For example, between February and June 2017, Panama and Guatemala were assisted in the drafting of their cybercrime laws.

GLACY+ serves as a tool to engage in co-operation with other organisations. For example, in July 2017, the Government of Mauritius, the International Organisation of Prosecutors and GLACY+ jointly organised the East Africa Regional Conference on Cybercrime and Electronic Evidence for 12 countries of that region.

Since the launch of GLACY+, an understanding has been reached with the Economic Community of West African States (ECOWAS) through which the ECOWAS Commission and the Council of Europe through GLACY+ and other projects will support countries of West Africa in the improvement of their legislation. A joint workshop for ECOWAS member states was held, for example, in September 2017. A similar agreement is now under discussion with the African Union Commission.

Given the progress made since the launch of GLACY+, discussions are now underway between the Council of Europe and the European Commission to further increase the budget and extend the duration of the project.

### 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[*] 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;

[*] 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.

- Co-operation between cybercrime, financial investigation and financial intelligence units;

- Public/private information sharing;

- Judicial training;

- International co-operation.

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

Following initial assessment visits to all project areas in spring 2016 and the launching conference held in “the former Yugoslav Republic of Macedonia” in June 2016, progress was made under all project components. For example:

- Advisory missions to all areas on the setting up or improvement of public reporting mechanisms.

- Review of judicial training curricula and update of training materials to mainstream cybercrime, electronic evidence and online financial investigations into the curricula of training academies as well as training of trainers for the delivery of courses.

- Meetings with multinational service providers to improve co-operation with law enforcement.

- Strengthening of interagency and international co-operation for the search, seizure and confiscation of proceeds from crime online.

- Training on darknet and virtual currency investigations.

- Participation of law enforcement officers from all project areas in the long-distance master’s programme on cybercrime investigations and computer forensics at University College Dublin.

- Guidelines for the prevention and detection of online crime proceeds.

iPROCEEDS is again a vehicle to engage in co-operation with numerous organisations such as EUROPOL, European Union Agency for Law Enforcement Training (CEPOL) and the UN Office on Drugs and Crime, as well as private sector organisations such as banking associations and Internet service providers.

The materials developed by iPROCEEDS will also be 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 complements and is part of the co-operation with neighbouring regions of the Organisation.

The project 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.

The project will focus 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 inception phase from July 2017 to January 2018 will be used for detailed assessments of legislation and institutional capacities and for the establishment of national country project teams.

The project launching conference is scheduled for January 2018.

While Morocco has been invited to accede to the Budapest Convention and has benefitted from capacity-building activities (such as GLACY and GLACY+) for some time, CyberSouth is expected to ensure the integration of other countries of the Southern Neighbourhood region into mainstream international efforts on cybercrime.

## 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:

- Continued and increased support to the Eastern Partnership region given that current Cybercrime@EAP projects are ending on 31 December 2017;
- 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;

- New project on the protection of children against online sexual violence on the basis of the Budapest and Lanzarote Conventions.

# 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.

Between October 2016 and September 2017 several T-CY activities were funded or co-funded from the budget of Cybercrime@Octopus, such as T-CY visits to Argentina, Chile, Costa Rica and Panama. In the T-CY plenaries of November 2016 and May 2017, Spanish interpretation was made available thanks to a USA contribution to the Cybercrime@Octopus project.

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

Following the signature of the Memorandum of Understanding in October 2013:

- The law ratifying the MoU was fast-tracked and published in the Official Gazette in early April 2014. The Office of the Deputy Prime Minister and the Ministry of Justice helped clear all issues regarding office space and related legal and administrative matters.

- Office space at the UN House, a prime location in Bucharest, was allocated to the Council of Europe. In 2015, additional space had been made available to allow for an expansion of the Office in view of the launch of new projects. In December 2016, an additional agreement was signed between the Council of Europe and the Romanian Ministry of Foreign Affairs regulating the use of the UN House by C-PROC. In summer 2017, the Government of Romania undertook important renovation work at the UN House. Security guards are provided by the Government of Romania.

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.

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 Premises

Office space in Bucharest is made available free of charge by the Government of Romania (see above, section 6).

## 7.2 Staff

Between October 2016 and September 2017, the number of staff increased from 18 to 21. In September 2015, C-PROC had six staff.

As proposed by the Secretary General, 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 (see above, section 5).

Given the increase in staff and resources managed at C-PROC, a Head of Operations (with Cost Centre Manager functions) was recruited and commenced his assignment on 1 July 2017. The position is funded from overheads generated by projects implemented by C-PROC.

By September 2017, the Office thus had one internationally recruited Head of Operations (A2 level), five internationally recruited project managers (A1/2 levels) and 14 locally recruited staff (six project officers at B4/5 levels, two finance assistants at B3 level, and six project assistants at B2 level).

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

Five additional positions were vacant and recruitment was in process. It is expected that two or three further positions will need to be filled in the coming months. This would then take the total number of staff to 29, which is the maximum capacity that the Office will be able to accommodate.

### 7.3 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 – are funded from the budgets of projects for which they are responsible.
- 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. In the period April 2014 to September 2017, savings for staff amounted to approximately EUR 1,500,000 and for office cost to EUR 700,000.

This makes it attractive for donors to fund projects for implementation by C-PROC.

## 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

- The Cybercrime Programme Office of the Council of Europe builds on an international consensus on capacity-building as an effective way to help societies in any part of the world address the key challenge of cybercrime. This consensus was affirmed once more at the UN Intergovernmental Expert Group on Cybercrime (Vienna, April 2017) where the joint project of the Council of Europe and the EU on Global Action on Cybercrime (GLACY) was considered an example of good practice. Through the Office, the Council of Europe remains a global leader for capacity-building on cybercrime and electronic evidence.

- The Budapest Convention (complemented by related instruments on data protection, child protection, terrorism or money laundering) is the reference standard for C-PROC projects which help ensure impact on the ground and add credibility to this treaty in all regions of the world. Between October 2016 and September 2017 – in addition to Andorra, Greece and Monaco – Chile, Costa Rica, Senegal and Tonga became Parties, and Cape Verde and Nigeria were invited to accede to the Budapest Convention.

- Capacity-building projects facilitate the participation of additional representatives of the 70 Parties and Observer states (signatories and those invited to accede) in the Cybercrime Convention Committee (T-CY). This in turn permits an inclusive approach to the drafting of an additional Protocol to the Budapest Convention, which commenced in September 2017.[10]

- These projects furthermore help ensure follow-up to recommendations of the T-CY. This demonstrates the effectiveness of a dynamic triangle combining common standards (Budapest Convention), with follow-up through the T-CY and capacity-building through C-PROC. Synergies between the inter-governmental work of the T-CY and capacity-building have been significantly strengthened since the Office was established.

- The portfolio of project covers priority regions in Europe (Eastern Partnership region, and South-East Europe and Turkey) as well as countries in other parts of the world committed to implement the Budapest Convention.

- 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 2017, projects with a volume

[10] In addition to COE member states, Australia, Canada, Chile, Japan, Mauritius, Senegal, Sri Lanka, Tonga and the USA participated in the first meeting of the Protocol Drafting Group in September 2017.

of more than EUR 24 million were underway. These were implemented by 21 staff, including a newly appointed Head of Operations, at C-PROC. A further 6 to 8 staff will be recruited in the coming months given the expansion of projects.

- The European Union remains the main donor. Between October 2016 and September 2017 additional voluntary contributions have also been received by Estonia, Hungary, Monaco, Slovakia, Japan and the United States of America for the project Cybercrime@Octopus.

- The Government of Romania offers rent-free premises to the Office but also supports 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.

The expectations linked with the establishment of the Office are thus being met. It is proposed that the Office continue to operate under the current arrangement.

# 10 Appendix: Inventory of activities supported by C-PROC (October 2016 – September 2017)

### October 2016

| | |
|---|---|
| iPROCEEDS | Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, Podgorica/Danilovgrad, Montenegro, 3-4 October 2016 |
| GLACY, GLACY+ | Progress review meetings and updated situation reports on GLACY project and Initial Assessment mission on GLACY+ project, Morocco, 3-6 October 2016 |
| GLACY+, Cybercrime@Octopus | INTERPOL Training on investigating cybercrime cases for investigators from African countries, Abuja, Nigeria, 3 - 7 October 2016 |
| CyberCrime@EAP III | Public-Private co-operation: Workshop on cybercrime and incident reporting framework including national CERT, Kishinev, Republic of Moldova, 6-7 October 2016 |
| GLACY+ | Workshop with the Heads of Cybercrime Units of African countries, Abuja, Nigeria, 10 - 11 October 2016 |
| GLACY+ | Initial Assessment mission for the project objectives, Accra, Ghana, 10-13 October 2016. |
| iPROCEEDS | Regional workshop to review the current state of judicial training curricular on cybercrime, electronic evidence and online crime proceeds, Zagreb, Croatia, 11-12 October 2016 |
| CyberCrime@EAP III | Public-Private co-operation: Workshop on co-operation between the law enforcement and ISPs, focusing on preservation, Baku, Azerbaijan, 12-14 October 2016 |
| GLACY+ | Participation in the UNTOC COP Side Event on Electronic Evidence and International Co-operation, Vienna, Austria,<br>18 October 2016 |
| iPROCEEDS | Participation in the EMPACT pilot training at CEPOL and collaboration with ECTEG on Darknets and Virtual Currencies, Budapest, Hungary, 19-21 October 2016 |
| CyberCrime@EAP II | Workshop on Electronic Evidence, Chisinau, Republic of Moldova, 20-21 October 2016 |
| iPROCEEDS / CyberCrime@EAP III | International meeting for Public-Private co-operation: meeting with foreign service providers, Dublin, Ireland, 24-25 October 2016 |
| GLACY, GLACY+ | International Closing Conference to discuss the results of the GLACY project, present the results of the statistics study and their impact on cybercrime policy, adopt the Declaration on Strategic Priorities, also combined with launching event for the GLACY+ project, Bucharest, 26-28 October 2016 |

### November 2016

| | |
|---|---|
| CyberCrime@EAP III | Legal package review of the Venice Commission on the Republic of Moldovan draft laws amending the legislation relating to the "security mandate" package, Kishinev, Republic of Moldova, 2-3 November 2016 |
| CyberCrime@EAP III | Roundtable discussion of procedural law reform: report presentation for Ukraine concerning legislative framework for procedural powers, Kyiv, Ukraine, 4 November 2016 |
| CyberCrime@EAP III | Workshop on best models in the EU and other states for public-private |

| | |
|---|---|
| | co-operation, Yerevan, Armenia, 7-8 November 2016 |
| CyberCrime@EAP III | Public-Private co-operation: Solutions for improved sharing of subscriber information (combined with GITI Information Security Day), Tbilisi, Georgia, 9-10 November 2016 |
| GLACY+<br>CyberCrime@EAP II<br>CyberCrime@EAP III<br>iPROCEEDS<br>Cybercrime@Octopus | Participation in the 16th plenary session of the Cybercrime Convention Committee (T-CY), Strasbourg, France, 14-15 November 2016 |
| GLACY+<br>CyberCrime@EAP II<br>CyberCrime@EAP III<br>iPROCEEDS<br>Cybercrime@Octopus | Participation in the Octopus Conference 2016, Strasbourg, France, 16-18 November 2016, 16-18 November 2016 |
| CyberCrime@EAP II | Workshop on EU co-operation in cybercrime and electronic evidence, Kyiv, Ukraine, 21-22 November 2016 |
| GLACY+ | Study visit by Moroccan law enforcement to the PHAROS team of the French National Police, Paris, France, 24 November 2016 |
| iPROCEEDS | Regional workshop for sharing international good practices on reporting mechanisms, Tirana, Albania, 25 November 2016 |
| GLACY+ | Participation at the 2nd Anti-Cybercrime Forum - Fighting Digital Fraud and Piracy in the Banking and Commercial Sectors in Lebanon, Beirut, 29 November 2016 |
| iPROCEEDS | Meeting of Implementing Partner Organizations Delivering The Western Balkans Integrated Internal Security Governance, Vienna, Austria, 30 November 2016 |

### December 2016

| | |
|---|---|
| GLACY+ | Participation in UNICRI Cyber Threats Master Class, Turin, Italy, 1-2 December 2016 |
| Cybercrime@Octopus | Participation in the Internet Governance Forum (IGF), Jalisco, Mexico, 6-9 December 2016 |
| CyberCrime@EAP II | Participation in the 4th Annual Meeting of the Cybercrime Working Group of the Pompidou Group, Strasbourg, France, 6 – 8 December 2016. |
| iPROCEEDS | Workshop on interagency and international co-operation for search, seizure and confiscation of online crime proceeds[4], Pristina, Kosovo*, 8-9 December 2016 |
| Cybercrime@Octopus | Seminar on "Internet, law and litigation", Paris, France, 9 December 2016 |
| iPROCEEDS | Regional workshop on Money Laundering risks related to new technologies and 2nd Steering Committee, Bucharest, 12-13 December 2016 |
| iPROCEEDS | Workshop on interagency and international co-operation for search, seizure and confiscation of online crime proceeds, Skopje, "The former Yugoslav Republic of Macedonia", 15-16 December 2016 |
| iPROCEEDS | Support in participation in long-distance master programme for 14 participants, July – December 2016 |

### January 2017

| | |
|---|---|
| GLACY+ | Advisory mission and workshop on cybercrime and cyber security policies and strategies, Dakar, Senegal  16-17 January 2017 |

| | |
|---|---|
| iPROCEEDS | Workshop on online financial fraud and credit card fraud, Belgrade, Serbia, 16-17 January 2017 |
| GLACY+ | Advisory mission and workshop on cybercrime and cybersecurity policies and strategies, Accra, Ghana, 19-20 January 2017 |
| iPROCEEDS | 14 law enforcement officers start the long-distance master programme on cybercrime investigation and computer forensics - University College Dublin, Ireland, Ireland, 23 January 2017 |
| CyberCrime@EAP III | Development of the cyberexercise as a preparatory work for the Co-ordination and partnership exercise, Tbilisi, Georgia, 23-25 January 2017 |
| GLACY+ | Participation in ICANN Capacity-building workshop for African law enforcement agencies (LEAs), Nairobi, Kenya, 25-26 January 2017 |
| CyberCrime@EAP II | Support to development and integration of judicial training on cybercrime and electronic evidence, Tbilisi, Georgia, 26-27 January 2017 |

### February 2017

| | |
|---|---|
| GLACY+ | Support meetings and activities carried out by regional and international organisations, The Hague, Netherlands, 3 February 2017 |
| CyberCrime@EAP III | Seminar on communication and information sharing with local Internet service providers, Kyiv, Ukraine, 8-9 February 2017 |
| CyberCrime@EAP III | Workshop on legal amendments related to cybercrime and electronic Evidence, Kyiv, Ukraine, 9-10 February 2017 |
| GLACY+ | Advisory mission on legislation on Cybercrime and Electronic Evidence, Guatemala City, Guatemala - 13-15 February 2017 |
| CyberCrime@EAP II | Workshop on reform of legislation to ensure compliance with Articles 16 and 17 of the Budapest Convention on Cybercrime, Baku, Azerbaijan, 13-15 February 2017 |
| CyberCrime@EAP III | Review of the package of legislative amendments related to cybercrime and electronic evidence and Roundtable Discussion on Reform of Cybercrime Laws and Regulations, Tbilisi, Georgia, 16-17 February 2017 |
| iPROCEEDS | Workshops on inter-agency and international co-operation for search, seizure and confiscation of online crime proceeds, Sarajevo, Bosnia and Herzegovina, 16-17 February 2017 |
| iPROCEEDS | Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, Skopje, "The Former Yugoslav Republic of Macedonia", 20-21 February 2017 |
| CyberCrime@EAP III,<br>iPROCEEDS | Development of the cyberexercise as a preparatory work for the Co-ordination and partnership exercise, Tbilisi, Georgia, 23-24 February 2017 |
| GLACY+,<br>CyberCrime@EAP II | Workshop on strengthening the 24/7 points of contact for cybercrime and electronic evidence organized in co-operation with another EU/CoE project GLACY+, as well as Interpol, Singapore, 27 February – 1 March 2017 |
| iPROCEEDS | Pilot training on Investigation on Darknet and Virtual Currencies, Bucharest, Romania, 28 February – 3 March 2017 |

### March 2017

| | |
|---|---|
| GLACY+ | Grant Agreement with INTERPOL for the implementation of the activities of Objective 2 – Law Enforcement Capabilities, 1 March 2017 – 29 February 2020 |
| Cybercrime@Octopus | Assessment and planning workshop for further capacity-building support |

| | |
|---|---|
| | to countries of the Mediterranean region, Bucharest, Romania, 6-7 March 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Yerevan, Republic of Armenia, 6 – 9 March 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Tirana, Albania, 13 March 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Baku, Republic of Azerbaijan, 13 – 16 March 2017 |
| GLACY+ | Support Regional Training of Trainers on Cybercrime and Electronic Evidence, with participation of West African countries, Dakar, Senegal, 14-17 March 2017 |
| GLACY+ | Development of cybercrime investigations, digital forensics capabilities, Colombo, Sri Lanka, 14-17 March 2017 |
| iPROCEEDS | Workshops on inter-agency and international co-operation, Tirana, Albania, 15-16 March 2017 |
| iPROCEEDS | Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, Ankara, Turkey, 15-16 March 2017 |
| Cybercrime@Octopus | T-CY visits on accession to the Budapest Convention (Costa Rica, Chile, Argentina), 16-24 March 2017 |
| GLACY+ | Study visit of the Philippines delegation to Mauritius CERT, Port-Louis, Mauritius, 23-24 March 2017 |
| CyberCrime@EAP III | Workshop on public-private partnerships in sector-specific approach, Minsk, Belarus, 23-24 March 2017 |
| iPROCEEDS | Advisory mission and workshop on online fraud and other cybercrime reporting mechanisms, Sarajevo, Bosnia and Herzegovina, 27-28 March 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Tbilisi, Georgia, 27 – 30 March 2017 |
| GLACY+ | International workshop on criminal justice statistics on cybercrime and electronic evidence, Accra, Ghana, 29-31 March 2017 |
| GLACY+ | Advisory mission on legislation on Cybercrime and Electronic Evidence, Panama City, Panama, 30-31 March 2017 |
| GLACY+ | Residential training on cybercrime and electronic evidence for Prosecutors, Panadura, Sri Lanka, 31 March – 2 April 2017 |
| Cybercrime@Octopus | Provide support to the T-CY Bureau (1) in the finalisation of the T-CY(2017)2 draft report on follow up given by Parties to the TCY(2013)17rev report on mutual legal assistance and (2) in the preparation of a TCY mapping study on cyber bullying and other forms of online violence, March – December 2017 |

**April 2017**

| | |
|---|---|
| GLACY+ | Introductory Cybercrime and Electronic Evidence Training of Trainers Course, Accra, Ghana, 3-7 April 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Kishinev, Republic of Republic of Moldova, 3-6 April 2017 |
| iPROCEEDS | Workshop on inter-agency co-operation and on international co-operation |

| | |
|---|---|
| | for search, seizure and confiscation of online crime proceeds, Ankara, Turkey, 3-4 April 2017 |
| GLACY+ | Participation in INTERPOL's 3rd Americas Working Group Meeting on Cybercrime for Heads of Units, Bridgetown, Barbados, 5-7 April 2017 |
| CyberCrime@EAP III | Workshop on the Cybercrime Law Reform, Kyiv, Ukraine, 6-7 April 2017 |
| iPROCEEDS | Meeting on public-private co-operation for fighting cybercrime and online crime proceeds, Belgrade, Serbia, 10 April 2017 |
| GLACY+,<br>CyberCrime@EAP II<br>iPROCEEDS | 3rd meeting of the UN Intergovernmental Expert Group on Cybercrime, Vienna, Austria, 10 – 13 April 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Kyiv, Ukraine, 10-13 April 2017 |
| iPROCEEDS | Workshop on inter-agency co-operation and on international co-operation for search, seizure and confiscation of online crime proceeds, Belgrade, Serbia, 19-20 April 2017 |
| CyberCrime@EAP III<br>iPROCEEDS | Co-ordination and Partnership Cyber Exercise, Georgia, Tbilisi, 24-28 April 2017 |
| GLACY+ | Malware Analysis Training organised by INTERPOL, Manila, Philippines, 24-28 April 2017 |
| GLACY+ | Training of trainers and development of training materials for basic and advanced modules for each country, Santo Domingo, Dominican Republic 24-28 April 2017 |

### May 2017

| | |
|---|---|
| CyberCrime@EAP III | Development of the Study on Strategy of Communications with Multinational Service Providers, May – June 2017 |
| GLACY+ | Review Meeting of the Training on Dark Web and Virtual Currencies, at EUROPOL, The Hague, 2-5 May 2017 |
| CyberCrime@EAP II | Training Programme on International Co-operation, including multinational ISPs, for the Eastern Partnership region, Minsk, Belarus, 2 – 5 May 2017 |
| CyberCrime@EAP III | Workshop on the Cybercrime Law Reform, Yerevan, Armenia, 3 – 5 May 2017 |
| CyberCrime@EAP III | Workshop on reform of legislation to ensure better compliance with the Budapest Convention on Cybercrime, Baku, Azerbaijan, 10 – 12 May 2017 |
| GLACY+ | Update Judicial training materials & creation of a bench book for magistrates – Brainstorming meeting, Bucharest, Romania, 15-16 May 2017 |
| CyberCrime@EAP III | Public Hearings on the Cybercrime Law Reform and Planning meeting, Kyiv, Ukraine, 17-19 May |
| GLACY+ | Introductory Cybercrime and Electronic Evidence Training of Trainers Course 22-25 May 2017, Rabat, Morocco |
| GLACY+ | National delivery of the Introductory Judicial Training of Trainers Course on Cybercrime and Electronic Evidence Koforidua, Ghana 22-26 May 2017, |
| iPROCEEDS | Support in participation in the summer examination 2017 of the Master Programme in Forensic Computing and Cybercrime Investigation, University College Dublin, Ireland, 22 May – 3 June 2017 |

| | |
|---|---|
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Sarajevo, Bosnia and Herzegovina, 22-23 May 2017 |
| GLACY+ | Pacific Islands Law Officers' Network Cybercrime Workshop, Nuku'alofa, Tonga, 23-25 May 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Ankara, Turkey, 25-26 May 2017 |
| GLACY+ | Advisory mission on the streamlining of procedures for Mutual Legal Assistance related to Cybercrime and Electronic Evidence, Nuku'alofa, Tonga, 26 May 2017 |
| Cybercrime@Octopus | First draft analysis of the provisions of the Electronic Transactions and Personal Data Bill of Lebanon against the requirements of the Budapest Convention and draft the necessary recommendations, 30 May 2017 |
| GLACY+ | Participation in the second Annual Meeting of the GFCE, Brussels, Belgium, 31 May - 1 June 2017 |
| Cybercrime@Octopus | Needs assessment visit and workshop on cybercrime and electronic evidence, Astana, Kazakhstan, 31 May – 2 June 2017 |

## June 2017

| | |
|---|---|
| CyberCrime@EAP III | Development of the Study on Liabilities of Internet Service Providers in the Eastern Partnership region, June – July 2017 |
| Cybercrime@Octopus | Regional Conference for Specialised Prosecution Services on Cybercrime and Electronic Evidence, Buenos Aires, Argentina, 1 – 2 June 2017 |
| GLACY+ | Lecture at the Specialized Training on International Criminal Law and Global Threats to Peace and Security, UNICRI, Turin, 5 June 2017 |
| GLACY+ | Participation in INTERPOL's 5th Eurasian Working Group meeting on Cybercrime for Heads of Units and in the Operational side-meeting on Business Email Compromise, Madrid, Spain, 5-8 June 2017 |
| CyberCrime@EAP II<br>CyberCrime@EAP III | Steering Committee meeting and participation in the Euro DIG 2017 conference, Tallinn, Estonia, 5-7 June 2017 |
| GLACY+<br>CyberCrime@EAP II<br>iPROCEEDS<br>Cybercrime@Octopus | 17th plenary meeting of the Cybercrime Convention Committee (T-CY), Strasbourg, France, 7-9 June 2017 |
| iPROCEEDS | 3rd meeting of the iPROCEEDS Project Steering Committee (PSC), Luxembourg, 12 June 2017 |
| iPROCEEDS | International workshop on search, seizure and confiscation of proceeds from crime online, Luxembourg, 12-13 June 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Podgorica, Montenegro, 13-14 June 2017 |
| GLACY+<br>CyberCrime@EAP II<br>iPROCEEDS | International Workshop on Cybercrime Training Strategies for Law Enforcement Agencies and access to ECTEG materials, Brussels, Belgium, 15-16 June 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Skopje, "the former Yugoslav Republic of Macedonia", 15-16 June 2017 |
| GLACY+ | Advisory mission on the streamlining of procedures for Mutual Legal Assistance related to Cybercrime and Electronic Evidence, Tagaytay City, Philippines, 19-20 June 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Pristina, Kosovo* , 19-20 June 2017 |

| | |
|---|---|
| GLACY+ | Regional LEA Trainer of Trainers course on Cybercrime and Electronic Evidence gathering, Dakar, Senegal, 19 – 26 June 2017 |
| iPROCEEDS | Regional training of trainers (ToT) on delivery of the introductory training module on cybercrime, electronic evidence and online crime proceeds, Budva, Montenegro, 20 -24 June 2017 |
| GLACY+ | Development of cybercrime investigations, digital forensics capabilities combined with National workshop and advice on interagency co-operation and public private collaboration to fight cybercrime, Manila, Philippines, 21-23 June 2017 |
| iPROCEEDS | Assessment mission of guidelines to prevent and detect/identify online crime proceeds, Belgrade, Serbia, 22-23 June 2017 |
| iPROCEEDS | Meeting on public-private co-operation for fighting cybercrime and online crime proceeds, Skopje, "the former Yugoslav Republic of Macedonia", 23 June 2017 |
| CyberCrime@EAP II | Participation in IAP Eastern European and Central Asian Regional Conference, Tbilisi, Georgia, 26-28 June 2017 |
| GLACY+ | Participation in the 59th ICANN Policy Meeting, Johannesburg, South Africa, 26-29 June 2017 |
| GLACY+ | ASEAN Regional meeting in view of sharing good practices and promote harmonisation of legislation on Cybercrime and EE as well as rule of law and human rights safeguards, Cebu City, Philippines, 27-29 June 2017 |
| CyberCrime@EAP II | 8th Eastern European and Central Asian Regional Conference of the International Association of Prosecutors, Tbilisi, Georgia, 28 June 2017 |
| iPROCEEDS | Meeting on public-private co-operation for fighting cybercrime and online crime proceeds, Pristina, Kosovo* , 29 June 2017 |

### July 2017

| | |
|---|---|
| GLACY+ | Advisory mission on CERT capacities, digital forensics lab and public-private co-operation, Nuku'alofa, Tonga, 3-5 July 2017 |
| CyberCrime@EAP III | Seminar on CSIRT/CERT Regulations and Operational Environment, Minsk, Republic of Belarus, 5-7 July 2017 |
| GLACY+ | Workshop on cybercrime reporting systems and collection and monitoring of criminal justice statistics on cybercrime and electronic evidence, Nuku'alofa, Tonga, 6 July 2017 |
| GLACY+ | Advisory mission and workshop on cybercrime and cybersecurity policies and strategies, Port Louis, Mauritius, 6-7 July 2017 |
| CyberCrime@EAP II | Advisory Mission on Findings and recommendations concerning 24/7 point of contact, Tbilisi, Georgia, 10-12 July 2017 |
| GLACY+ | East African Regional Conference on Cybercrime and Electronic Evidence, in collaboration with the GPEN and with the participation of regional and international organizations and relevant countries from the Eastern African Region, Pointe aux Piments, Mauritius, 10-12 July 2017 |
| GLACY+ | - Development of cybercrime investigations, digital forensics capabilities;<br>- In-country workshop and advice on interagency co-operation and public private collaboration to fight cybercrime, Nuku'alofa, Tonga, 10-14 July 2017 |
| GLACY+ | Nigeria invited to join the Budapest Convention on Cybercrime, Strasbourg, 11 July 2017 |
| GLACY+ | Residential workshop for High Court Judges on cybercrime and electronic evidence, Kalutara, Sri Lanka, 28-30 July 2017 |

| | |
|---|---|
| iPROCEEDS | Update of the basic course material on cybercrime, electronic and online crime proceeds following the regional training of trainers on delivery of the basic training module on cybercrime, electronic evidence and online crime proceeds for judges and prosecutors with the aim to be further delivered at the national level, desk study, July 2017 |

## August 2017

| | |
|---|---|
| iPROCEEDS | Preparatory meeting to agree on the aspects/elements, including technical solutions of the Cyber Exercise Scenario that need to be revised/updated/developed with the aim to be further replicated at the national level (C-PROC, consultants), Bucharest, Romania, 9-11 August 2017 |
| GLACY+ | Support to the Residential Workshop on Cybercrime and Electronic Evidence for Intake of New Judges, Colombo, Sri Lanka, 9-13 August 2017 |
| GLACY+ | - Development of cybercrime investigations, digital forensics capabilities;<br>- In-country workshop and advice on interagency co-operation and public private collaboration to fight cybercrime, Port Louis, Mauritius, 15-18 August 2017 |
| Cybercrime@Octopus | Translation in Arabic of the Budapest Convention and its explanatory report, Bucharest, Romania, 16 August 2017 |
| GLACY+ | Special training on cybercrime and electronic evidence for Nepal judicial officers, Kathmandu, Nepal, 16-20 August 2017 |
| GLACY+ | Support to the national delivery of Introductory Course on cybercrime and electronic evidence for prosecutors First Batch, Ada, Ghana, 17-18 August 2017 |
| GLACY+ | Support to the national delivery of Introductory Course on cybercrime and electronic evidence for prosecutors Second Batch, Kumasi, Ghana, 21-22 August 2017 |
| GLACY+ | Workshop for priority countries on data protection and overall police capabilities implemented by INTERPOL, Dakar, Senegal, 21-23 August 2017 |
| iPROCEEDS | Development of a Questionnaire on obtaining and using electronic evidence in criminal proceedings under the respective domestic legislation of the beneficiary countries, desk study, August 2017 |
| Cybercrime@Octopus | Participation at the 10th ASSOCHAM Annual Summit on Cyber and Network Security, New Delhi, India, 31 August 2017 |

## September 2017

| | |
|---|---|
| iPROCEEDS | Participation in the Underground Economy Conference 2017, Barcelona, Spain, 5 - 8 September 2017 |
| CyberCrime@EAP III | Seminar on memorandum of co-operation: technical details, and presentation of memorandum principles at Annual Telecom meeting of Ukraine, Kyiv, 7-8 September and Odessa, Ukraine, 9 – 10 September 2017 |
| CyberCrime@EAP III | 4th Regional meeting on public/private co-operation: Legislation, Safeguards and Co-operation with Service Providers, Kishinev, Republic of Republic of Moldova, 11-12 September 2017 |
| GLACY+ | Regional Conference on Harmonisation of legislation on Cybercrime and Electronic Evidence with rule of law and human rights safeguards, Abuja, Nigeria, 11-13 September 2017 |

| | |
|---|---|
| GLACY+ | ECTEG Course, Cybercrime and Digital Forensics Specialized Training for Law Enforcement Officers (Linux as an investigation tool), Accra, Ghana, 11-15 September 2017 |
| CyberCrime@EAP III | Workshop to support the review of Law 161 to follow up on an Opinion of the Venice Commission, Kishinev, Republic of Moldova, 14 September 2017 |
| Cybercrime@Octopus | Supports Training on Cybercrime and E-Evidence for Prosecutors in Argentina, Mendoza, Argentina, 14-15 September 2017 |
| iPROCEEDS | Online Financial Fraud and Credit Card Fraud Workshop, Podgorica, Montenegro, 18-19 September 2017 |
| CyberCrime@EAP II | Workshop on Support to development of the Law of Armenia on International Co-operation in Criminal Matters/Mutual Legal Assistance, Yerevan, Republic of Armenia, 19-20 September 2017 |
| GLACY+ | In Country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence, Kenitra, Morocco, 20-22 September 2017 |
| GLACY+ | Residential Workshop on Cybercrime and Electronic Evidence for District Judges and Magistrates, Colombo, Sri Lanka, 22-24 September 2017 |
| GLACY+ | Advisory mission on the streamlining of procedures for Mutual Legal Assistance related to cybercrime and electronic evidence, Rabat, Morocco, 25-26 September 2017 |
| GLACY+ | Participation at the GFCE Meeting on Global Good Practices, The Hague, Netherlands, 25-26 September 2017 |
| iPROCEEDS | Cybercrime Simulation Exercise on cybercrime and financial investigations, Skopje, "The former Yugoslav Republic of Macedonia", 25-28 September 2017 |
| GLACY+ | Introductory Cybercrime and Electronic Evidence Training of Trainers Course for the Pacific Region, Nuku'alofa, Tonga, 25-29 September 2017 |
| Cybercrime@Octopus,<br>GLACY+,<br>CyberCrime@EAP II,<br>iPROCEEDS | Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime, The Hague, Netherlands, 26-27 September 2017 |
| Cybercrime@Octopus | Participation in the Cybersecurity Forum and Symposium for the Americas region, Montevideo, Uruguay, 26-29 September 2017 |
| GLACY+,<br>CyberCrime@EAP II,<br>iPROCEEDS | Participation in the 5th INTERPOL – Europol Cybercrime conference, The Hague, Netherlands, 27-29 September 2017 |