COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 23 September 2015[1]

**Information Documents
SG/Inf(2015)35**

The Council of Europe Office on Cybercrime in Bucharest

C-PROC activity report for the period April 2014 – September 2015

---

[1] This document has been classified 'restricted' at the date of issue; it will be declassified in accordance with Resolution Res(2001)6 on access to Council of Europe documents.

Contents

Executive summary

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 would establish a Programme Office on Cybercrime in Bucharest, Romania. The Council of Europe Office on Cybercrime (C-PROC) became operational on 7 April 2014, and all capacity-building activities on cybercrime are now being implemented by this Office.

In the period April 2014 to September 2015, the Office supported some 110 activities under the projects Cybercrime@Octopus, CyberCrime@EAP I and II and Global Action on Cybercrime (GLACY).

By September 2015, the Office managed on-going projects with a combined budget of approximately EUR 6 million. The Office has eight staff (from five different member States) funded from extra-budgetary resources. It is headed by the Head of Data Protection and Cybercrime Division who divides his time between Strasbourg and Bucharest.

C-PROC is located at the UN House in Bucharest. With the start of additional extra-budgetary projects, the Office is likely to expand considerably. In anticipation of this growth, in July 2015, the Office relocated within the UN House and will now be able to accommodate up to 25 staff.

The experience of the initial 18 months of operations suggests the following:

▪ The Council of Europe is in a position to contribute substantially to capacity-building on cybercrime and electronic evidence worldwide. A large number of activities are being carried out in an efficient and cost-effective manner through the Office.

▪ The conditions are in place to expand the Office at any time in order to absorb and manage additional resources.

▪ The Office is attractive to donors. By September 2015, new projects with a volume of more than EUR 16 million are being prepared and are expected to commence between December 2015 and April 2016. Additional project proposals have been developed and more will follow in the future.

▪ The Office is funded by extra-budgetary resources. The Government of Romania has honoured its commitment and made premises available free of rent. Initial furniture and equipment was funded by a voluntary contribution by the United Kingdom in Spring 2014. Operational costs are covered through project budgets. All staff – with the exception of the Head

of Office – is funded from the budgets of projects which they are responsible for.

▪ Relevant authorities of the Government of Romania but also of other member States (currently Estonia, France, Germany and Turkey) as well as the European Cybercrime Centre at EUROPOL) are partners in C-PROC projects and contribute their expertise.

▪ Capacity-building projects of C-PROC follow up to results of the Cybercrime Convention Committee (T-CY) and contribute to the work of the T-CY. Synergies between the inter-governmental work of the T-CY and capacity-building have been further strengthened.

The expectations linked with the establishment of the Office have thus been metIt is proposed that the Office continue to operate under the current arrangements.

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 on the activities of the Council of Europe Office on Cybercrime (C-PROC) in Bucharest, Romania, during the period April 2014 to September 2015.[2]

Cybercrime – that is, 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.[3] Possibly a peripheral issue in the past, today any crime – be it fraud, or attacks against media, parliaments or public infrastructure, be it child abuse or other forms sexual exploitation, be it the theft of personal data, racism and xenophobia, money laundering, or be it the smuggling of persons – is likely to entail cybercrime or electronic evidence.

With the Budapest Convention on Cybercrime (ETS 185) of 2001[4], the Council of Europe, in co-operation with other States, succeeded in negotiating an international legal framework already at an early stage. Today, that treaty is more relevant than ever, not only for Europe but also other regions of the world. Following the recent accession by Sri Lanka and the ratification by Canada, 47 States are now Parties and another 19 have signed it or been invited to accede to it.

Follow-up to the Budapest Convention is ensured by the Cybercrime Convention Committee (T-CY). As from 2012, it 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 68 member and observer States[5] and eleven observer organisations, the T-CY appears to have become the main intergovernmental body on cybercrime internationally.

---

[2] Future reports will be provided on an annual basis as requested by the Deputies. The report complements quarterly External Presence Activity reports, reports to permit the external presence review (such as SG/INF)2015)25) and the internal 6-monthly review of the functioning of the C-PROC by the Secretary General.

[3] See "Cybercrime Breakfast Briefing" for Permanent Representations of Parties to the Budapest Convention, Strasbourg, 3 February 2015.

[4] 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.

[5] 47 Parties, 19 signatories or States invited to accede as well as the Russian Federation and San Marino.

Capacity-building on cybercrime has been an essential component of the approach of the Council of Europe from 2006 onwards when the first phase of the Global Project on Cybercrime was launched. The value of strengthening the criminal justice capacities on cybercrime of countries worldwide has since been underlined also by the European Union, the United Nations[6] and others. By early 2013,[7] the international community had reached broad agreement on capacity building as an effective way ahead to help societies meet the challenge of cybercrime and electronic evidence.

This raised the question of enhancing the capacities of the Council of Europe itself to contribute to capacity building worldwide.

In response, and further to an offer by the Prime Minister of Romania and a proposal by the Secretary General (SG/Inf(2013)29), the Deputies decided on 9 October 2013 (at their 1180th meeting), that the Council of Europe establish a Programme Office on Cybercrime in Bucharest, Romania. On 15 October 2013, a Memorandum of Understanding (MoU) regarding the Office was signed between the Council of Europe and the Ministry of Foreign Affairs. The law implementing the MoU was passed by the Parliament of Romania and published in the Official Gazette on 2 April 2014. The MoU entered into force and the Office became operational on 7 April 2014.

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 by extra-budgetary resources.

Experience after 18 months of operations suggests that these expectations are met.

---

[6] At the UN Congress and Crime Prevention and Criminal Justice in Salvador, Brazil in 2010, UN Commissions on Crime Prevention and Criminal Justice since 2010, the and most recently at the UN Congress on Crime Prevention and Criminal Justice, Doha, April 2015.
[7] Outcome of the 2nd meeting of the UN Intergovernmental Expert Group on Cybercrime

2   Mandate of the Office[8]

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 coordination 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;
- Cooperation 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 activities

C-PROC is thus 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.[9] The C-PROC meets its purpose through capacity-building projects.

3.1   Projects in the period April 2014 – September 2015

In the period April 2014 to September 2015, C-PROC supported some 110 activities[10] under the following projects:

Title	Duration	Budget	Funding
Cybercrime@EAP I (number 2523) on Cooperation against Cybercrime in the Eastern Partnership region	Mar 2011 – Dec 2014	EUR 894,000	EU/CoE JP

---

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

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

[10] See Appendix for the list of activities.

GLACY project on Global Action on Cybercrime (number 2688)	Nov 2013 – Oct 2016	EUR 3.35 million	EU/CoE JP
Project Cybercrime@Octopus (number 3021)	Jan 2014 – Dec 2016	EUR 1.8 million	Voluntary contributions (Estonia, Japan, Monaco, Romania, UK, USA and Microsoft)
Cybercrime@EAP II (number 3271) on international cooperation in the Eastern Partnership region	May 2015 – Oct 2017	EUR 800,000	EU/CoE JP (Programmatic Cooperation Framework under the Eastern Partnership)

In September 2015, projects with a combined volume of approximately EUR 6 million were being implemented by C-PROC.

3.1.1 Cybercrime@EAP I

Cybercrime@EAP I was a project under the Eastern Partnership Facility and covered Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine and ended in December 2014.

During the course of 2014, C-PROC supported EAP countries in particular in the preparation of judicial and law enforcement training strategies. A major conference on cybercrime policies and capacities was organised by C-PROC in Chisinau, Republic of Moldova, in November 2014. This served as the closing event of the project and prepared the ground for the Cybercrime@EAP II project.

In terms of overall impact, Cybercrime@EAP I contributed to the strengthening of criminal justice capacities and policies on cybercrime within participating countries and facilitated their co-operation with other parties to the Budapest Convention, including their participation in the Cybercrime Convention Committee.

3.1.2 GLACY Project on Global Action on Cybercrime

GLACY is a joint project with a global scope. Priority countries are Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga. These countries have joined or are committed to join (that is, they have signed or been invited to accede to) the Budapest Convention on Cybercrime.

GLACY helps ensure full implementation of this treaty through:

▪ The strengthening of legislation (including also on data protection and child online protection);

- Law enforcement training, interagency cooperation and advice on specialised units;
- Mainstreaming cybercrime and electronic evidence modules into judicial training;
- Public/private co-operation;
- International co-operation;
- Cybercrime reporting mechanisms.

Since the start of the project, Mauritius and Sri Lanka have become Parties to the Budapest Convention. GLACY also facilitates participation of these countries in the Cybercrime Convention Committee.

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

3.1.3 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. The Octopus Conferences are also organised under this project.

Examples of events organised with the support of the Office in 2014 and 2015 included:

- A workshop on cybercrime legislation in the Latin America region held in Mexico City in April 2014. This activity added impetus to the process of accession by Mexico. It furthermore led to requests for accession to the Budapest Convention by Paraguay and Peru. Both have since been invited to accede.
- An international conference on Article 15 safeguards and criminal justice access to data in Strasbourg in June 2014.
- The Octopus Conference 2015 in Strasbourg in June 2015.

Through this project, the Council of Europe furthermore ensures participation in the Internet Governance Forum, activities of the OSCE and the United Nations, and other events.

Moreover, Cybercrime@Octopus is designed to support the Cybercrime Convention Committee by funding participants and through human resources.

The project has so far been funded by Estonia, Japan, Monaco, Romania (in-kind), United Kingdom, USA and Microsoft. A voluntary contribution by the United Kingdom to this project in spring 2014 was earmarked to fund equipment for C-PROC and was essential to making the Office operational as from April 2014.

3.1.4 Cybercrime@EAP II

Cybercrime@EAP II is aimed at strengthening the capacities of Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) for international legal and police cooperation on cybercrime and electronic evidence. It is to ensure follow up to the recommendations of the Cybercrime Convention Committee (T-CY) adopted in December 2014.

Partners are Estonia, France, Germany, Romania and the European Cybercrime Centre at EUROPOL.

The project commenced technically in May 2015. It ensured participation of Eastern Partnership countries in the T-CY and Octopus Conference in June 2015. A project planning meeting was held in Strasbourg following the Octopus Conference. The project launching conference and workshops were held in Bucharest in September 2015.

3.2   Preparation of new projects and resource mobilisation

Fund-raising and the design of additional projects are important functions of the Office. Indications are that the establishment of C-PROC helps attract resources given the specific profile of a dedicated office for capacity building on cybercrime, the favourable ratio between operational versus non-operational cost (staff, office cost, overheads) and the fact that there are project staff located in an external office who are exclusively responsible for project implementation.

By September 2015, the following projects were at an advanced stage of preparation, funding had been pledged and agreements are likely to be signed by December 2015:

Title	Duration	Budget	Funding
Cybercrime@EAP III – Public/private cooperation in the Eastern Partnership region (number 3608)	Dec 2015 – Nov 2017	EUR 700,000	EU/CoE JP (Programmatic Cooperation Framework under the Eastern Partnership)
Project on Proceeds from Cybercrime in South-Eastern Europe (number 3156)	Jan 2016 – June 2019	EUR 5.5 million	EU/CoE JP
GLACY+ on Global Action on	Mar 2016	EUR	EU/CoE JP

Cybercrime Extended (number 3148)	– Feb 2020	10 million	

If these projects are finally confirmed and contracts are signed on time, C-PROC will implement projects with a combined volume of more than EUR 22 million by spring 2016.

Additional projects are foreseen although funding has not yet been identified:

Title	Duration	Budget	Funding
Cybercrime XR – Support to implementation of the Protocol on Xenophobia and Racism (number 3333)	Dec 2015 – May 2018 (subject to funding)	EUR 600,000	To be identified
Cybercrime@Ukraine – Strengthening criminal justice capacities on cybercrime and electronic evidence in Ukraine (number 3364)	3 years (subject to funding)	EUR 2.5 million	To be identified
Cybercrime@Children – Protection of children against online sexual violence worldwide (number 3365)	May 2016 – Dec 2018 (subject to funding)	EUR 1.3 million	To be identified

Resources for these projects are yet to be mobilised.

4   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.

Projects run by C-PROC follow up to results of the T-CY.

The Office 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.

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

Experience since April 2014 points at strong synergies. The work of the T-CY feeds directly into the work of capacity building activities and vice-versa.

5   Relations with the Government of Romania

The Government of Romania has honoured its commitments following 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.

- Office space at the UN House, a prime location in Bucharest, was allocated to the Council of Europe. Sufficient space is available to allow for the expected expansion of the Office with the launch of new projects at the end of 2015 and the beginning of 2016.

- 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.

- Political support was expressed in particular by the Prime Minister of Romania who hosted a formal ceremony to announce the opening of the C-PROC in the presence of several ministers and more than 25 Ambassadors accredited in Bucharest on 2 June 2014.

Relevant services (Ministries of Justice, Interior and Foreign Affairs, the Prosecution Service, the National Institute of Magistracy and the Computer Emergency Response Team) are seeking close cooperation 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.

6   Administrative and financial matters

6.1   Premises

C-PROC is located within the UN House in Bucharest. Office space is made available free of charge by the Government of Romania.

The space allocated to the Council of Europe was renovated by the Government of Romania prior to March 2014. The Council of Europe is sharing common premises with UN agencies such as the conference room and reception. Security guards are provided by the Government of Romania.

In March 2014, the Office was furnished and equipped – including the IT system – with funding by a voluntary contribution from the United Kingdom. The Office was thus fully functional as from April 2014.

From April 2014 to July 2015, C-PROC was based on the ground floor. In July 2015, the Office moved to the 3rd floor and is now able to accommodate staff responsible for new projects.

6.2 Staff

By September 2015, the Office had two internationally recruited project managers (A2 level) and six locally recruited staff (two project officers at B5 level, one finance assistant at B3 level, and three project assistants at B2 level).

The eight staff were from five different member States. They are funded from project budgets and their exclusive responsibility is project implementation.

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

Should the projects, which are currently in preparation materialise, the number of staff is likely to increase to twenty or more by early 2016.

A specific international recruitment procedure for project managers was completed in July 2015 and a reserve list is available. Following local recruitment competitions, lists of recruitable local candidates have also been established. This means that once project agreements have been signed, the necessary staff can be recruited without delay.

The increase of staff will entail require additional resources for the management of the Office. These should be made available from the administrative overheads that will be generated by new projects.

6.3 Financial matters

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

- Office space is provided rent-free by the Government of Romania.
- Staff are funded from project budgets.
- Initial office furniture and IT equipment were funded by a voluntary contribution from the United Kingdom.

- 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 2015, savings for staff amount to more than EUR 300,000 and for office cost to more than EUR 150,000.

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

7   Conclusions

The following conclusions can be drawn from the experience of the first 18 months of operations:

- Through the Office, the Council of Europe is in a position to contribute substantially to capacity building on cybercrime and electronic evidence worldwide. Large numbers of activities are being carried out in an efficient and cost-effective manner.

- This makes the Office attractive to donors. By September 2015, new projects with a volume of more than EUR 16 million were in preparation and expected to commence between December 2015 and April 2016. Additional project proposals have been developed and more will be prepared in the future.

- The coming projects will focus on Eastern Partnership countries (Cybercrime@EAP III), on countries and areas of South-eastern Europe and Turkey (CyberProceeds@IPA) as well as other regions of the world (GLACY+).

- The conditions are in place to expand the Office rapidly in order to absorb and manage additional resources. Following relocation within the UN House in July 2015, the Office can now accommodate up to 25 staff. Reserve lists for international and local project staff have been established.

- The Office is funded by extra-budgetary resources. Office space is provided rent-free by the Government of Romania. Initial furniture and equipment were funded by a voluntary contribution from the United Kingdom in spring 2014. Operational costs are covered from project budgets. All staff – with the exception of the Head of Office – are funded from the budgets of projects for which they are responsible.

- The Government of Romania is supporting the Office through expertise. Relevant services (Ministry of Justice, Ministry of Foreign Affairs, National Police, the Prosecution Service, the National Institute of Magistracy and

the Computer Emergency Response Team) are seeking close cooperation with the Office, are project partners or contribute in substance to project activities.

▪   Several other member States (Estonia, France, Germany and Turkey) as well as the European Cybercrime Centre at EUROPOL are also partners in one or more projects.

▪   Capacity building projects of C-PROC follow up to results of the Cybercrime Convention Committee (T-CY) and contribute to the work of the T-CY. Synergies between the inter-governmental work of the T-CY and capacity building have been further strengthened since the Office has been established.

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

8 Appendix: Inventory of activities supported by C-PROC

April 2014

Cybercrime@Octopus	Workshop on cybercrime legislation in Latin America, Mexico City, 31 March - 2 April
Cybercrime@Octopus	Support to a technical assistance mission of the Organisation of American States (OAS) to Colombia, Bogota, 1–4 April
Cybercrime@Octopus	Support to regional OAS workshop on cybersecurity, San José, Costa Rica, 3–4 April
Cybercrime@Octopus	Support to "Legal Frameworks for ICTs -Building Capacity and Implementing Regulation" Conference, St. Julians, Malta, 21 – 26 April
GLACY	Needs assessment visit to TONGA, Nuku'alofa 28 April–2 May

May 2014

GLACY	Workshop on law enforcement training strategies for GLACY countries (organised in cooperation with the European Cybercrime Centre (EC3) at EUROPOL), The Hague, Netherlands, 12–16 May
Cybercrime@EAP	Workshop on law enforcement training strategies for Eastern Partnership countries (organised in cooperation with the European Cybercrime Centre (EC3) at EUROPOL), The Hague, Netherlands, 12–16 May
Cybercrime@Octopus	Side-event on Capacity Building on Cybercrime at the UN Commission for Crime Prevention and Criminal Justice, Vienna, Austria, 14 May
Cybercrime@Octopus	Contribution to regional workshop on cybercrime organised by the UN Office on Drugs and Crime, Kampala, Uganda, 27–28 May
T-CY	Contribution to the Pompidou Group: Working Group On Cybercrime, Strasbourg, 14-15 May
T-CY	T-CY ad-hoc sub-group on Jurisdiction and Transborder Access to Data and Data Flows, Strasbourg, 27-28 May
C-PROC	C-PROC: Contribution to a regional conference of Ministers of Justice and Home Affairs organised under the South-East Europe Cooperation Process (SEECP), Bucharest, Romania, 29 May

June 2014

GLACY	Workshop on judicial training strategies for GLACY countries (organised in cooperation with the National Institute of Magistrates of Romania), Bucharest, 2–3 June
Cybercrime@EAP	Workshop on judicial training strategies for Eastern Partnership countries (organised in cooperation with the

	National Institute of Magistrates of Romania), Bucharest, 2–3 June
Cybercrime@Octopus	Contribution to a workshop on cybercrime and advice on cybercrime legislation in Jordan, 4-5 June
Cybercrime@Octopus	Legislative advice to Ecuador, Jamaica, Kenya and Mauritania, May/June
T-CY	11th Plenary of the T-CY, Strasbourg, 17–18 June
Cybercrime@Octopus	Conference on Article 15 safeguards and criminal justice access to data, Strasbourg, 19–20 June
C-PROC	Project planning meeting at INTERPOL, Singapore, 26 June
C-PROC	Discussion on future capacity building projects with EEAS and DEVCO, Brussels, 11 June
C-PROC	C-PROC: Official opening of the Programme Office, Bucharest, Romania, 2 June
C-PROC	Contribution to a regional cybersecurity conference organised under the South-East Europe Cooperation Process (SEECP), 23 June

August 2014

GLACY	Capacity building in Mauritius - Conference and workshops, Port Louis, Mauritius, 11-14 August

September 2014

GLACY	Computer Crime Unit Training – Belgian Federal Police, Brussels, Belgium 8-19 September
Cybercrime@Octopus	Contribution to the Internet Governance Forum 2014 in Istanbul, Turkey, 2 - 5 September
T-CY	Contribution to the International Conference on Terrorism and Organised Crime, Málaga, Spain, 25 - 26 September
C-PROC	President of the Parliamentary Assembly of the Council of Europe, Ms. Anne Brasseur, visit to the Cybercrime Programme Office (C-PROC), Bucharest, 5 September
GLACY	Judicial training of trainers: preparation of a concept, Montpellier, France, 8-10 September
GLACY	Desk study on amendments of the current Moroccan Criminal Code and Criminal Procedure Code in line with the Budapest Convention

October 2014

GLACY	INTERPOL-Europol Cybercrime Conference, Singapore, 1-3 October
GLACY	Computer Crime Unit Training – Belgian Federal Police, Brussels, Belgium, 13-17 October
T-CY	Bureau meeting and T-CY ad-hoc sub-group on Jurisdiction and Transborder Access to Data and Data Flows", Strasbourg, 7-9 October

November 2014

Cybercrime@Octopus	Contribution to Cyber Security Summit 2014 organised by Deutsche Telekom and the Munich Security Conference, Bonn, 3 November 2014
GLACY	Needs assessment visit to Sri Lanka, Colombo, Sri Lanka, 10-14 November
GLACY	Law Enforcement First Responder Trainer's Course and Law Enforcement Training Strategy Workshop Pretoria, South Africa, 17 – 21 November
GLACY	Introductory Judicial Training of Trainer's, Rabat, Morocco, 24-28 November
GLACY	Introductory Judicial Training of Trainer's, Law Enforcement Training Strategy Workshop and Workshop on Interagency Cooperation, Manila, Philippines, 24 – 28 November
Cybercrime@EAP	Cybercrime Capacity Building for EAP Countries, Chisinau, Moldova, 12-14 November
Cybercrime@Octopus	Contribution to EUROJUST strategic meeting on cybercrime, The Hague, 19-20 November
Cybercrime@Octopus	Contribution to the International Conference on Cyberlaw, Cybercrime and Cybersecurity in New Delhi, India, 20 November
Cybercrime@Octopus	Contribution to strengthening the cybercrime legislation in the context of the development of a National Information Security Policy (ANIS Policy) in the Islamic Republic of Afghanistan, November
C-PROC	Visit of Law enforcement experts from Jordan to C-PROC, Bucharest, 18 November
C-PROC	Visit of the Head of Norway's Permanent Mission to the Council of Europe to C-PROC, Bucharest, 28 November
C-PROC	Visit of Project Proteus delegation to C-PROC, Bucharest, 28 November

December 2014

GLACY	GLACY Steering Committee Meeting, Strasbourg, France, 1 December
GLACY	Introductory Judicial Training of Trainers, Dakar, Senegal, 8-12 December
GLACY	Law Enforcement Training Strategy Workshop, Rabat, Morocco, 15-16 December
Cybercrime@Octopus	Delivery of a comparative report on cybercrime model laws, Strasbourg, 2-3 December
T-CY	12th T-CY Plenary, Strasbourg, 2-3 December
Cybercrime@Octopus	Contribution to Global Cyberspace Summit organised by the East West Institute, Berlin, Germany, 3 – 5 December

January 2015

GLACY	Judicial Training of Trainers (Act 3.4), Port Louis, Mauritius, 26-30 January
GLACY	Judicial Training (Continuing Judicial Education) (Act 3.4), Limpopo, South Africa, 19-20 January
Cybercrime@Octopus	Participation in a panel in cybercrime at the Forum Internationale de la Cybersecurité, Lille, France, 20 January
Cybercrime@Octopus	Meeting on trust, data and national sovereignty: solutions for a connected world organised by the Centre for European Policy Studies (CEPS), Brussels
Cybercrime@Octopus	Participation in Transnational Policy Network: US-EU Roundtable on National jurisdiction and digital data flows, Brussels, 20 January
GLACY	Establishment of Cybercrime WIKI and enhancement of Octopus Community, Strasbourg

February 2015

GLACY	Establishment of Cybercrime WIKI and enhancement of Octopus Community
Cybercrime@Octopus	Participation in CYBER NEEDS conference organized by the European Commission and the EU Institute for Security Studies, Brussels, 23-24 February 2015
GLACY	Adaptation of Judicial training materials for domestic use (Act 3.3), Rabat, Morocco, 26 - 27 February
GLACY	Advice on cybercrime legislation of South Africa (desk study and remote advice)
GLACY	Advice on cybercrime legislation of Tonga (desk study and remote advice)

March 2015

Cybercrime@Octopus	Participation in the Development of a National Cyber Security Strategy (OAS event), San Jose, Costa Rica, 2-3 March
GLACY	Audit and delivery of the Judicial Introductory Course (Act 3.6) and workshop on the Budapest Convention, Manila, Philippines, 9-13 March
Cybercrime@Octopus	Meeting on the draft law on cybercrime, Panama City, Panama, 4-5 March 2015
Cybercrime@Octopus	Workshop on the draft cybercrime laws of the Islamic Republic of Mauritania, Nouakchott, Mauritania, 9-10 March
Cybercrime@Octopus	Participation in the "Strategic Approach on Cybercrime. Future Challenges in Tackling Online Criminality", Jūrmala, Latvia, 25-27 March
GLACY	International conference for policy- and decision-makers (Act 1.3), Colombo, Sri Lanka, 26-27 March

GLACY	Workshop on Adaptation of training materials (act 3.3), Dakar, Senegal, 30-31 March
Cybercrime@Octopus	Participation in workshop on international cooperation against cybercrime organized by DIPLO Foundation in view of the UN Crime Congress, Geneva, Switzerland, 30 March

April 2015

Cybercrime@Octopus	Participation in the Innovation and cybercrime: challenges of the digital transformation in Europe, Montpellier, FRANCE, 8-9 April
Cybercrime@Octopus	Participation in the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (UN CCPCJ), including side-event on capacity building, Doha, QATAR, 12-19 April
GLACY	Audit and delivery of the Judicial Introductory Course (Act 3.6), Rabat, MOROCCO, 13-16 April
GLACY	Training workshop on the role of Prosecution Service in international cooperation (Act 5.4), SOUTH AFRICA, 22-23 April
GLACY	Training for legal advisors of the General Secretariat of the Government (Act. 2.2), Rabat, MOROCCO, 27-30 April
GLACY	Judicial training and LEA Training (Act, 3.4, Act 4.4 and 6.2), Nuku'alofa, TONGA, 24 April – 1 May

May 2015

GLACY	Introductory Judicial Training (Regional and District magistrates) (Act. 3.4), Johannesburg, SOUTH AFRICA, 18-21 May 2015
GLACY	Cybercrime legislation: Needs assessment mission and workshop in Myanmar (Act. 2.2), Myanmar, 18 – 19 May
Cybercrime@Octopus	Contribution to CEPOL course on Combatting Card Fraud, Bucharest, Romania, 12 – 15 May
Cybercrime@Octopus	Participation in 43rd INTERPOL European Regional Conference, Bucharest, Romania, 19 – 21 May
Cybercrime@Octopus	Support to African Forum on Data Protection, Dakar, Senegal, 19 – 20 May 2015
Cybercrime@Octopus	TAIEX workshop on Cybercrime and meetings on the cybercrime legislation of Jordan, Amann, Jordan, 19 – 21 May
Cybercrime@Octopus	Support in the organisation of the stakeholders' workshop Afghan Cyber Crime Legislation organised in Istanbul, TURKEY, 31 May – 4 June

June 2015

Cybercrime@Octopus	Participation in the European Dialogue on Internet Governance, Sofia, Bulgaria, 5 June

GLACY	Participation in the 13th Plenary of the T-CY, Strasbourg, 15–16 June, Octopus Conference, 17-19 June and Steering Committee Meeting, 19 June
CyberCrime@EAP II	Participation in the 13th Plenary of the T-CY, Strasbourg, 15–16 June, Octopus Conference, 17-19 June and project planning meeting, 19 June
Cybercrime@Octopus	OCTOPUS Conference 2015, Strasbourg, 17-19 June
GLACY	Standard Operating Procedures workshop, Pretoria, South Africa, 23-26 June
Cybercrime@Octopus	Assessment (desk study) of the current Suriname laws against the provisions of the Budapest Convention

July 2015

Cybercrime@Octopus	Contribution to COMESA (Common Market for Eastern and Southern Africa) Cyber Security Forum and bilateral meetings with the authorities of Kenya, Nairobi, 2-3 July 2015
GLACY	Introductory judicial training for judges, Pretoria, South Africa, 13-17 July
GLACY	Introductory judicial training for judges, Clark, Philippines, 13-17 July
GLACY	First Responders training course, Clark, Philippines, 13-17 July
GLACY	Introductory training for Public Attorney's Office, Manila, Philippines, 20-24 July
GLACY	International cooperation on cybercrime and electronic evidence workshop, Clark, Philippines, 14-15 July

August 2015

GLACY	Study visit of the Ministry of Justice of Philippines to Ankara, Turkey, 17-20 August
Cybercrime@Octopus	Co-organisation of the ASSOCHAM cybersecurity summit, and bi-lateral meetings with the authorities of India, New Delhi, India, 25-26 August
GLACY	First responders training course, Mauritius, 17-21 August
Cybercrime@Octopus	Support to regional workshop on cybercrime legislation in the Pacific organised by the US Department of Justice, Fiji, 17-19 August
GLACY	Advice on the cybercrime legislation of Tonga, Nuku'alofa, 24-28 August

September 2015

Cybercrime@Octopus	Participation in the regional conference on "Regional Partnerships in the Fight against Organised Crime", Mamaia, Romania, 4 September
GLACY	Training of Supreme Court judges, Port Louis, Mauritius, 3-4 September

GLACY	First responders training course, Dakar, Senegal, 7-11 and 14-18 September
GLACY	First responders training course, Kenitra, Morocco, 20-23 September
CyberCrime@EAP II	"Improving international cooperation on cybercrime in the Eastern Partnership region", international meeting and launching event of the CyberCrime@EAP II project, Bucharest, 9 – 11 September
CyberProceeds@IPA	Planning workshop for the project CyberProceeds@IPA on confiscation of proceeds from online crime in South-eastern Europe, Bucharest, 14-15 September
GLACY	Support to training of district and regional magistrates, South Africa, 14-19 September
GLACY	Workshop and advice on the establishment of a Computer Emergency Response Team, Pretoria, South Africa, 21-25 September
GLACY	Pilot of advanced judicial training module, Mauritius, 21-25 September
GLACY/ CyberCrime@EAP II	Participation of experts from GLACY and EAP countries in EUROPOL/INTERPOL annual cybercrime conference, The Hague, Netherlands, 30 September – 2 October