



Capacity building on cybercrime and e-evidence

The Cybercrime Programme Office of the Council of Europe (C-PROC) @ 5: Case studies and impact 2014 - 2019



1



Cybercrime@Octopus

To support implementation of the Budapest Convention on Cybercrime (CETS 185) and related instruments

- ▶ Octopus conferences on cooperation against cybercrime
- ▶ Support to Cybercrime Convention Committee (T-CY)
- ▶ Assistance to countries in the implementation of the Budapest Convention and related standards on data protection and the protection of children online



2



Cybercrime@Octopus

Duration: 72 months (January 2014 – December 2019)

Budget: EUR 3.5 million

Funding: Voluntary contributions from State Parties and Observers to the Convention on Cybercrime (Estonia, Hungary, Japan, Monaco, Romania, Slovakia, United Kingdom, USA) and other public and private sector organisations (Microsoft)



3



Cybercrime@Octopus: activities and results

The Octopus Conference on Cooperation against Cybercrime

► A leading global forum on cybercrime as a matter of criminal justice since 2004

**11th edition,
Strasbourg,
11-13 July
2018**



4



GLACY+

EU/COE Joint Project on Global Action on Cybercrime Extended

- To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

Funded by the European Union and the Council of Europe



COUNCIL OF EUROPE



Implemented by the Council of Europe



5



Duration	60 months (Mar 2016 – Feb 2021)		
Budget	EUR 13.5 million		
Funding	European Union (Instrument Contributing to Peace and Stability) and Council of Europe		
GLACY+ Priority and Hub countries	<ul style="list-style-type: none"> • Cape Verde • Dominican Republic • Morocco • Senegal 	<ul style="list-style-type: none"> • Costa Rica • Ghana • Nigeria • Sri Lanka 	<ul style="list-style-type: none"> • Chile • Mauritius • Philippines • Tonga



6



GLACY+: objectives

CYBERCRIME LEGISLATION, POLICIES AND STRATEGIES

- To promote **consistent cybercrime legislation, policies and strategies** as stand-alone and as part of broader cyber security strategies.

POLICE AUTHORITIES AND INVESTIGATIONS

- To strengthen the **capacity of police authorities** to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with EU and other regions.
- Implementing Partner: **INTERPOL**

CRIMINAL JUSTICE AND INTERNATIONAL COOPERATION

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

7



GLACY+ : activities and results

Policy dialogue to support accession to the Budapest Convention

Workshops for Members of Parliament and senior judges in Ghana under GLACY+ and Cybercrime@Octopus projects



Accra, Ghana, October 2018

- ▶ **Ghana became the 62nd Party to the Budapest Convention in December 2018**

8

GLACY+ : activities and results

Policy dialogue with regional and international organizations

The African FORUM on Cybercrime and Electronic Evidence

300+ participants, 50 African countries, 50+ experts from Africa and the rest of the world



African Union Commission, Addis Ababa, 16-18 October 2018

- **Coordination with regional and international organizations on cybercrime capacity building programs in Africa**

9

GLACY+: activities and results

Strengthening cybercrime policies and legislation in the Pacific Region

Regional Workshops on Cybercrime and Online Child Sexual Exploitation, in collaboration with PILON and Australia



Nuku'alofa, Tonga, May 2018

- **Legislative reforms undertaken in Tonga, Samoa, Vanuatu and Fiji, to achieve full alignment with the Budapest Convention**

10

GLACY+: activities and results

Technical training on cybercrime and electronic evidence for investigators

ECTEG Specialized training courses

- Live Data Forensics
- Internet Investigations
- Darknets and Virtual Currencies
- Open Source Investigations



Santo Domingo, May 2018

- **Technical skills of cybercrime units enhanced and access to ECTEG training courses and materials provided**

11

GLACY+: activities and results

Sustainable capacity building programmes for Law Enforcement Agencies

INTERPOL Instructor Development Course

- Singapore, November 2017
- Singapore, June 2018
- Colombia, February 2019



Singapore, November 2018

- **30+ INTERPOL-certified instructors on cybercrime in GLACY+ countries, able to deliver training courses to their peers**

12

GLACY+: activities and results

Triangular cooperation in Asia for judicial training on cybercrime and e- evidence

Special program on cybercrime and e-evidence for the judiciary in Nepal delivered by Sri Lankan trainer-justices



Kathmandu, August 2017

Training workshop for prosecutors of Indonesia, delivered by Philippines Judges and Prosecutors



Jakarta, January 2019

- Sri Lanka and Philippines judicial training hubs for South Asia and the ASEAN region



13

www.coe.int/cybercrime

iPROCEEDS

EU/COE Joint Project on targeting crime proceeds on the internet in South Eastern Europe and Turkey

- To strengthen the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet.

Funded by the European Union and the Council of Europe



Implemented by the Council of Europe



14



iPROCEEDS

Duration	42 months (Jan 2016 – June 2019)
Budget	EUR 5,56 million
Funding	European Union (IPA II Multi-country action programme 2014) and Council of Europe
	<ul style="list-style-type: none"> <li style="width: 33%; text-align: left;">• Albania <li style="width: 33%; text-align: left;">• Serbia <li style="width: 33%; text-align: left;">• Turkey <li style="width: 33%; text-align: left;">• Bosnia and Herzegovina <li style="width: 33%; text-align: left;">• “The former Yugoslav Republic of Macedonia” <li style="width: 33%; text-align: left;">• Kosovo*

*This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.



15



iPROCEEDS: objectives

- Public reporting systems (with preventive functions) on online fraud and other cybercrime improved or established
- Legislation strengthened regarding the search, seizure and confiscation of cybercrime proceeds and the prevention of money laundering on the Internet in line with data protection requirements
- Cybercrime units, financial investigators and financial intelligence units cooperate with each other at the domestic level in the search, seizure and confiscation of online crime proceeds
- Guidelines on the prevention and control of online fraud and criminal money flows for financial sector entities developed and disseminated, and indicators for the prevention of online money laundering reviewed and updated



16



iPROCEEDS: objectives

Public/private information sharing and intelligence exchange mechanisms on cybercrime established or enhanced at domestic and regional levels

Judicial training academies are providing training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures

International cooperation and information sharing strengthened between cybercrime units, financial investigation units and financial intelligence units (FIUs) as well as between competent authorities for judicial cooperation

17



iPROCEEDS: results and impact

Increased number and relevance of cybercrime investigations accompanied by parallel financial investigations

Protocols and procedures established for interagency cooperation in the search, seizure and confiscation of online crime proceeds

Increased technical and practical skills of LEA to search, seize and confiscate online crime proceeds

New cybercrime indicators for the financial sector

Public/private information sharing and intelligence exchange mechanisms on cybercrime with financial sector established at domestic level

Training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures is part of the regular curriculum of judicial training academies

Enhanced partnerships between IPA national authorities with counterparts from other countries and international organisations

18



iPROCEEDS: activities and results

Structured and documented procedures (domestic protocols) for inter-agency cooperation in the search, seizure and confiscation of online crime proceeds

Workshops on inter-agency cooperation and General guide on Protocols on inter-agency and international cooperation for investigations involving proceeds from crime online



Pristina, Kosovo*, December 2016

- ▶ **Institutionalised interagency cooperation in the search, seizure and confiscation of online crime proceeds**

19



iPROCEEDS: activities and results

Working together to investigate cybercrime and its financial gain

Regional and national case simulation exercises on cybercrime and financial investigations



Bucharest, Romania, November 2018

- ▶ **Efficient cross-sector information and evidence sharing between cybercrime units, financial investigation units, FIUs and prosecution services**

20

iPROCEEDS: activities and results



Dublin, Ireland, December 2018

“Little did I know that UCD could have such a profound impact on me”.
İbrahim ÖZDEMİR, Cybercrime Department, Turkish National Police

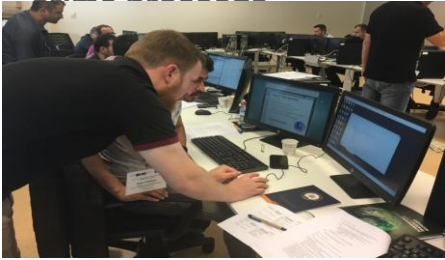
Master Programme in Forensics Computing and Cybercrime Investigations, University College of Dublin

- Equipped with increased knowledge and improved investigatory skills

21

iPROCEEDS: activities and results

Responding to the needs and current challenges related to investigation of cybercrime and online crime proceeds




Ankara, Turkey, October 2018

More than 15 specialised trainings and workshops for law enforcement authorities

- New investigative techniques to search, seize and confiscate online crime proceeds


22



iPROCEEDS: activities and results

Support in improving and developing indicators for the prevention and control of online fraud and criminal money flows on the Internet for financial sector entities

Assessment missions to all project countries/areas and reports on indicators, regional workshop on guidelines and indicators, working groups for the review and update of indicators



Ljubljana, Slovenia, October 2017

► **New cybercrime indicators for the financial sector**

23



iPROCEEDS: activities and results

Working with the financial sector


Public/private meetings for fighting cybercrime and online crime proceeds in all project countries/areas



Belgrade, Serbia, April 2017

► **Public-private information sharing and intelligence exchange mechanisms on cybercrime established**

24



iPROCEEDS: activities and results

Improving the knowledge and skills of judges and prosecutors

Review of the current state of judicial training curricula on cybercrime in all project countries/areas; development/update of introductory and advanced training modules; training of trainers; national delivery of training courses in all project countries/areas.

- ▶ **Cybercrime training integrated in the curriculum of judicial training institutions. A pool of national trainers available in each project country/area. More than 250 judges and prosecutors trained.**



Budva, Montenegro,
June 2017



25



www.coe.int/cybercrime

Cybercrime@EAP II: International cooperation (2015-2017)

Cybercrime@EAP III: Public/private cooperation (2015-2017)

Cybercrime@EAP 2018: one-year extension

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

26



Cybercrime@EAP projects: 2015-2018

- Project area:** Eastern Partnership countries: Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
- Overall Duration:** 44 months (1 May 2015 – 31 December 2018)
- Budget:** ~ EURO 3,000,000
- Funding:** European Union and Council of Europe Programmatic Cooperation Framework (2015-2017) / Partnership for Good Governance (2018)

129 activities in 44 months, 33% of them regional/international
~ 3600 participants engaged throughout the projects directly
Expenditure rates above 90% at project closure

27



Cybercrime@EAP: objectives

Authorities responsible for mutual legal assistance have their capacities enhanced with regard to cybercrime and electronic evidence

The effectiveness of 24/7 points of contact will be enhanced

Draft amendments to rules and procedures on mutual legal assistance will be available for adoption

Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region available

28



Cybercrime@EAP: objectives

A structured process of public/private cooperation on cybercrime underway and agreements concluded

Criminal procedure law strengthened

Focus on cybercrime/security strategies (extension 2018)

Focus on capacities of investigative units (extension 2018)

29



Cybercrime@EAP: results and impact

Improved legislation, rules and regulations in compliance with the Convention

- *Recommendations for improving procedural powers and practical cooperation*

Improved process of cooperation for MLA authorities

- *Uniform knowledge and skills for practical aspects of cooperation*
- *Online resource for cooperation and templates for MLA requests under Article 31*
- *Processing multiple times more requests (~300%) than before start of the project*

Increased role of 24/7 points of contact

- *Institutional reforms and additional regulations through advise and regional focus*
- *Knowledge and skills developed through training programmes and exercises*

30



Cybercrime@EAP: results and impact

Increased understanding of issues on public/private cooperation

- *Elements of legislation, counterparts, compliance and access across borders*

Better strategic and policy cooperation between government actors

- *Willingness to work for the common goal of safer cyberspace*

Meaningful dialogue between the government and private sector

- *Stronger contacts and understanding of each others' issues*

Increased technical and practical skills of cooperation

- *Development of skills for incident and crime response through joint cyber exercises*

31



Cybercrime@EAP: activities and results

Improve international cooperation in the region:

Project country teams developed self-addressed sets of recommendations to improve mutual legal assistance and police-to-police cooperation; project addressed these recommendations by organizing activities in EAP countries and regionally

- **Manifold increase of cooperation requests concerning cybercrime/electronic evidence in the region; cooperation templates adopted officially by the T-CY**



Launching Conference of the project Bucharest, Romania, September 2015

32



Cybercrime@EAP: activities and results

Establish and maintain dialogue between law enforcement and Internet service providers:

Dedicated track of events (10 activities in 2016-2018) specifically designed to support Ukraine, aiming to address main problems of public/private cooperation on cybercrime and e-evidence

► **Ukraine received a comprehensive package of draft amendments to legislation and draft memorandum of cooperation; practical cooperation improved significantly**



IGF-UA, Kyiv, Ukraine, September 2018

33



Cybercrime@EAP: activities and results

Practical skills and interagency cooperation, also extending to private sector:

Regional Cybercrime Cooperation Exercises bring together all professional communities for technical simulation exercises, testing and developing practical skills of handling cyber incidents and crime reports

► **Yearly Regional Cyber Exercises became major regional platform showcasing the need for interagency cooperation**



Regional Cyber Cooperation Exercise
Tbilisi, Georgia, April 2017

34

Eastern Partnership region: Future outlook for capacity building

Participatory project planning:

Workshops to identify priorities for capacity building in Eastern Partnership countries under the Cybercrime@EAP project



Workshop on capacity building
Bucharest, Romania, October 2018

► **The new CyberEast joint project of the European Union and the CoE will be launched in early 2019**

35

www.coe.int/cybercrime

CyberSouth

Cooperation on cybercrime in the Southern Neighbourhood Region

► **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.**

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

36



Priority countries	Algeria, Jordan, Lebanon, Morocco and Tunisia
Duration	36 months (1 July-2017 / 30 June-2020)
Budget	EUR 3.35 million
Funding	European Union and Council of Europe
Implementation	C-PROC (Council of Europe Programme Office on cybercrime)



37



Strengthened legislation

Specialised police services and interagency as well public/private cooperation strengthened

Judicial training on cybercrime and electronic evidence mainstreamed

24/7 points of contact strengthened and enhanced international cooperation on cybercrime and electronic evidence

Strategic priorities on cybercrime and electronic evidence identified



38



CyberSouth: activities and results

Policy dialogue to support accession to the Budapest Convention

National inter ministerial workshops on the Budapest Convention in priority countries non Party

September 2018 Algeria

September 2018 Tunisia

November 2018 Lebanon

November 2018 Jordan



- **Lebanon cybercrime Law in line with Budapest Convention in force since January 2019**
- **Jordan is reviewing its current and draft law based on Council of Europe's recommendations**

39



CyberSouth project: activities and results

Judicial training

Within the next 6 months:

- **mainstreaming of training materials for judges and prosecutors and**
- **kick-off meeting of CyberSouth network of magistrates on cybercrime and electronic evidence**



Regional workshop on judicial training strategies, Lebanon, 23-25 January 2019

- **Group of magistrates trainers consolidated in all 5 priority countries**

40

CyberSouth project: activities and results

Trainings for cybercrime investigators

Within next 6 months:

- **First responder course integrated in training curricula**



Business email compromise and credit card fraud workshop, Bucharest, November 2018

- **Specialised police services and interagency as well public/private cooperation strengthened**

41

CyberSouth project: activities and results

- ▶ **CyberSouth facilitated the participation of Algeria, Jordan Lebanon, Morocco and Tunisia in international fora on cybercrime and electronic evidence**



Advisory mission for the establishment of the 24/7 contact point, Tunisia, August 2018

- ▶ **More effective international cooperation on cybercrime and e-evidence**

42



End online child sexual exploitation and abuse@Europe

Project area: Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine, Albania, Bosnia and Herzegovina, Montenegro, Serbia and Turkey

Overall Duration: 30 months (1 July 2018 – 31 December 2020)

Budget: EURO 849,041

Funding: End Violence Against Children Fund,

PROC) in Implemented by the Children's Rights Division of the Council of Europe, in co-operation with the Cybercrime Office (C-Romania).

OVERALL OBJECTIVE:

The rights of children are protected through effective multi-national, interdisciplinary, cross sectorial cooperation and child-friendly measures to prevent and combat child sexual exploitation and abuse (OCSEA) facilitated by ICT, at pan-European level

43



EndOCSEA@Europe: objectives

Increased awareness of decision makers regarding OCSEA threats and the implication for the rule of law and human rights

Interagency and multi-stakeholder cooperation; policies and strategies are developed, strengthened and promoted in focus countries and at European level

Improved law enforcement capacities to lead, support and coordinate OCSEA investigations

Improved criminal justice capabilities regarding OCSEA cases

Improved interagency cooperation for the protection of victims

Children, parents, professionals and parliamentarians have an improved understanding of OCSEA and actions taken to prevent and report

Strengthened capacity of civil society organisations to prevent and combat OCSEA

44



EndOCSEA@Europe: expected results and impact

Steering Committee meeting (4th of March 2019, Strasbourg)
18 National Representatives and other relevant bodies

Launching Conference (16-17 May 2019, Strasbourg - tbc)
80 participants from relevant authorities and experts

Baseline mapping and gap analyses in target countries

Country-specific support for policy and strategy development

45



EndOCSEA@Europe: expected results and impact

Comparative review of existing mechanisms for collective action against OCSEA at pan-European level

Technical support for legislative and procedural reforms in focus countries

Review of training strategies, materials and programmes available for law enforcement, judiciary and prosecutors on OCSEA and electronic evidence

Offline and online campaigns and initiatives to prevent OCSEA, in collaboration with civil society, businesses and specialised organisations

46