



# Cybercrime@Eastern Partnership

Արևելյան Գործընկերության  
Օգնության Կարգադրություն Eastern  
Partnership օգնության կարգադրություն  
Հարցընկերության Կարգադրություն Estic  
Sąqół tarczafidngli Parteneriat Oriental  
Усподне Իարտերեստ

First Meeting of the Eastern Partnership Rule of Law Panel  
Cybercrime activities in the Partnership for Good Governance

## Cybercrime@EAP

Overview of capacity building projects implemented by the Council of Europe under the Partnership for Good Governance

Brussels, 16 June 2017



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1



## Cybercrime@EAP projects: overall rationale



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

2




## Cybercrime@EAP: Summary

Summary CEAP II	Cybercrime@EAP II – International cooperation Budget ca. EUR 800,000 32 months (1 May 2015 – 31 December 2017)
Summary CEAP III	Cybercrime@EAP III – Public/private cooperation Budget ca EUR 1,200,000 25 months (1 December 2015 – 31 December 2017)
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

3



## Cybercrime@EAP II: Objectives and Expected Results

Objective	To enable efficient regional and international co-operation on cybercrime and electronic evidence.
Expected result 1	Authorities responsible for mutual legal assistance have their capacities enhanced with regard to cybercrime and electronic evidence.
Expected result 2	The effectiveness of 24/7 points of contact will be enhanced.
Expected result 3	Draft amendments to rules and procedures on mutual legal assistance will be available for adoption.

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

4



## Cybercrime@EAP II: Achievements so far

- Project working groups on MLA and on 24/7 contact points established;
- Detailed [analysis](#) of the rules and procedures for the mutual legal assistance (will be updated by end of 2017);
- Recommendations for improving international cooperation developed and proposed by country teams during 3 regional meetings under the project, followed up by in-country events to put them into action (e.g. training sessions March 2017);
- Draft standardized templates for international requests to access stored computer data and for data preservation were developed (e.g. training sessions March 2017);
- On-line information [resource tool](#) for international cooperation on cybercrime and electronic evidence was developed, tested and made available to all Parties to the Budapest Convention and the Republic of Belarus;
- Participation of country team supported in various international events: T-CY/Octopus; INTERPOL/Europol Annual Conferences; INTERPOL trainings; many upcoming events this year (Brussels, Hague, Strasbourg, etc.)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

5



## Cybercrime@EAP III: Objectives and Expected Results

Objective	To improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region.
Expected result 1	Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region.
Expected result 2	A structured process of public/private cooperation on cybercrime underway and agreements concluded.
Expected result 3	Criminal procedure law strengthened.

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

6



## Cybercrime@EAP III: Achievements so far

- Project teams were appointed in the beginning of 2016 and revised in 2017;
- Regional analysis/ [Mapping Study](#) of public/private cooperation strengths, weaknesses, opportunities and threats in EAP countries undertaken (will be updated and revised by end of 2017);
- Platform for the structured dialogue on public/private cooperation is established through several regional meetings and in-country workshops;
- Regional meeting with the multinational service providers was organized in Dublin in close cooperation with another capacity project run by C-PROC (IPROCEEDS);
- First ever regional cybercrime coordination and partnership exercise completed for 12 countries of the EAP and West Balkans/Turkey;
- Upcoming studies on MSPs/ISP liabilities and Article 15 regional meeting in Chisinau (September);
- Improvement of capacities of the country teams is being supported through facilitating their participation in international events/conferences (T-CY hearings, EuroDIG, few major events in upcoming in 2017).

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

7



## CEAP II & III - remaining activities 2017

- **Ongoing studies: MSP communications/ISP liabilities (June, July)**
- **Ongoing: ECTEG training for cybercrime investigators /police academies (Brussels, June)**
- **Support to IAP Regional Meeting in Georgia, cybercrime track (Tbilisi, June)**
- **Workshop on legal and practical aspects of CERT cooperation (Minsk, July)**
- **Advisory mission on 24/7 operations and regulations (Tbilisi, July)**
- **Series of events on memorandum between LEA/ISP (Ukraine, September-November)**
- **Regional meeting on safeguards, guarantees and legislation (Moldova, September)**
- **Follow up implementing Joint Opinion of the Venice Commission (Moldova, September)**
- **INTERPOL/Europol Annual Cybercrime Conference & 24/7 training (Hague, September)**
- **G-PEN Cybercrime and Money Laundering Conference (Azerbaijan, October)**
- **Data retention workshop [*unconfirmed*] (Azerbaijan, October)**
- **South & Eastern European Conference on public-private cooperation (Sofia, October)**
- **Advisory visits to all EAP countries to update EAP studies/inventory (October-November)**
- **T-CY sessions, Octopus conference and related hearings/events ( November)**

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

8



## Priorities for 2018: Observations ► State of Play Report

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
<b>Strategies/action plans</b>	No	No	No	Yes	Draft	Yes
<b>Procedural law: gaps in terms of Convention</b>	- Definitions of data - Articles 16, 17 and 18 - Special powers under Art. 19	- Definitions of data - Art. 16 and 17 - Partial Art. 18 - Special powers under Art. 19	- Definitions of data - Articles 16, 17 and 18 - Special powers under Art. 19; - Judicial oversight	- Art. 16 and 17 - Special powers under Art. 19	- Partial Art. 16 - Partial Art. 18 - Special powers under Art. 19	- Definitions of data - Articles 16, 17 and 18 - Special powers under Art. 19 - Art. 20 BCC – no traffic data
<b>Operational cybercrime units</b>	- National Police - Investigative Committee	- Ministry of National Security - Ministry of the Interior (being set up)	- Ministry of Interior - Investigative Committee	- Ministry of Internal Affairs - Ministry of State Security	- Ministry of the Interior - Prosecutor General's Office	- Cyber Police - State Security Service
<b>Police-to-police cooperation units</b>	- National Police	- Ministry of National Security	- Ministry of Interior	- Ministry of Internal Affairs	- Ministry of the Interior - Prosecutor General's Office	- Cyber Police - State Security Service
<b>Authorities for judicial cooperation</b>	- Prosecutor General's Office (pre-trial) - Ministry of Justice (trial stage)	- Prosecutor General's Office (pre-trial) - Ministry of Justice (trial stage)	- Office of the Prosecutor General - Other authorities on treaty basis - Supreme Court	- Office of the Chief Prosecutor at the Ministry of Justice	- Prosecutor General's Office (pre-trial) - Ministry of Justice (trial stage)	- Prosecutor General's Office (pre-trial) - Ministry of Justice (trial stage)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

9



## Priorities for 2018: Observations

**“State of Play report” ► Further improvement required regarding:**

- **Strategic approaches and policies on cybercrime and electronic evidence**
- **Procedural law powers on cybercrime and electronic evidence (major gaps in implementation of Budapest Convention in this respect)**
- **Division of competencies between security services and criminal police**
- **Problems in international cooperation due to gaps in domestic procedural law**
- **Cooperation with multi-national service providers**

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

10



## Priorities for 2018: Reminder ► Strategic priorities

**Strategic priorities  
adopted at EAP  
conference (Kyiv,  
October 2014)**

1. **Cybercrime policies and strategies**
2. **A complete and effective legal basis for criminal justice action**
3. **Specialised cybercrime units**
4. **Law enforcement training**
5. **Judicial training**
6. **Financial investigations and prevention and control of fraud and money laundering on the Internet**
7. **Cooperation between law enforcement and Internet service providers**
8. **More efficient regional and international cooperation**

11



## Priorities for 2018+?: Proposals

### **Focus on procedural legislation: prerequisite for further progress**

- Completion of reforms of procedural law as basis for domestic investigations, public/private and international cooperation
- Related regulations including division of competencies
- Additional focus on 24/7 regulations, where necessary

### **Practical tools for international cooperation**

- Online resources related to EAP states: further development
- Use of cooperation templates for Article 29/30 and Article 31 requests

### **Policies of national service providers, cooperation agreements and cooperation with multinational service providers**

- Information hard to come by – cooperation is rare – agreements are needed
- More focus on MSPs as they now process more and more requests
- Track and implement recommendations of T-CY Cloud Evidence Group

### **Promote strategic approaches to cybercrime and electronic evidence:**

- Assess state of play against strategic priorities of October 2014
- Organise conference for decision-makers on cybercrime policies and strategies

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

12



## Priorities for 2018-2020?

### Strengthening operational capabilities

- LEA training – EGTEG materials – systematic and scalable training
- Judicial training

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

13



Funded  
by the European Union  
and the Council of Europe



COUNCIL OF EUROPE



Implemented  
by the Council of Europe

EUROPEAN UNION  
CONSEIL DE L'EUROPE

# Thank you for your attention

**Alexander SEGER**  
 Head of Cybercrime Division  
 Head of Cybercrime Programme Office  
 Council of Europe - Conseil de l'Europe  
 Strasbourg, France / Bucharest, Romania  
[Alexander.Seger@coe.int](mailto:Alexander.Seger@coe.int)

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

14