Project Cybercrime@EAP III
Public/private cooperation

Արևելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul
Estic Şərq tərəfdaşlığı Partenariat
Oriental Усходняе Партнёрства

Draft Version 13 March 2016

Study on mapping current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership region

Under the CyberCrime@EAP III project of the Council of Europe

March-June 2016
Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine

(Draft) Outline

Background

Cooperation between criminal justice authorities and private sector entities, including in particular service providers, is essential to protect society against crime. Such cooperation concerns primarily access by police and prosecution services to data held by service providers for criminal justice purposes, but also the sharing of information and experience, as well as training.

In recent years, the question of public/private cooperation and specifically the issue of criminal justice access to data has become more complex. This is also true for countries participating in the Eastern Partnership. Often, local and multinational service providers are reluctant to cooperate, criminal justice measures and national security measures are not clearly separated, and public trust is limited. Moreover, law enforcement powers such as those foreseen in the Budapest Convention on Cybercrime are not always clearly defined in criminal procedure law, and this adversely affects law enforcement/service provider cooperation as well as human rights and the rule of law.

The present project, managed by the Cybercrime Programme Office of the Council of Europe (C-PROC), is aimed to address these issues. However, due to lack of regulation and generally sensitive nature of the topic, there is not much information available to properly assess the current situation with public/private cooperation on cybercrime in the region and thus establish a baseline for the project. Therefore, it is essential that the study that maps current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime, as envisaged by the logframe of the project, is conducted in the manner of dedicated study visits to EaP jurisdictions, to study information on the ground and, most importantly to hear both government and private sector views on cooperation.

Programmatic Cooperation Framework for
Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine and Belarus

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Objectives

Map current strengths, weaknesses, opportunities and risks regarding public/private and specifically law enforcement/service provider cooperation, document good practices and initiatives already underway, and establish a baseline for the CyberCrime@EAP III project to address these issues by regional and in-country events.

Additional objective is to familiarize with newly established CyberCrime@EAP III project teams and discuss their involvement in the organization of in-country events under the project.

Expected results

Contracted consultants conduct study visits to all of the project countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine) to map current strengths, weaknesses, opportunities and risks regarding public/private and specifically law enforcement/service provider cooperation and to document good practices and initiatives already underway.

The study produces a detailed report on the situation with regard to public/private cooperation on cybercrime in the Eastern Partnership region.

Participants

- International experts in public/private cooperation in cybercrime;
- Project country team members;
- Authorities tasked with legislative reform (Ministries of Justice);
- Cybercrime investigative units (including operative/detective units and 24/7 points of contact);
- Prosecution units specialized or mainly tasked with cybercrime and electronic evidence;
- Telecommunications regulatory authorities;
- Cybersecurity institutions that report cybercrime (CERTs or others);
- Internet associations or other business forums;
- Individual ISPs (where necessary);
- Data protection authorities (where applicable);
- C-PROC staff.

The main working language will be English, however on-site Ukrainian interpretation may be provided, as necessary.

Tentative Programme of the study

30 March to 1 April 2016:	Study visit to Ukraine (2.5 working days)
13-15 April 2016:	Study visit to Armenia (2.5 working days)
18-20 April 2016:	Study visit to Azerbaijan (2.5 working days)
21-23 April 2016:	Study visit to Georgia (2.5 working days)
10-12 May 2016:	Study visit to Belarus (2.5 working days)
16-18 May 2016:	Study visit to Moldova (2.5 working days)
23 May – 31 June 2016:	Drafting and finalization of study report

Contact

Giorgi Jokhadze
Project Coordinator
Giorgi.Jokhadze@coe.int
www.coe.int/cybercrime