Project Cybercrime@EAP II

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

Online Resource for International Cooperation

Prepared by the Cybercrime Programme Office
Council of Europe

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

www.coe.int/cybercrime

Background

- Recommendation of T-CY at 12th Plenary, December 2014:
  "to establish an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as the disclosure of stored computer data for use in criminal proceedings"
- Joint effort between the Cybercrime@EAP and other capacity building projects (GLACY, iProceeds, Octopus)
- Awareness of other potentially useful/competing resources:
  - PC-OC (Country information and implementation tools)
  - EJN (Judicial Atlas, Fiches Belges, Compendium, etc.)
  - UNODC (Mutual Legal Assistance Request Writer Tool)
  - Europol (operational cooperation tools)

- Rationale: more specialized and focused resource needed
- Start small, develop later
- Involve more countries

Preparation process

- CEAP II Launching event in Bucharest - proposal by Armenia:
  - Contact persons (pre-trial and trial stage)
  - Legal acts regulating mutual legal assistance
  - Requirements that should be met in requests,
  - List of international treaties that that country is a Party,
  - Articles from the Criminal Code related to cybercrime offences
  - Use of English as accepted language of communication
  - Statistical data on sent/received requests, time limits, main obstacles

- CEAP II second regional meeting in Tbilisi:
  - Online platform as a combination of open and member-only domains
  - Additional features: cooperation with providers and discussion forum

- Third CEAP II regional meeting in Kyiv:
  - Focused on the questionnaire/form for input (ten/six steps)

Structure of the Platform

Module 1: Central authorities

- Authority for extradition and provisional arrest in the absence of other treaties (Article 24)
- Authority for Mutual Legal Assistance in the absence of other agreements (Article 27)
- 24/7 Contact point (Article 35)
- Resources, guides and links

Module 2 – Specific Procedures (step-by-step) for:

- Preservation Requests (Art. 29-30)
- Request for Subscriber's Information (Art.31)
- Request for Traffic Data (Art. 31)
- Request for Content Data (Art. 31)
- Request for Real Time Collection of Traffic Data (Art. 33)
- Request for Interception of Content Data (Art. 34)

Module 3 – Additional resources (specific templates, guides, etc.)

Current and further action

- **Action by EAP countries**
  - Complete information for Module 1 (Contact details of competent authorities under Articles 24, 27 and 35 of the Budapest Convention)
  - Agree on typical steps for preservation requests and subscriber information (Kyiv Regional Meeting, 4-5 April 2016)
  - Examples presented to the T-CY (done at the 15th Plenary in May 2016)
  - Questionnaire/information form for the resource (completed)

- **Follow-up action by the Council of Europe**
  - Putting collected information online (timeline: by October 2016)
  - Request other Parties to the Budapest Convention to provide the same information (in progress)

Long-term

- EAP and other contributing countries responsible for keeping the online resource up to date and support development through in-country events

Project Cybercrime@EAP III

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

Online Resource for Public-Private 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

www.coe.int/cybercrime

Background and context

- Cybercrime@EAP III **project objective**:
  - ✓ To improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region

- Implementation **indicator**:
  - ✓ An online resource on public/private cooperation data is available and contributes to transparency on criminal justice access to data.

- **Result** 2: A structured process of public/private cooperation on cybercrime underway and agreements concluded:
  - ✓ An online resource is maintained by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania to service [structured process of public/private cooperation], to improve transparency and thus public confidence, and to link up existing initiatives (+ feasibility to develop further)

Logic: Information is key

Servicing the process of cooperation:

- Status with regard to relevant standards (including treaties), reservations
- Legislative acts (criminal justice /communications /data protection) and any explanations, practices or case law applicable to these regulations
- Instructions, manuals, guidelines, SOPs and templates for accessing data
- Information on main stakeholders in the process (government and industry)

Improving transparency and public confidence: fairly obvious

Linking up existing initiatives:

- Information on national/regional/global projects relevant to the topic
- Memoranda of cooperation and other arrangements to facilitate cooperation
- Any possibilities for training, membership of associations, etc.

Development process so far

- Information received from two sources:
  - ➢ Responses to forms sent directly to EAP country teams
  - ➢ Country reports from the CEAP III Mapping Study

- Information that is there:
  - ✓ Institutional setup/who does what
  - ✓ Basic legal framework

  More specifically:
  - ☑ Existence of cooperation agreements
  - ☑ Competent authority/legal basis to request information (BCC Art. 18)
  - ☑ Definitions/competent authority/legal basis to preserve data(Art.16/17)
  - ☑ Emergency situations: definitions, legal obligation to cooperate
  - ☑ Confidentiality: legal basis and liability for non-compliance
  - ☑ Data protection treaties/agreements (basic information only)
  - ☑ Sources and links to legal acts in English

Development process so far

- **Still needs to be done**:
  - ❑ Data quality review and complete missing/inadequate information
  - ❑ Information on specific laws and regulations that authorize access to data needs to be laid out more logically
  - ❑ Information on the rest of procedural powers under the Convention
  - ❑ Information on applicable safeguards and guarantees is mostly missing (and needs to be structured along procedural powers)
  - ❑ Information on remedies
  - ❑ Practice or case law explaining the application of law
  - ❑ Manuals, guidelines, agreements, and other similar documents
  - ❑ Policies of national Internet service providers
  - ❑ Policies from multinational service providers
  - ❑ Contact points on both sides to refer to in case of inquiries

  …
  - ❑ Testing the process (!!)

Potential benefits (for both resources)

- Integration into the country profiles available under the Cyber Wiki;
- Facilitate international cooperation between members of the Budapest Convention through better knowledge of the requirements of other States and easier access to the information related to:
  - The laws of Parties on substantive and procedural matters;
  - Legal thresholds, evidentiary and other requirements for preservation and disclosure of stored computer data, and other procedural powers;
  - Practical templates and steps for MLA requests;
  - Contact lists of competent authorities.
- Facilitate cooperation of criminal justice authorities with the foreign/multinational service providers:
  - Verifiable source on legal background and requirements of states for service providers who process requests through direct cooperation options;
  - Trust building by designating the contact points for sending and processing requests;
  - Firsthand access to up-to-date templates, guidelines, policies and other sources;
  - Clarity with regard to who-does-what.

Thank you for your attention

Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania