Online resource for international cooperation: example of capacity building projects

www.coe.int/cybercrime

Online Resource on International Cooperation

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"

➢ Proposal to develop in parallel an online tool for Public/Private Cooperation

➢ Resources foreseen in Cybercrime@EAP and other capacity building projects

Benefits

➢ Integrated into the country profiles into the 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;

▪ Practical templates and steps for MLA requests;

▪ Contact lists of Competent Authorities.

Timeline

➢ To be finalised by October 2016

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 or arrangements (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.)

Online Resource on International Cooperation

Next Steps	**Action by EAP countries**
	1. Complete information for Module 1 (Contact details of competent authorities under Articles 24, 27 and 35 of the Budapest Convention)
	2. Agree on typical steps for
	■ Preservation requests
	■ Requests for subscriber information
	(DONE at the Kyiv Regional Meeting, 4-5 April 2016)
	3. Complete "typical steps" for their respective countries
	4. Examples presented to the T-CY
	Follow-up action by the Council of Europe
	1. Putting information online
	2. Request other Parties to the Budapest Convention to provide the same information
Updating the platform	EAP and other contributing countries responsible for keeping the online resource up to date / support through in-country events (e.g. Armenia, June 15-17, 2016)

Capacity building projects:
Compliance with T-CY recommendations

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

Implemented
by the Council of Europe

CONSEIL DE L'EUROPE

- *Rec 2*: Parties should consider maintaining **statistics** or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence;

- *Rec 4*: Parties should consider providing for better **training** to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be **supported by the capacity building programmes** of the Council of Europe and other organisations.

- *Rec 5*: Parties and the Council of Europe should work toward strengthening the role of **24/7 points of contact** in line with Article 35 Budapest Convention, including through:

  c) Conducting regular **meetings and training** of the 24/7 network among the Parties;

  e) Considering to establish, where feasible, contact points in **prosecution offices** to permit a more direct role in mutual legal assistance and a quicker response to requests;

  f) Facilitating 24/7 points of contact to play a **supportive role in "Article 31" requests**

- *Rec 6*: Parties should consider **streamlining** the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.

- *Rec 7*: Parties should make use of **all available channels** for international cooperation. This may include formal mutual legal assistance, police to police cooperation and others.

- *Rec 8*: Parties are encouraged to establish **emergency procedures** for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.

- *Rec 9*: Parties should **confirm receipt** of requests systematically and give, upon request, notice of action taken.

- *Rec 11*: Parties should make use of **electronic transmission of requests** in line with Article 25.3 Budapest Convention on expedited means of communication.

- *Rec 12*: Parties should ensure that requests are **specific** and **complete** with all necessary information.

Specific capacity building recommendations

- *Rec 17*: The Council of Europe should – under capacity building projects – develop or link to standardised, multi-language **templates** for **Article 31-requests**.

- *Rec 18*: The Council of Europe should explore the possibility of establishing an **online resource** providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.

- "*Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region*" adopted under the EAP I in Ukraine, October 2013:

- **Strategic priority 8**: More efficient regional and international cooperation:

  - Exploit the possibilities of the Budapest Convention on Cybercrime and other bilateral, regional and **international agreements** on cooperation in criminal matters.

  - Provide for **training and sharing of good practices**.

  - Evaluate the **effectiveness** of international cooperation.

  - **Strengthen** the effectiveness of **24/7 points of contact**.

  - Compile **statistics** on and review the effectiveness of 24/7 contact points and other forms of international cooperation on a regular basis.

- Cybercrime@EAP II: **more focused** continuation of EAP I – linked to strategic priorities;

- Country-sourced, specific recommendations (**all countries – without exception!**);

- **Linking** between the capacity building efforts: 24/7 workshop and training for GLACY countries in Sri Lanka, April 2016: setup, authority and Guide on 24/7 POC – participation of the 24/7 representative from **Moldova**.

Thank you for your attention