iPROCEEDS-2

Project of the European Union and the Council of Europe on Targeting crime proceeds on the Internet and securing electronic evidence in South East Europe and Turkey

Specialised Judicial Training Course on International Cooperation

Provided under the iPROCEEDS-2 Project

North Macedonia|20 – 22 April 2021

Outline

Background and justification

Due to the ongoing Covid-19 pandemic, many businesses and institutions changed their activities from physical presence to an online environment, thus relying even more on technology. As criminals are adaptable by nature to the ongoing changes in a society, they also shifted their activities to the online world and preyed on the increasing number of internet users worldwide.

Given the reliance of societies worldwide on information and communication technologies, major efforts are required to provide judges and prosecutors with the necessary skills, in particular through training.

The Council of Europe has been supporting judicial authorities to tackle this need through global capacity building initiatives, by delivering judicial training courses on cybercrime and electronic evidence in a vast number of countries, by training pools of judges, magistrates and prosecutors to become trainers themselves on these matters, and by working with training institutions to integrate relevant modules into regular curricula.

The primary purpose of international cooperation in cybercrime investigations and proceedings is the preservation and production of admissible and reliable evidence that can be used in pre-trial and trial proceedings in criminal cases. Electronic evidence in cases of offences against and by means of information technology is usually difficult to collect and relatively volatile. It is therefore crucial that, in investigating and prosecuting cybercrime, countries/areas are prepared to employ a variety of international cooperation modalities available under the Budapest Convention on Cybercrime in an efficient and timely manner.

The iPROCEEDS-2 project, in coordination with other projects implemented by the Cybercrime Programme Office has therefore developed a Specialised Online Module on International

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

Cooperation that is aimed at improving the skills of criminal justice authorities in relation to the international cooperation aspects provided by the Budapest Convention on Cybercrime and the

upcoming second Additional Protocol to the treaty.

The training also features strong focus on the use of standard cooperation templates approved by the Cybercrime Convention Committee (T-CY) for improving the process of cooperation.

It would be advisable that professionals that will be attending the Specialised Judicial Training Course on International Cooperation have previously taken part in the Introductory Judicial Training Course also developed under the Council of Europe framework.

Expected outcome

Organised by the Joint project of the European Union and Council of Europe iPROCEEDS-2, the activity contributes directly to its Result 6, *Judicial training on cybercrime and electronic evidence and related financial investigations and anti-money laundering measures with a focus on data protection and rule of law safeguards*, output 6.5 Delivery of introductory/advanced and specialised training courses in each beneficiary.

The training course will be delivered in all project countries/area pending their need to increase capabilities in the exchange of cybercrime related information on an international level and in the use of templates for international requests for data preservation and subscriber information.

Whenever possible, local judicial trainers that were trained under the previous iPROCEEDS project will be invited to attend the course, assess it, learn from its delivery and subsequently implement it in their countries/area. Requests of adaptation of the training course to national specificities or further support in delivering it might follow the initial training course.

Additional trainers from the project countries/area will be invited to attend this Specialised Judicial Training Course on International Co-operation, thus possibly contributing to an increase in the countries/area pool of trainers.

By the end of the event, participants will be expected to have up-to-date knowledge and understanding of currently available framework and practice for international cooperation in cybercrime and electronic evidence as provided by the Budapest Convention on Cybercrime and draft second Additional Protocol to the treaty.

Participants

The training course will be attended by judges and prosecutors, cybercrime investigators, representatives of the Judicial Training Academies, national trainers, Council of Europe experts and iPROCEEDS-2 team members.

Administrative arrangements

The workshop will be organised online, on 20 – 22 April 2021, from 10h00 – 12h00 and 14h00 – 16h00, North Macedonian time. To connect, please use the link to Zoom. Credentials for the meeting with details on how to connect and other practical aspects will be sent by email.

Translation from and into Macedonian and English will be provided by the Council of Europe.

Programme

Day 0, Monday, 19 April 2021

15 min	Complete a short online survey

Day 1, Tuesday, 20 April 2021

10h00	**Course opening and welcome remarks** • Academy for Judges and Public Prosecutors „Pavel Shatev"– Prof. Dr.Sc. Natasha Gaber DAMJANOVSKA, Director of the Academy; • Council of Europe – Lejla DERVISAGIC, Head of Operations, Council of Europe Office in Skopje; • Council of Europe – Virgil SPIRIDON, Head of Operations, Cybercrime Programme Office of the Council of Europe; • Council of Europe – Alexandru CRISTEA, Project Manager, Cybercrime Programme Office of the Council of Europe;
10h15	**Session 1.1: Introduction to the Course** During the introduction the objectives and aims of the course are explained to the delegates who are encouraged to consider and voice their expectations regarding attending the course. Experts explore with delegates any concerns they may have or have experienced in handling cases involving cybercrime and electronic evidence. Such concerns should be listed and addressed by the experts during the course.
10h30	**Session 1.2: International Cooperation in a Global Economy** This session will be used as a general introduction to the topic and a reminder of some information from the introductory course. This session will give an overview of the need for international cooperation and will provide the delegates with a general introduction to the issues. It will discuss the challenges faced in obtaining electronic evidence in a global economy, with the focus on the Budapest Convention and the need to be aware of the tools available for international cooperation.
11h30	**Session 1.3: Overview of Legal Basis of International Cooperation in Relation to Cybercrime and Electronic Evidence** This session provides participants with an understanding of the specific provisions of the Budapest Convention and how these are crucial in prosecuting and investigating cybercrime as well as digital evidence acquisition.
12h30	*Lunch break*
14h00	**Session 1.4: Mutual Legal Assistance Practice and Procedure** There should be a discussion of the concept of Mutual Legal Assistance (MLA) practice and procedure and extradition. A discussion of some of the present challenges of the MLA process and how different legal systems can affect the efficiency of the MLA process. MLA procedure should be complemented also with private entities cooperation procedures since some of the formal aspects of it are coming from the Convention and national laws, e.g. direct ISP cooperation.
15h00	**Session 1.5: Informal Methods of International Cooperation** This session is making the delegates aware of some informal methods of international cooperation, a case study can be used to make this session more interesting. This

	session will also cover the advantages and disadvantages of using informal methods, will mention some regional and international organizations and networks that may assist them.
16h00	**End of Day 1**

Day 2, Wednesday, 21 April 2021

10h00	**Session 2.1: Mechanisms under the Budapest Convention to Facilitate International Cooperation** The delegates will be taught the Budapest Convention's substantive and procedural provisions. The delegates will understand and know the appropriate use of procedural powers such as preservation and productions orders and how these can facilitate international cooperation especially in acquiring evidence from other outside jurisdictions. This session will also include a discussion on the safeguards contained in the Budapest Convention. Budapest Convention Articles related to international cooperation will be discussed in more depth.
12h00	*Lunch break*
14h00	**Session 2.2: Utilizing Digital Evidence Acquisition through International Cooperation Mechanisms - Case Study** The aim in this session is to present the complete step by step process of how digital evidence is acquired through international cooperation mechanisms. This is best done by a case study that will start with the commission of a crime in country A with the offender in country B and the evidence in various jurisdictions.
15h00	**Session 2.3: Challenges Faced** This session should discuss the pressing challenges faced by jurisdictions in seeking cooperation from others. Challenges such as different prevailing systems and laws. There should be a brief discussion to explain the different legal systems.
15h30	**Session 2.4: Public Private Partnership/Cooperation** This session aims to show the importance of cooperation with the private sector especially in digital evidence acquisition. Evidence needed by police to solve a cybercrime is often held by private industry outside of the jurisdiction concerned. In some cybercrime investigations, cross border cooperation may be easier for industry than national law enforcement. Private industry is often interested in working with law enforcement as they are often victims of such crimes. Partnerships are therefore essential to make cross jurisdiction, cross border investigations work.
16h00	**End of Day 2**

Day 3, Thursday, 22 April 2021

10h00	**Session 3: Skills Building in Cybercrime** Participants will be divided into groups. Each group will be given a case scenario where they are to use the CoE templates to draft an MLA request and/or other instrument and mechanism of international cooperation. The CoE expert can drip feed them further information based on the requests for information they receive from the groups. The case study should conclude with all the delegates having completed the CoE MLA templates thereby becoming aware of not just how to use the templates but

	also how useful the templates are.
12h00	*Lunch break*
14h00	**Session 3: Skills Building in Cybercrime – Group Report** The rapporteur(s) for each group will report what they have discussed during the group discussion, explain what international cooperation mechanism they have used for the case study and present their draft MLA. The experts will encourage the delegates to explain the reasoning behind their decisions and give helpful and constructive comments on their work.
15h00	**Post-Test and Open Forum** The post-test (same test given during the pre-test) is given to gauge whether participants understood the topics delivered. The experts will answer any questions the delegates may have. This session serves to clarify and strengthen the knowledge and understanding of the delegates relating to international cooperation.
15h45	**Closing Remarks**
16h00	**End of training**

Contact:

Alexandru CRISTEA
Project Manager
Cybercrime Programme Office of the Council of Europe
Email: alexandru.cristea@coe.int
www.coe.int/cybercrime

Liliana TROFIM
Senior Project Officer
Cybercrime Programme Office of the Council of Europe
Email: liliana.trofim@coe.int
www.coe.int/cybercrime