**SPECIALIZED JUDICIAL COURSE ON INTERNATIONAL COOPERATION**

This course can be taught as a three day online course facilitated by a CoE Expert(s). The online version (preferably using the Moodle platform) is recommended due to the present situation around the world with the COVID-19 and the need for social distancing.

Delegates attending this course should have attended the Introductory Training Course.

This specialized judicial course on International Cooperation seeks to discuss the importance of cooperation and coordination amongst different jurisdictions in combatting cybercrime and in the acquisition of digital evidence. 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, prosecuting and adjudicating on cybercrime and cybercrime related cases that parties to the Budapest Convention are prepared to employ a variety of international cooperation modalities available under the Convention in an efficient and timely manner.

It is important that delegates of the training would improve their knowledge and skills on the above issues and would be able to apply this newly acquired expertise during their daily work. The CoE Expert using videos, case studies, actual cases and discussion points should make sure that the delegates actively engage in the training course and encourage them to ask questions.

Unless otherwise stated all training is by Council of Europe experts.

**DAY 0**

A short pre-test delivered as online quiz (30 min to complete). CoE Expert will have an idea of the delegates’ present knowledge of the topics concerned. This gives the CoE Expert an idea of the best way to deliver the training so that it is understood. It will be then coupled with the post-test/feedback assessment to give an indication of what benefit the course has been to the delegates.

**DAY 1**

**11:00 COURSE OPENING AND WELCOME REMARKS**

A short video/online address by a CoE and /or an EU representative

**11:05 1.1 INTRODUCTION TO THE COURSE**

**(Length – 15 min)**

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.

The CoE Expert should also explore with the delegates any concerns they may have or may have experienced in handling cases involving cybercrime and electronic evidence. Such concerns should be listed and addressed by the CoE Expert during the course.

**11:20 1.2 INTERNATIONAL COOPERATION IN A GLOBAL ECONOMY**

**(Length – 40 min)**

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.

There should be:

* What challenges are involved in obtaining electronic evidence in a global economy – this will include amongst others looking at what is the problem
* The need for international cooperation and to be aware of the tools available. This will involve a brief discussion on formal and informal cooperation (with the focus on the Budapest Convention).
  + Formal cooperation (mutual legal assistance in criminal matters – exchange of evidence)
  + Quasi-informal cooperation (exchange of information based on some rules/structure – e.g. Interpol)
  + Informal cooperation (exchange of information informally – e.g. police-to-police cooperation)
  + Private sector cooperation (exchange of information between private sector and law enforcement)

**12:00 1.3 OVERVIEW OF THE LEGAL BASIS OF INTERNATIONAL COOPERATION IN RELATION TO CYBERCRIME AND ELECTRONIC EVIDENCE**

**(Length – 1 Hour)**

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.

Should have:

* A discussion on cybercrime and electronic evidence looking at their main defining characteristics
* Should compare approaches to formal international cooperation in different conventions demonstrating how principles are the same across the conventions but should highlight that the Budapest Convention although principally similar to other conventions has been adapted specifically for electronic evidence.
* A short case study should be discussed that can illustrate challenges for cooperation from the previous session and put legal basis in focus – Both Europol and Interpol have on their websites case details of various successful cross border joint investigations that could be adapted for such a case study

**13:00 LUNCH BREAK (2 hr)**

**15:00 1.4 MUTUAL LEGAL ASSISTANCE PRACTICE AND PROCEDURE**

**(Length – 1 Hour)**

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. Consider using a short case study to demonstrate the kind of challenges that could arise.

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.

**16:00 1.5 INFORMAL METHODS OF INTERNATIONAL COOPERATION**

**(Length – 1 Hour)**

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.

This can include:

* Police to police cooperation (informal networks such G7 and Interpol)
* Europol
* Eurojust
* European Judicial Cybercrime Network
* Global Prosecutors E-Crime Network (International Association of Prosecutors)
* Add regional organizations to this list, if none are known request assistance from the country concerned.

The need for information sharing needs to be mentioned here and delegates need to consider whether other agencies such as the Financial Investigation Units, Multiagency Task Forces, Joint Investigation Units etc… can obtain information/data that other cannot either obtained it or obtain it as quickly.

.

**17:00 END OF DAY 1**

**DAY 2**

**11:00 2.1 MECHANISMS UNDER THE BUDAPEST CONVENTION TO FACILITATE INTERNATIONAL COOPERATION**

**(Length – 2 Hours)**

This will be the central session of the course.

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.

Article 35 (24/7 network) should be also discussed as one of the formal ways of cooperation that can be also utilized for assistance in criminal cases and MLA process.

The session is closed by introduction of the 2nd Additional Protocol of the Budapest Convention. It may be a good idea to have a member of the T-CY record a short video to be played here outlining the progress of the 2nd Additional Protocol.

**13:00 LUNCH BREAK**

**15:00 2.2 UTILIZING DIGITAL EVIDENCE ACQUISITION THROUGH INTERNATIONAL COOPERATION MECHANISMS - CASE STUDY**

**(Length – 1 Hours)**

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.

The case study will discuss the types of data, how it is gathered/obtained through the various international cooperation mechanism including informal methods. How police, prosecutors and others deal with the data. This session will enable prosecutors, judges and magistrates to be able to accurately assess data obtained which will be presented in the next session to the court as evidence.

In this session the case study will allow a discussion of the data concerned and whether the data can be used by the police officer in his/her investigation, and the admissibility or otherwise of the evidence when put before the court by the prosecutor. Include in the discussion any relevant case law of the country or region concerned.

**16:00 2.3 CHALLENGES FACED**

**(Length – 30 min)**

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.

This includes:

* Common law
* Civil law and
* Hybrid systems
* Islamic law

It should be explained that even among countries that may call themselves common law (or civil law) jurisdictions there can still be substantial differences in their legal systems. Under the above legal systems the other challenge is that there are not only different power and functions (for police and prosecutors) but also different codes of procedure in respect of search and seizure.

Other challenges to be discussed include dual criminality.

**16:30 2.4 PUBLIC PRIVATE PARTNERSHIP / COOPERATION**

**(Length – 30 min)**

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.

Emphasis should be put on the practical aspects of cooperation:

* Cooperation with industry
* Social media companies such as Facebook etc..
* Communication Service Providers (CSP) and Internet Service Providers
* Legal Attaché of the Department of Justice

**16:30 END OF DAY 2**

**DAY 3**

**11:00 SKILLS BUILDING IN CYBERCRIME**

**(Length – 2 Hours)**

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.

**13:00 LUNCH BREAK**

**15:00 SKILLS BUILDING IN CYBERCRIME - GROUP REPORT**

**(Length – 1 hour)**

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 CoE experts will encourage the delegates to explain the reasoning behind their decisions and give helpful and constructive comments on their work.

**16:00 POST-TEST AND OPEN FORUM**

**(Length – 45 min)**

The post-test (same test given during the pre-test) is given to gauge whether participants understood the topics delivered. The CoE 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.

The results of the post-test will be communicated to each participant confidentially vis-à-vis the pre-test to determine the level of improvement.

**16:45 CLOSING REMARKS**

**(Length – 15 Mins)**

Course should be closed by:

* A Senior Official of the country concerned
* EU delegation
* Council of Europe (CoE) Project Manager

**17:00 END OF TRAINING**