**Lesson 1.3 International Cooperation in a Global Economy**

|  |  |  |
| --- | --- | --- |
| Lesson 1.3. International Cooperation in a Global Economy | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Internet access (if available) * PowerPoint or other presentation software * Case study synopsis in electronic and/or printed version * Handouts 1, 2, 3 and 4 in electronic and/or printed version | | |
| **Session Aim:**  This session is designed to be 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. | | |
| **Objectives:**  By the end of this session delegates will be able to:   * Recognise the global dimension of Internet and the international dimension of cybercrime * Explain the importance of international cooperation and recognise the available instruments for international cooperation in the field of cybercrime * Identify the need of very fast and efficient channels for international cooperation and the available instruments, the ways they are used, the timelines and effectiveness * Describe the efforts from international organisations regarding the implementation of new modalities of international cooperation * Discuss the Budapest Convention on Cybercrime - identify its general principles | | |
| **Trainer Guidance**  During the session following topics should be considered:   * A discussion on cybercrime and electronic evidence looking at their main defining characteristics * 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) * A case study should be used that can illustrate such challenges | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The opening slides are the introduction to the session and include the Agenda and the session objectives together with some refresher subtopics from Introductory training. | |
| 4 - 6 | These slides are setting the “stage” for basic questions about mutual legal assistance in criminal matters. Expert should present them as a preface to the ensuing proceedings which will occur.  In MLA proceedings, like in domestic investigations, competent authorities will be faced with questions about territorial, authority and inner-authority jurisdiction or competence of the conducting authority/authorities. As in many countries, place of the perpetration will be the defining fact for establishing proper competency.  Delegates should be aware that there are certain difficulties regarding investigations which are exceeding domestic borders. They can be limiting factor like need for cross-border investigation and access to the place of storage of data in the ”cloud” technical environment explained during the electronic evidence session in Introductory training. | |
| 7 to 20 | These slides are refreshing delegates memory about many International organizations which are trying to find adequate approach to the phenomenon of the cybercrime. Interpol, EU 24/7 CoP Network, Europol, Eurojust, European Judicial Cybercrime Network, European Judicial Network, Council of Europe, United Nations, G8, African Union and Commonwealth examples are presented with detailed additional material in the notes of each slide. | |
| 21 to 28 | These slides are refreshing delegates memory about Budapest Convention international cooperation articles and its general principles and specific procedural powers together with international cooperation tools in general sense such as Mutual Legal Assistance Treaties and Mutual Legal Assistance Laws. | |
| 29 to 34 | These slides are presenting some of the existing main defining characteristics of concepts like “computer crime” and “netcrime” together with existing offences classification based on the Budapest Convention provisions.  Expert should explain to delegates that due to the development of the technology it should not be expected that all of the crime should be considered as cybercrime but only the forms which are defined as such by the law or they are dependent on ICT for its perpetration. | |
| 35 to 44 | These slides are presenting electronic evidence exposure to significantly more important challenges for its finding, acquisition, analysis and use during course of criminal proceedings. Slides will cover some of the important aspects of it like challenge of speed, time, attribution and challenge of legal systems and applied rules.  Speed is crucial for finding and acquisition of the electronic evidence. Different countries have different rules regarding keeping and storage of the electronic evidence. Some countries do have data retention regime while others do not. However, it should not be taken for granted that electronic evidence will be possible for acquisition for indefinite period of time. On the contrary, it should be understood that as fast as possible action should be undertaken for securing of it.  Time can be neglected as important part of the cybercrime investigation and electronic evidence finding and acquisition. There are 24 time zones in the world and maximum time difference can be up to 12 hours. Having on mind that one second can make difference between one and another user of dynamic IP address, it is of crucial importance that exact time of perpetration of the crime has been established properly.  Electronic evidence has a source. Source is computer executing computer program used by human. Connection between them must be established to identify the true suspect, later defendant. Paramount importance is that this process is undertaken in accordance to procedural laws in place. If not, whole proceeding is under jeopardy of being abolished on second or later instance of appeal.  World in 2020 has 195 countries and number of different legal systems. Criminal justice systems are complex, and now-days can be not only classical ones like Common or Civil law, but hybrid as well combining different procedures from number of systems. In the International cooperation this fact should be additionally observed and examined. | |
| 45 to 50 | These slides cover the aspects of cooperation in forma, quasi-informal, informal and private sector capacity.  Formal cooperation is most present form of the international cooperation. It has its positive and negative aspects. However, it seems that negative aspects are overweighting positive ones and that they are more of the problem than of a solution today.  Quasi-informal cooperation is rather popular amongst the LEA and prosecution since it uses channels of the communication which are formally set but without necessity for acquiring different approvals or orders by different directly or connected competent authorities. However, question of admissibility of the evidence can be an issue later in proceedings.  Informal cooperation is usually the beginning of all cybercrime investigations both on domestic and international level. However, it has numerous negative aspects which should be addressed.  Public-private sector cooperation in cybercrime regarding international aspects of the crime is extremely important component of the investigation and main trial phase. Private sector providers of the services connected to the information-communication technologies (ICT) are the principle holders of most useful information for the crime investigators, prosecutors and judges.  Cooperation with them in finding the ways how to expedite cooperation and how to make it more precise and useful is of the very high importance if speed in detection and acquisition of the evidence wants to be achieved. Thus, within legal boundaries, all forms of such cooperation should be explored and established not only on the based on coercive measures and orders but on the voluntary agreements and similar forms of cooperation | |
| 51 to 56 | Case study is planned to be organized for illustration of described challenges.  Case study material is provided in the session and training folder. | |
| 57 to 59 | The final slides allow the trainer to review the learning objectives with the audience so that they may be sure that they have been achieved. It is also an opportunity for the delegates to raise any issues that may be outstanding or where they have not fully understood the subjects presented. In addition, the trainer may use the session to check the knowledge learned by asking questions of the participants. This is important as there is no formal assessment for the course. | |
| **Practical Exercises**  Case study is envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No knowledge check or assessment has been requested for this session. | | |