****

**GLACY+**

**Global Action on Cybercrime Extended**

**Action globale sur la cybercriminalité elargie**

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Draft Version March 2018 |

**Advanced Cybercrime and Electronic Evidence Training Course for**

**Judges and Prosecutors**

**2018**

**Training Manual and Resource Pack**



**Contents**

[Introduction 3](#_Toc510174422)

[1. General Overview 5](#_Toc510174423)

[1.1 Aim of the Course 5](#_Toc510174424)

[1.2 Why is this training necessary? 5](#_Toc510174425)

[1.3 The curriculum 6](#_Toc510174426)

[2. How to use the trainers guide? 7](#_Toc510174427)

[3. Course Overview 8](#_Toc510174428)

[3.1 How long is the course and who is it for? 8](#_Toc510174429)

[3.2 Who will deliver the course? 8](#_Toc510174430)

[3.3 How will the course be delivered? 8](#_Toc510174431)

[3.4 Course objectives 8](#_Toc510174432)

[3.5 Target students and trainers group 8](#_Toc510174433)

[3.5.1 Students 8](#_Toc510174434)

[3.5.2 Experience Prerequisites 8](#_Toc510174435)

[3.5.3 Trainers 9](#_Toc510174436)

[3.5.4 Experience Prerequisites 9](#_Toc510174437)

[3.6 Resources 9](#_Toc510174438)

[3.6.1 Course Resources requirements 9](#_Toc510174439)

[3.6.2 Course Resources customisation 9](#_Toc510174440)

[3.7 Assessment 10](#_Toc510174441)

[3.8 Timetable 11](#_Toc510174442)

[3.9 Course and lesson objectives 12](#_Toc510174443)

[4. Key Contacts 15](#_Toc510174444)

[5. Lesson plans 16](#_Toc510174445)

[6. Evaluation 49](#_Toc510174446)

[7. Assessment 49](#_Toc510174447)

Introduction

Given the reliance of societies worldwide on information and communication technologies, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. While in many countries law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges and prosecutors. Experience suggests that in most cases judges and prosecutors encounter difficulties in coping with the new realities of the cyber world. Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

A concept to support such efforts has been developed by the Council of Europe under the Project on Cybercrime in cooperation with the Lisbon Network of judicial training institutions in cooperation with a multi-stakeholder working group in the course of 2009.

The purpose of the concept was to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training.

The objectives of a training concept for judges and prosecutors are:

* To enable training institutes to deliver initial and in-service cybercrime training based on international standards
* To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
* To provide advanced training to a critical number of judges and prosecutors
* To support the continued specialisation and technical training of judges and prosecutors
* To contribute to enhanced knowledge through networking among judges and prosecutors
* To facilitate access to different training initiatives and networks.

Through the Joint Regional Project of the European Union and Council of Europe CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime)[[1]](#footnote-1), the training institutions from the projects areas (Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, “the former Yugoslav Republic of Macedonia”, Turkey and Kosovo[[2]](#footnote-2)) are supported to implement the training concept.

In this context, training materials have been developed to be used by training institutions, a “Training of Trainers Programme” has been carried out and a regional centre created based in Croatia.

The current (2018) update of the course has been undertaken to ensure that the materials are reflecting contemporary development of the cybercrime and perpetrations vectors and that are these factors also relevant to other areas of the world. It is intended that the updated training materials will enable the scenario, at the core of the course, to be adapted for delivery in any part of the world during its implementation phase and the next update. In addition, the presentations have been renewed and reviewed to ensure that they reflect the learning objectives of each session, as well as that lessons are updated in such way which will take into the account changes of technology and approach of the contemporary cybercriminals to the perpetration of such criminal acts.

Under the previous GLACY project a guideline document has been created entitled “Guidelines for the delivery of Council of Europe judicial training courses on cybercrime and electronic evidence”. The document should be available from the Council of Europe website at [www.coe.int/cybercrime](http://www.coe.int/cybercrime). The concept of the COE is to empower countries to develop their own programme by providing the first levels of training and then supporting countries as they incorporate the available training into their programmes. The paper provides information about the available training in order that it may be delivered during and following the involvement of the COE in each country. The report does not repeat the content of the existing material and provides references to that material in order that readers may consider them in conjunction with the information provide therein. The document may be useful for countries that are planning to deliver cybercrime training nationally.

This update of the course is implementing significant changes to the before existing material on the advance training. New case study and new approach to the delivery of topics such mutual legal assistance, applications, hearings and Budapest Convention case studies was adopted. Also, significant changes have been made in the area of electronic evidence and contemporary techniques of committing cybercrime as well. The goal of such significant changes is to present the trainees with contemporary set of the skills which will not only enable them to transfer this knowledge to their prosecution offices and courtrooms, but also to make them competent trainers for the future local training programs.

1. General Overview

## 1.1 Aim of the Course

This course is designed to build upon the introductory training course for judges and prosecutors developed by the Council of Europe GLACY project and further amended and updated by GLACY+ project during 2017. Training is designed with intention to provide judges and prosecutors with additional level of knowledge on cybercrime and electronic evidence and to allow them access to the enhanced levels of understanding and implementation of advanced techniques for legal analysis of presented evidence during the preparatory and main trial phase. The training should provide legal and practical information’s about the subject matters and concentrate on how these issues impact on the day-to-day work of judges and prosecutors.

* *The aim of the course is to provide the knowledge and skills to allow judges and prosecutors to fulfill their roles relating to cybercrime investigation and trial.*
* *This course is designed to build upon the learning outcomes of the basic cybercrime training course for judges and prosecutors and should be attended only by those that have successfully completed that course.*

The course will cover the following subjects:

* *Conducting of an investigation;*
* *Identifying the types of crime committed;*
* *Establishing the location of evidence, witnesses and suspects;*
* *Traditional and alternative currencies;*
* *Securing evidence in an acceptable way, irrespective of where it is held;*
* *Preparing for search and seizure activities involving electronic evidence;*
* *Dealing with digital devices that are part of the investigation;*
* *Briefing of forensic specialists and others needed to support the investigation phase;*
* *Preparing for interviews with suspect;*
* *Presenting cybercrime evidence;*
* *Applications and hearing implementation regarding cybercrime case with respect to the Common and Civil Law criminal legal systems;*
* *Considering the relevant aspects during the judicial proceedings and trial with ultimate goal of rendering rightful decision.*

## 1.2 Why is this training necessary?

Prosecutors and judges play the central role in the investigation and adjudication of individuals or groups that have committed crimes. With the increased number of the incidents where crimes have a digital element, a need is created for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle cases of cyber criminality.

Criminals and criminal groups in general do not apply limitations of themselves and their activities based on the country borders. Cybercrime is the type of the crime that excludes the necessity for the offender to travel locally and across these borders to commit a crime, thus making the investigation and the prosecution of the crime and perpetrator much harder. This situation puts the emphasis on the need for improved international/regional cooperation as well as to the interagency cooperation when dealing with such cases.

Cases of cybercrime often require a swift and very efficient international or regional cooperation, which would provide for a prompt and timely investigation and prosecution. One of the results the training institutions should have is to make the effort to include in their curriculum education modules that would contain knowledge about various possibilities for criminal legal practitioners in ways how these cases can be handled, and also to put additional effort to the training regarding important procedural tools like, for example, the instruments for international cooperation that can be used when investigating cybercrime cases including the use of the 24/7 contacts, mutual legal assistance procedures and tools, judicial cooperation activity, judicial cooperation platforms etc.

## 1.3 The curriculum

This curriculum is a tool to be considered by the training institutions when conducting training on cybercrime. The aim of this document is to focus on the establishment and production of harmonised courses or modules that would be used in project countries/areas in the carrying out of the advance training for judges and prosecutors involved in adjudicating or prosecuting cybercrime cases.

The proposed template of the module for the training is to serve only as the basis for the training of judges and prosecutors and not as the final goal for their training. Project countries/areas should discuss the needs at the national level and request additional specific training in the areas of cybercrime that they identify as most critical.

The lessons that have been prepared provide the headlines/topics of presentations/lectures as well as detailed explanations to be made by the trainers. The course is designed to be amended to meet national requirements, while ensuring that the course aim and objectives are met. This will provide consistency of training modules across borders. Trainers should consider introducing a number of exercises/discussions, which will facilitate the learning experience of the participants in each country.

This Advanced Training Module is built in such a way that will enable judges and prosecutors that have passed through introductory module to enhance their knowledge of the nature of cybercrime, the terms and the technology by dealing with a practical case scenario from the initial complaint, through the investigation and to the trial process finalizing it with sufficient legal grounds and evidence for successful adjudication.

This module has been created with the goal of providing the judges and prosecutors with the additional knowledge that can be applied in practice on the functioning of computers and networks, what is cybercrime, cybercrime legislation, jurisdiction, investigative means and electronic evidence, international cooperation and applications and hearings.

This course has been designed as a mixture of taught lessons and a practical scenario, taken from the first report of the crime through to the preparation of the case for court. The presentations complement the learning created during the practical scenario. The scenario was time specific and will require updating to make it relevant to the period of time in which it is being delivered. It may also be adapted so that the victim company resides in the country in which the course is delivered, in order to make the criminal and procedural legislation more relevant, although effort has been made that scenario follows neutral/fictional countries and entities for avoiding possible political and intellectual property disputes.

2. How to use the trainers guide?

This guide is intended to provide trainers with information on the course structure and content. The objectives for each lesson outline what information should be covered. The training methodology for this course has been prepared and all the relevant training aids should be with this training pack. The aim of this guide is to keep the course standard and ensure consistency during delivery.

It is recommended that training developers ensure that the material they prepare is as up to date and incorporates the latest technology issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. These will be important issues to include in training programmes and require inclusion as changes become more prevalent.

As with any other programme, any training course developed for Judges and prosecutors should have clear objectives, which are SMART (Specific, Measurable, Achievable, Relevant and Time Bound). This is essential to be able to ensure the objectives are met. Avoid use of objectives with words such as “understand” or “know” as these do not meet the criteria. For example how do you measure if the objective of “knowing” a subject is achieved? It is better to use words such as list or identify, which are measurable.

The key role of the training developer is to ensure the overall aim of any learning event and the specific objectives are achieved. This chapter provides some information to assist that process.

Although this course has been developed as a generic, not country specific programme, it is important that trainers personalise their training materials to ensure a more effective delivery of the course material. The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching.

For the 2017/2018 update, the evidence files relate to the fictitious countries, cities and legal and natural persons. Purpose of this approach is to have generic environment which will allow trainees to concentrate on case development through investigation and evidence analysis, followed by legal issues raised both through investigation and court proceeding ending with adjudication.

However, it does not exclude potential of the material to be adjusted to the needs of local judicial training institutions by introducing real geographical and other components for the purpose of achieving more localized experience for the trainees.

3. Course Overview

3.1 How long is the course and who is it for?

This course is designed as a 4-day programme for judges and prosecutors as part of their initial training programme or in-service programme where they have not had the earlier benefit of this training.

3.2 Who will deliver the course?

The course has been developed in order to be delivered by in house trainers within the judicial training centres of countries. Where necessary, it is advisable that subject specialists are introduced to deal with specific technical subjects if the expertise is not available with the judicial centres. For this course it is particularly important to include trainers that have some experience of this type of investigation and criminal procedure.

3.3 How will the course be delivered?

The course as currently structured should be delivered in classroom setting using classroom based trainer instruction and practical paper feed exercises. Still, use of computer equipment, especially mobile computers like laptops and tablets is highly recommended. It is also recommended that the cohort is divided into working groups of not more than 5 people for the entire course. As detailed above, in Section 1, trainers should consider adapting the exercises and other teaching methods in the programme at the national level. This course is very interactive and will require a great deal of investigation work on the part of the students as well as the provision of high levels of support from the trainers on the course.

3.4 Course objectives

The course objectives have been written in a traditional manner that will allow trainers to use various teaching methods to achieve them. All objectives are SMART in order to support this. For those unfamiliar with SMART objectives, the following explanation of the mnemonic is given:

* **Specific -** Objectives should specify what they want to achieve.
* **Measurable** - You should be able to measure whether you are meeting the objectives or not.
* **Achievable** - Are the objectives you set, achievable and attainable?
* **Realistic -** Can you realistically achieve the objectives with the resources you have?
* **Time -** When do you want to achieve the set objectives?

Based on this, the following course objectives have been set and these should be read in conjunction with the overall aim of the course.

3.5 Target students and trainers group

### 3.5.1 Students

This course is designed for delivery to judges and prosecutors during their initial training period or during in service training for those that has not taken this course before.

### 3.5.2 Experience Prerequisites

This course is designed to be attended only by those that have already completed the introductory cybercrime and electronic evidence, training course, designed by the Council of Europe, or its national equivalent.

### 3.5.3 Trainers

Judicial training centres should employ trainers for this course and should include trainers with experience of conducting cybercrime investigations as well as being responsible for the prosecution and adjudication of such cases.

### 3.5.4 Experience Prerequisites

Trainers should have a good level of knowledge of cybercrime issues/ trends and cybercrime legislation in their country of origin. Previous experience as trainers with knowledge of teaching theory and practice is required.

3.6 Resources

### 3.6.1 Course Resources requirements

For delivery of this course in a training room environment, the following equipment is necessary:

* A Room of suitable size for the anticipated number of students. This should be set up utilising one round table per team, where possible based on a guide of 5 students per group;
* PC/Laptop running Windows 7, 8 or 10 and loaded with MS Office Professional;
* Projector and display screen;
* Internet access (if available);
* Copies of the Council of Europe Convention on the Cybercrime;
* Copies of the Council of Europe Electronic Evidence Guide, version 2;
* Whiteboard for each workgroup;
* Whiteboard pens (at least 2 each of blue, black, red and green) for each work group;
* A Flipchart with adequate paper for each work group;
* Student notepaper and pens;
* Stapler, hole punch and scissors for each work group;
* Blue tack or a similar product to allow for paper to be affixed to the walls temporarily per work group;
* One laptop per work group with similar set up to the trainer PC and with Internet access to allow for investigative research to be undertaken;
* All supporting materials provided with the training pack.

The following resources have been prepared to support the delivery of the course. They are provided in electronic form, as they are voluminous. The COE will provide all resources to countries.

### 3.6.2 Course Resources customisation

The course discusses the legal matters arising using the framework of relevant international treaties and conventions (e.g. Council of Europe Budapest and Warsaw conventions). It will be necessary for the trainer to identify the relevant provisions in their national legislation for incorporation into the course material. Examples of decisions, forms, templates etc. from national courts relating to cases involving search, seizure and confiscation of crime proceeds will also be required.

3.7 Assessment

No assessment of student knowledge was requested or provided as a part of this pilot course. Countries implementing this training at the national level may wish to introduce assessment. In any event trainers should check the knowledge of students during the course, by questioning, quizzes or other methods to ensure that the learning objectives are being achieved.

3.8 Timetable



3.9 Course and lesson objectives

|  |  |  |
| --- | --- | --- |
| **Session Number** | **Lesson Title** | **Objectives** |
| 2.1.1 | **Course Introduction and Introduction** | Have an introductory knowledge of Advanced Cybercrime Training for Judges and Prosecutors 2018 agenda and fields of training.  Provide delegates with information about the need for the training course and its aim and objectives.  Ensure that they have sufficient information about the programme of activities and the timetable.  Provide information about the health, safety and administrative details of the course.  Introduce the delegates to the trainers and other delegates. |
| 2.1.2 | **Refresher on the Budapest Convention and New Aspects** | Budapest Convention Substantial, Procedural and International Cooperation aspect of the ETS 185 with Additional Protocol on Xenophobia and Racism  Guidelines and Opinions  Second Additional Protocol progress  New Aspects of the connected activities |
| 2.1.3 | **Technology and Cybercrime** | Explain the different types of Business Email Compromise  Identify the threats offered by the Internet of Things (IOT)  Differentiate between the layers of the Internet  Explain how virtual currency transactions are conducted |
| 2.1.4 | **Budapest Convention Case Study** | Recall the substantive law, procedural law & international cooperation-related provisions of the Budapest Convention covered in the introductory course  Explain the scope and extent of the substantive law, procedural law & international cooperation-related provisions of the Budapest Convention  Apply the provisions of the Budapest Convention and corresponding domestic legislations apply to case studies related to substantive, procedural & international cooperation law |
| 2.2.1  2.2.2 | **Introduction to the Case Study**  **Investigation Exercise** | Identify legal and natural persons involved in scenario.  Explain case layout and state of the introductory facts.  Follow and explain flow and development of the case investigation.  Explain how the criminal act was perpetrated and who were the key players.  How and where criminal investigation should start and what should the vectors be. |
| 2.3.1 | **Electronic Evidence Challenges** | Identify methods of validating electronic evidence.  Review admissibility issues for electronic evidence in the trial process  Examine and explain has values of electronic evidence files |
| 2.3.2 | **Mutual Legal Assistance – International Cooperation** | Learn or remind themselves of the basic principles of mutual legal assistance applied to cybercrime  Identify good practices in preparing and drafting of a request  Have a constructive view on foreign requests they may receive for execution |
| 2.3.3 | **Drafting Applications**  **or**  **Requesting Authorization** | Recognize particular considerations relating to the drafting of applications for exercise of electronic evidence procedural powers  Realize the contents of a typical application including scope & duration and other requests  Understand what to look for in an application seeking exercise of electronic evidence procedural powers  Understand some of the considerations and safeguards that should be kept in mind when drafting and looking at applications for exercise of electronic evidence procedural powers |
| 2.3.4 | **Conducting Hearing and Drafting Orders**  **or**  **Considering Request for Authorization**  **Preparation for hearing**  **Hearing Exercise**  **or**  **Preparation for Exercise on Considering Requests for Authorization** | Recognize various considerations with respect to conducting hearings on applications for the exercise of electronic evidence procedural powers  Explain the conditions and procedural safeguards that are relevant to applications for the exercise of electronic evidence procedural powers  Identify important judicial skills that may be implemented to effectively conduct a hearing on electronic evidence procedural powers  Understand the key elements of a judicial order enabling exercise of electronic evidence procedural powers to be considered while drafting such order |
| 2.3.5 | **Preparation for Hearing Exercise**  **or**  **Considering Requests for Authorization** | Group work on previous module. |
| 2.4.1 | **Hearing Exercise**  **or**  **Exercise on Considering Requests for Authorization** | Recognize various considerations with respect to conducting hearings on applications for the exercise of electronic evidence procedural powers  Explain the conditions and procedural safeguards that are relevant to applications for the exercise of electronic evidence procedural powers  Identify important judicial skills that may be implemented to effectively conduct a hearing on electronic evidence procedural powers  Understand the key elements of a judicial order enabling exercise of electronic evidence procedural powers to be considered while drafting such order |
| 2.4.2 | **Feedback on Hearing Exercise**  **or**  **Feedback on Exercise on Considering Requests for Authorization** | Feedback on hearing or request for authorization exercise by delegates and trainers. |
| 2.4.3 | **Course Closure** | Provide appropriate feedback on the course and its effectiveness  Evaluation form dissemination  Complete the course evaluation forms  Identify the next level of learning that they need to undertake to improve their knowledge and skills in the subject matter.  Closing remarks and way forward |

4. Key Contacts

The following persons are the points of contacts for any enquiries about the course and its content:

|  |
| --- |
| Alexander Seger  Head of Cybercrime Division  Directorate General of Human Rights and Rule of Law (DG-I)  Council of Europe  F-67075 Strasbourg Cedex  Tel. +33 3 88 41 21 03  Fax +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int)  Matteo Lucchetti  Programme Manager  Cybercrime Programme Office (C-PROC), Cybercrime Division  Directorate General of Human Rights and Rule of Law (DG-I)  Council of Europe  Bucharest, Romania  Tel. +40 (21) 201 78 30  [matteo.lucchetti@coe.int](mailto:matteo.lucchetti@coe.int) |

5. Lesson plans

Lesson 2.1.1 (Course Opening and Introduction)

|  |  |  |
| --- | --- | --- |
| Lesson 2.1.1 (Course Opening and Introduction) | | Duration: 30 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The aim of this session is to introduce delegates about course of the training and agenda topics and fields which will be covered. | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Have an introductory knowledge of Advanced Cybercrime Training for Judges and Prosecutors 2018 agenda and fields of training. * Provide delegates with information about the need for the training course and its aim and objectives. * Ensure that they have sufficient information about the programme of activities and the timetable. * Provide information about the health, safety and administrative details of the course. * Introduce the delegates to the trainers and other delegates. | | |
| **Trainer Guidance**  This presentation is of introductory nature and should give overall picture and impression about training and skills which are going to be developed during its course. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. Health and safety questions will be covered as well. | |
| 4 | This slide provides information about the background of the course is provided for the delegates, The title of this course is “Advanced Cybercrime and Electronic Evidence Training for Judges and Prosecutors”. It has been developed as an output of the European Union/Council of Europe Joint Project on Regional Cooperation on Cybercrime in the IPA region. Latest additions are belonging to the GLACY and GLACY+ projects. | |
| 5 | This slide provide information about This training is necessary because Judges and prosecutors play an important role in the investigation and adjudication of individuals or groups that have committed crimes.  With the increased number of incidence where these crimes have an element of cybercrime there is an increased need for judges and prosecutors to be properly trained to understand the nature of these crimes and to also be aware of the legislation and the instruments for international cooperation available to handle cases of cybercrimes. | |
| 7 | Overall aim of the course is explained to the delegates at the very beginning.  This will enable them to appreciate the overarching reason for them being there.  The aim of the course is to provide the knowledge and skills to allow judges and prosecutors to fulfill their roles relating to cybercrime investigations.  This course is designed to build upon the learning outcomes of the basic cybercrime training course for judges and prosecutors and should be attended only by those that have successfully completed that course. | |
| 8 | Session objectives. | |
| 10 | This slide is left blank for each country to complete with the names of the trainers that are teaching the course. | |
| 12 | Methodology slide should provide information about further content of the training as a mixture of presentations and exercises based around a scenario.  It is structured in that way as a result of requests received during the basic course for more information on cases and digital forensics.  This course will enable the delegates, not only to listen to experts providing information, but also to work on an investigation themselves, working on the information that will be provided during the course. | |
| 13 | The course timetable should be explained to the students at this stage.  This should include the times of the course, the lunch and other breaks and a brief description of each session.  The inclusion or exclusion of any assessment should be dealt with at this stage.  If there is an assessment, this should be explained in detail, including the expectations of the students in terms of study. | |
| 15 | This slide provides introduction of the trainers and students as the next stage. It is important to take this early opportunity to get them to interact with each other and the trainers. The delegates should be asked to pair with someone in the class that they do not already know.  They should then be directed to ask their “partner” the to provide answers to these questions:  Their Name and Country  Where they work  What they do  Their experience as a trainer  Something Interesting about them  The pairs should ask the same questions of each other.  They should then introduce their “new colleague to the rest of the class.  The trainer should keep notes of the information that is provided to assist their knowledge of the students. | |
| 16 | The trainer should recap / test knowledge on the following points to ensure that the students have appreciated the learning objectives of the session.  Time should be allowed for questions at appropriate times during the session. | |
| **Practical Exercises**  There are no compulsory practical exercises. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |

Lesson 2.1.2 (Updates on the Budapest Convention – Access to the evidence in the cloud and the Additional Protocol)

|  |  |  |
| --- | --- | --- |
| Lesson 2.1.2 (Updates on the Budapest Convention – Access to the evidence in the cloud and the Additional Protocol) | | Duration: 60 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The aim of this session is to introduce delegates about course of the training and agenda topics and fields which will be covered. | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Provide an updated picture of the reach of the Budapest Convention * List the main issues encountered when accessing electronic evidence on the cloud * Explain what solutions are currently being pursued in the context of international legislation | | |
| **Trainer Guidance**  This presentation should provide update to trainees and delegates about latest developments regarding Council of Europe Convention on Cybercrime (ETS 185) and capacity building projects organized by the Council and implemented by the C-PROC office.  It should also present latest developments in the field of contemporary perpetration of the cybercrime criminal acts. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 - 5 | This slide provides information about main contemporary challenges regarding understanding and practical implementation of substantial, procedural and international law in the field of cyber criminality. | |
| 6 | This slide provides information about Budapest Convention, its implementation and articles. Trainers should have text of the Convention with Explanatory notes ready at side. | |
| 7 | Reach of the Convention graphical slide. 130+ countries ratified, signed or are implementing in different ways Convention. | |
| 8 | Scope of the Convention slide. Criminal conduct, Procedural tools and International cooperation articles of the Convention graphically presented with emphasize on harmonisation link and need. | |
| 9 | This slide is presenting challenges of evidence and Cloud computing and Cybercrime Convention relation to it. | |
| 10 - 11 | Slides are presenting the organization and work of T-CY Committee Cloud Evidence Group (CEG), including issues which were identified and for which T-CY should in possible and effective way recommend solution. | |
| 12 | This slide provides information about comparison between subscriber, traffic and content data. | |
| 13 | This slide provides information about Mutual legal assistance and contemporary challenges of continuous and successful cooperation regarding cyber-crime. | |
| 13 | This slide provides information about Mutual legal assistance and contemporary challenges of continuous and successful cooperation regarding cyber-crime. | |
| 13 | This slide provides information about Mutual legal assistance and contemporary challenges of continuous and successful cooperation regarding cyber-crime. | |
| 14 - 15 | Loss of location slide. Trainer should be aware of the challenges presented on T-CY meetings with this regards and solutions implemented so far by different national jurisdictions. | |
| 16 - 18 | These slides are giving closer insight in public-private cooperation namely, in this case, between competent criminal justice authorities and Internet service provider companies. Different aspects are considered with this regards like presence of the ISP, offering of the services, voluntary disclosure of BSI and traffic data by ISP’s in certain countries (or not) etc.  2015 statistical data for certain companies and countries is provided as well. | |
| 19 - 20 | Slides are covering emergency procedures through MLA and Direct cooperation and data protection and other safeguards. | |
| 21 - 28 | These slides are covering solutions identified by CoE Cloud Evidence Group, including more efficient MLA, Guidance Note on Art. 18 of Budapest Convention, Domestic rules on production orders, Cooperation with providers: practical measures and additional Protocols to Budapest Convention. | |
| **Practical Exercises**  There are no compulsory practical exercises. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |

Lesson 2.1.3 (Technology and Cybercrime)

|  |  |  |
| --- | --- | --- |
| Lesson 2.1.3 (Technology and Cybercrime) | | Duration: 150 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The aim of this session is to update delegates in relation to new crime types and threats delivered by new technology. Although some of the subjects were covered briefly on the introductory course, they are covered in more detail in this session | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Explain the different types of Business Email Compromise * Identify the threats offered by the Internet of Things (IOT) * Differentiate between the layers of the Internet * Explain how virtual currency transactions are conducted | | |
| **Trainer Guidance**  This session introduces the latest technologies that are impacting on criminal behaviour. The Internet Online Threat Assessment (IOCTA) 2017 was released in September 2017 and is used in some slides as it is the most up to date information available. Trainers will need to revisit this information as new reports and information becomes available. The videos used in this session are acknowledged and are available for free download and use. The trainer may wish to use demonstration as a teaching method, for example in the Darknet session, by using the TOR browser to show delegates how to access on line crime tools. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 18 | These slides provide information about the influence of the Internet, on a global scale (slides 5 to 12) and specifically for the country that the course is being delivered (slides 13 to 18). The trainer should ensure that these slides are relevant to the country of delivery and use them to discuss the impact of the Internet in the country and in the global context. | |
| 19 to 30 | These slides provide information about recent crimes that impact at a significant level. The trainer should familiarise themselves with the crimes and introduce those that are relevant to the region of the training delivery. The trainer may wish to substitute cases from the country. | |
| 31 to 32 | Introduces information from IOCTA 2017 in relation to BEC. | |
| 33 | Trainer to ask the delegates the question in the slide. If there is no response, continue with the presentation. If there are some examples, give time for explanations from the delegates and use the information given to compare with the information in the presentation | |
| 34 to 42 | These slides and the videos are sourced from Trend Micro/Europol information and data and provide a very good explanation of the business Email Compromise methodologies and prevention measures. The final video introduces Business Process Compromise (BPC) as a variation of BEC. | |
| 43 to 44 | These are an introduction to the subject of Internet of Things (IOT). The trainer should invite the delegates to share any knowledge or experience they may have of IOT.  Please note that Slide 45 is a video that gives a very good example of how a motor vehicle may be connected to multiple services by IOT and how the services may be of great benefit to a customer. The trainer may also reflect on the availability of electronic evidence because of these connections. | |
| 45 | This video gives a very good example of how a motor vehicle may be connected to multiple services by IOT and how the services may be of great benefit to a customer. The trainer may also reflect on the availability of electronic evidence because of these connections. | |
| 46 | This slide provides an opportunity to introduce IP version 6 as the platform that enables IOT | |
| 47 | This slide gives the trainer the opportunity to discuss the issues of security of the IOT devices and the fact their producers are not security experts. IOT devices are a security time bomb. The trainer may wish to expand on the bullet points according to their own knowledge of the subject. | |
| 48 to 49 | These slides provide further up to date information from the IOCTA 2017 report. They support the issues raised in slide 20. | |
| 50 to 57 | These slides give information about IOT devices and some of the issues. Trainers are encouraged to use examples they are aware of and in particular if there are security issues with them, such as is the case with the iKettle. | |
| 58 to 60 | This is the beginning of the session on Dark net and services. These slides provide the context from IOCTA to set the subject in motion. | |
| 61 to 67 | These slides explain the Darknet, criminal use and services, as well as some successes in closing sites used for criminal activity. The trainer is encouraged to use live demonstrations of accessing the Darknet where appropriate and there is a suitable Internet connection. | |
| 68 to 77 | These slides are mostly a reminder of the issues raised in the introductory course, with additional video support and, as with other subjects, the most up to date information from the IOCTA 2017 report. | |
| 78 to 79 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  There are no compulsory practical exercises, although trainers are encouraged to give live demonstration of Darknet access where appropriate. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |

Lesson 2.1.4(Budapest Convention Case Study)

|  |  |  |
| --- | --- | --- |
| Lesson 2.1.4 (Budapest Convention Case Study) | | Duration: 60 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. * Copies of case study and Budapest Convention for delegates | | |
| **Session Aim:**  The purpose of this session is to provide delegates with an opportunity to develop practical aspects of their knowledge of the Budapest Convention by working on a case study problem that covers substantive law, procedural powers, mutual legal assistance and other forms of international cooperation enabled by the Budapest Convention. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Recall the substantive law, procedural law & international cooperation-related provisions of the Budapest Convention covered in the introductory course * Explain the scope and extent of the substantive law, procedural law & international cooperation-related provisions of the Budapest Convention * Apply the provisions of the Budapest Convention and corresponding domestic legislations apply to case studies related to substantive, procedural & international cooperation law | | |
| **Trainer Guidance**  Budapest Convention is the first international treaty specifically addressing cybercrimes, procedural powers relating to cybercrimes and electronic evidence and international cooperation between parties. This advanced lesson is in the form of a short case study that covers all aspects of the Budapest Convention, relying on concepts covered in introductory modules related to substantive law, procedural powers, mutual legal assistance and public-private cooperation. The case study is appropriately divided into four parts and the accompanying presentation which includes an introduction to the case study has five parts. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 18 | These slides introduce the delegates to the facts and questions of the case study that the delegates will be expected to work on. The trainer should explain the facts in detail to the delegates and in particular should focus on the key aspects of the facts that are important for the purposes of answering the questions. The trainer should give an opportunity to the delegates to ask any questions about the facts or any of the questions at this preliminary stage before giving them time to solve the case study. | |
| **Case Study Exercise** | | |
| 19 to 35 | These slides cover the questions pertaining to substantive law. It is expected that the delegates have had the opportunity to attempt to answer the relevant questions. The trainer should revise the relevant facts and then deal with each question individually. The slides are organised in this way. Each question is followed by slide(s) highlighting facts relevant to the question, which is followed by slide(s) highlighting relevant parts of related Budapest Convention provisions, which is finally followed by the appropriate responses and explanations.  The trainer should give ample opportunities to the delegates to verbally answer the questions to sharing answers to the questions. These slides are intended to test both theoretical and practical aspects of the delegates’ understanding of the Budapest Convention and in particular concepts related to Articles 2 (Illegal access), 5 (System interference) and 6 (Misuse of devices) of the Budapest Convention. | |
| 36 to 51 | These slides cover the questions pertaining to procedural powers. It is expected that the delegates have had the opportunity to attempt to answer the relevant questions. The trainer should revise the relevant facts and then deal with each question individually. The slides are organised in this way. Each question is followed by slide(s) highlighting facts relevant to the question, which is followed by slide(s) highlighting relevant parts of related Budapest Convention provisions, which is finally followed by the appropriate responses and explanations.  The trainer should give ample opportunities to the delegates to verbally answer the questions to sharing answers to the questions. These slides are intended to test both theoretical and practical aspects of the delegates’ understanding of procedural powers of the Budapest Convention and skills in regard to identifying relevant procedural powers to exercise given certain facts. In particular concepts related to Article 16 (Expeditious Preservation of Stored Computer Data), 18.1.a. & 18.1.b. (Production order related to subscriber information & computer data) of the Budapest Convention are tested in this part. | |
| 52 to 64 | These slides cover the questions pertaining to other forms of international cooperation. In particular they cover forms of international cooperation enabled by the Budapest Convention that do not require mutual legal assistance requests. It is expected that the delegates have had the opportunity to attempt to answer the relevant questions. The trainer should revise the relevant facts and then deal with each question individually. The slides are organised in this way. Each question is followed by slide(s) highlighting facts relevant to the question, which is followed by slide(s) highlighting relevant parts of related Budapest Convention provisions, which is finally followed by the appropriate responses and explanations.  The trainer should give ample opportunities to the delegates to verbally answer the questions to sharing answers to the questions. These slides are intended to test both theoretical and practical aspects of the delegates’ understanding of forms of cooperation under the Budapest Convention. In particular concepts related to Article 18.1.b. (Direct trans-border production orders seeking subscriber information) and Article 32 (Trans-border access to data with consent) are the subject of the questions included in this part. | |
| 65 to 79 | These slides cover the questions pertaining to mutual assistance. It is expected that the delegates have had the opportunity to attempt to answer the relevant questions. The trainer should revise the relevant facts and then deal with each question individually. The slides are organised in this way. Each question is followed by slide(s) highlighting facts relevant to the question, which is followed by slide(s) highlighting relevant parts of related Budapest Convention provisions, which is finally followed by the appropriate responses and explanations.  The trainer should give ample opportunities to the delegates to verbally answer the questions to sharing answers to the questions. These slides are intended to test both theoretical and practical aspects of the delegates’ understanding of mutual assistance related provisions of the Budapest Convention and skills in regard to identifying relevant mutual assistance provisions to use given certain facts. In particular concepts related to Article 29 (Expedited Preservation of Stored Computer Data), Article 30 (Expedited Disclosure of Preserved Traffic Data), Article 31 (Mutual assistance regarding accessing stored computer data) and Article 33 (Mutual assistance regarding real-time collection of traffic data) are tested in this part. | |
| 80 to 82 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  The delegates are expected to complete the case study included in this lesson after the trainer completes Slides 1 to 18. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively after completion of case study exercise. | | |

Lesson 2.2.1 (Introduction to the Case Study)

|  |  |  |
| --- | --- | --- |
| Lesson 2.2.1 (Introduction to the Case Study) | | Duration: 30 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  Purpose of this session is to present basic concepts of the Case Study. Session should also present conclusive session of this first part of the course, which will serve for following presentations about Business E-mail Compromise schemes, virtual currencies, and Budapest Convention. | | |
| **Objectives:**  By the end of the lesson the students will be able to:   * Identify legal and natural persons involved in scenario. * Explain case layout and state of the introductory facts. * Follow and explain flow and development of the case investigation. * Explain how the criminal act was perpetrated and who were the key players. * How and where criminal investigation should start and what should the vectors be. | | |
| **Trainer Guidance**  This session has been prepared to provide delegates with an introductory explanation about key elements of the Case Scenario. This session has been divided into five parts. Part One of the presentation will make introduction and present key parties of the case. Part Two will present case layout. Part Three will perpetration of the criminal act. Part Four will lay down grounds for beginning of the investigation and work of the trainees. Part Five is summary of previously presented. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 9 | These slides are providing introduction into the fictitious world of countries who are non-existent in the real world, but which ratified Budapest Convention, for the purpose of the training. Trainees are going to be acquainted with Federal Bank of Atlantis, United Bank Printing and Docklands Securitas Bank of Norland.  Case study scenario begins with establishment of Federal Bank of Atlantis (FBA) as well known, well and long established and reputable international bank. Description like this should lead trainees into direction that this kind of bank shouldn’t be involved in any kind of problems, let alone ones similar to one which is going to be described further on.  Trainees should identify main facts and key business divisions and players in order to understand the scope and the setup of the business circle in which further case facts are going to be laid-down. | |
| 10 to 14 | For this training fictitious countries and companies have been created. These are Atlantis, Norland, Ostland, Westland etc. For the exercise, all of them have ratified the Council of Europe Convention on Cybercrime (“Budapest Convention”).    This approach is to allow transferability of the training among jurisdictions, without the need for major changes to the course materials.  Financial setup should indicate that initial banking transfer was without problems and that mentioning of SWIFT and IBAN accounts means that money transfer is of the international, not domestic nature. | |
| 21 to 25 | These slides are presenting the beginning of the Investigation. Investigation should commence in working groups with group leaders and members starting to work on the case from the base provided in the Case Material.  Electronic evidence should be examined and used as essential tool for building up and finishing of the investigation and preparing case for the trial. | |
| 26 to 27 | Summary.  Repeating of all main steps is recommended with giving of some additional time for the trainees to ask questions and cope with the Case Scenario “reality”.  Trainers should be very much knowledgeable about both case and mechanics used for its creation ready to answer and assist to trainees. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |

Lesson 2.2.2 (Case Study Evidence Overview and Investigation Exercise)

|  |  |  |
| --- | --- | --- |
| Lesson 2.2.2 (Case Study Evidence Overview and Investigation Exercise) | | Duration: 360 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  Purpose of this session is to present basic concepts of the case study evidence. Important parts should be presented only, without going into too many revealing details in order not to make exercise unchallenging. | | |
| **Objectives:**   * By the end of the lesson the students will be able to: * Understand introduction to and initial evidence of the case; * Understand development of the case by analyzing presented electronic and real evidence; * Follow actual perpetration and find additional facts in witness statements; * Find additional information about key terms and definitions of cyber world and crime tools and used in this case. | | |
| **Trainer Guidance**  This session has been prepared to provide delegates with an introductory explanation about key evidence elements of the Case Scenario. This session has been divided into five parts. Part One of the presentation will make introduction to the initial evidence provided in the case scenario material. Part Two will present case layout. Part Three will perpetration of the criminal act. Part Four will lay down grounds for beginning of the investigation and work of the trainees. Part Five is summary of previously presented. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 9 | These slides are providing introduction into the scenario which begins with establishment of Federal Bank of Atlantis (FBA) as a well-known, long established and reputable international bank. A description like this should lead trainees to conclude that this kind of bank shouldn’t be involved in any kind of problems, let alone ones similar to that, which are going to be described later in this document.  Company profile of companies involved in the Case Scenario. 3 different MS Word files in 97-2003 format are produced in the material. They should be at the disposal for delegates in hard copy, or, if circumstances allow and all delegates have single access to the computers, in electronic way.  Miscellaneous supporting documents for the Case Scenario. 3 different MS Word files in 97-2003 and in Adobe Reader format are produced in the material. They should be at the disposal for delegates in hard copy, or, if circumstances allow and all delegates have single access to the computers, in electronic way. | |
| 10 to 13 | Case development follows 10 e-mails which are regular ones following exchange between FBA and UBP persons in charge of different business and contract deals for printing Anniversary bond.  FBA – UBP contract is following e-mail exchange and puts into the perspective outline of the commercial framework of the deal. It also sets crucial steps for further case development.    Bank statements are closely following development of the case. Delegates will be able to implement “follow the money” principle by analyzing FBA and UBP bank statements.  Pro forma invoice is genuine one issued by UBP to FBA for 100K advance. | |
| 14 to 16 | Glossary slides.  Investigation should commence in working groups with group leaders and members starting to work on the case from the base provided in the Case Material. | |
| 22 | Summary.  Repeating of all main steps is recommended with giving of some additional time for the trainees to ask questions and cope with the Case Scenario “reality”.  Trainers should be very much knowledgeable about both case and mechanics used for its creation ready to answer and assist to trainees. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |

Lesson 2.3.1 (Electronic Evidence Challenges)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.1 (Electronic Evidence Challenges) | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. * Hard copies of the evidence file mail11.doc and the additional file mail11(hash).doc for each delegate * Copies of the COE Electronic Evidence Guide and the COE Digital Forensic Laboratory Guide | | |
| **Session Aim:**  The purpose of this session is to provide delegates with an opportunity to consider the challenges to the electronic evidence that is used in the BEC case study. | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Identify methods of validating electronic evidence. * Review admissibility issues for electronic evidence in the trial process * Examine and explain has values of electronic evidence files | | |
| **Trainer Guidance**  The main purpose of this session is to lead the delegates towards identifying the main admissibility issues involving electronic evidence and the importance of them being able to consider the them on the context of allowing or rejecting electronic evidence. They are introduced to the ability to check evidence by validating hashes of different files. There are limitations to being able to assess different types of evidence as the email evidence is created in MS word files and there are no artefacts to consider. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 5 | These slides provide definitions of electronic evidence and list some of the unique characteristics. The delegates should be reminded that they were introduced to these issues in greater detail in the introductory course | |
| 6 to 11 | These slides set out in greater detail than covered in the introductory course, the considerations for the admissibility of electronic evidence. The trainer should ensure they cover all aspects of the slides | |
| 12 to 13 | These slides remind the delegates that their national legislation and practice takes precedence, and reminds them of the availability of COE documents that cover the issue of electronic evidence. The delegates should be encouraged to acquire them. | |
| 14 | The trainer should ask the questions on the slide and be prepared to discuss the real case examples before moving on to the course case study evidence. | |
| 15 to 16 | These slides list the documents used in the case study. The delegates should be asked if there are any admissibility issues they have identified with any of the documents and the trainer should lead a discussion about these. | |
| 17 to 22 | These slides are the demonstration of hashing of files and how one small change to a file can be identified by this process. The use of the files mail11.doc and mail11(hash).doc are fundamental to this session. It is recommended that the trainer gives a demonstration of hashing and comparing two files where there is one minor difference. | |
| 23 | This slide sets out some of the advantages of electronic evidence, how it may be validated and some questions judges may ask | |
| 24 to 25 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  The practical exercise is dealt with in slides 16 to 21. The trainer should consider a live demonstration of hashing on the lines shown. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |

Lesson 2.3.2 – Mutual Legal Assistance Requests: practicalities

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.2 - Mutual Legal Assistance Requests: practicalities | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Whiteboard. * Whiteboard pens (at least 2 each of blue, black, red and green). * 2 Flipcharts with adequate paper. * Student notepaper and pens. * If possible, local examples of mutual legal assistance requests (for visualization and/or discussion on good or bad practices) | | |
| **Session Aim:**  The overall purpose of this lesson is to bring basic knowledge of mutual legal assistance principles on a practical level to delegates who may not be familiar with the use of MLA requests. It also aims at sharing practical tips and good practices applicable no matter what country the delegate come from or where they would intend to send an MLA request.  This lesson will explore all steps from the preparation to the drafting of a request, as well as the way a foreign request should be approached in order to allow for its execution.  This lesson should give participants the necessary, basic tools and reflexes before the drafting exercise during which they will be asked to draft a mutual legal assistance in a cybercrime case. | | |
| **Objectives:**  By the end of the lesson, the delegates will be able to:   * Learn or remind themselves of the basic principles of mutual legal assistance applied to cybercrime * Identify good practices in preparing and drafting of a request * Have a constructive view on foreign requests they may receive for execution | | |
| **Trainer Guidance**  This session aims at preparing delegates to the drafting exercise. It may also be used, if needed, as a general course for all delegates. This session will not present legal rules of MLA, which depend on each country, but it will focus on the practical aspects or tips which can help delegates with the drafting with a view of a better execution of MLA requests. Although cybercrime and mutual legal assistance are often related, judges or prosecutors specialized in cybercrime may not always be familiar with MLA rules, and vice versa. This session aims at providing delegates with a practical view of MLA in cybercrime cases, which can be completed by the study of theoretical rules applicable to the specified country (outside of this course). | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3  Mandatory | The first slides set out the agenda and objectives of the session. The objectives for this session are explained to the delegates, these are the things that the delegate should be able to do or understand at the end of the session. These objectives may be used to test the knowledge obtained and to allow the delegates to evaluate the training. | |
| Slides 4 to 7  Mandatory | These slides remind delegates of the general principles of mutual legal assistance, and try to put in perspective general principles and challenges brought about by technology. | |
| Slide 8  Not mandatory | This chart tries to summarize the main differences and challenges between a “traditional crime” and a crime committed in the digital world. | |
| Slide 9  Mandatory | This slide sums up the challenge between sovereignty (principle) and efficiency/speed (very much needed in cybercrime) | |
| Slide 10  Not mandatory | This slide details the challenge set up in slide 9. | |
| Slide 11  Mandatory | Time for questions and exchange with delegates. | |
| Slides 12 to 20  Mandatory  (except slide 19) | These slides deal with the useful steps to go through in order to better prepare a mutual legal assistance request, including the use of articles 29 and 35 of the Budapest convention (24/7 network for expedited preservation requests). | |
| Slides 21 to 52  Mandatory (except slides 23, 24, 26 to 40, 44, 45, 47, 48) | Theses slides explore the different steps to go through during the drafting phase of a request. They include regional examples (non-mandatory slides 23 to 24 regarding the European Investigation Order in the European Union, as well as a model of a model MLA form by the council of Europe (non-mandatory slides 26 to 39), in order for the delegates to visualize an example of request (no universal, mandatory model). This part could be possibly completed with other examples of regional or local initiatives.  The following slides go through the different parts of a request to be drafted, i.e. the legal basis, useful contact information, summary of facts, specific demands (slides 41 to 44). It brings tips in all these sections.  Then, slides 44 and 46 focus on requests sent to the US.  Slides 46 to 49 explore other tips for better drafting. | |
| Slides 53 to 61  Mandatory  (except slides 57, 58) | These slides aim at giving tips on how to consider in practice a foreign request, notwithstanding the applicable legal national rules.  Slides 59 to 61 (blank) should be used to detail some of the specific, national rules regarding the execution of foreign requests. | |
| Slides 62 to 64 | These slides provide for a summary of the objectives which should have been reached at the end of the lesson, and for a time for discussion with and questions from delegates. | |
| **Practical Exercises**  No practical exercises are prepared for this session | | |
| **Assessment/Knowledge Check**  The trainer should check knowledge and understanding by asking relevant questions during each of the session aspects, for instance by raising local examples. | | |

Lesson 2.3.3 (Drafting Applications)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.4 (Drafting Applications) | | Duration: 60 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The purpose of this lesson is to provide delegates with guidelines on applying for investigative or procedural powers corresponding to the Budapest Convention. This lesson will also provide information on what judicial officers or other competent authorities should expect from law enforcement or prosecutors applying for procedural powers. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Understand ways in which different legal systems enable applying for procedural powers * Recognize particular considerations relating to applying for procedural or investigative measures relating to electronic evidence * Understand some of the considerations and safeguards that should be kept in mind when applying for procedural powers | | |
| **Trainer Guidance**  Many jurisdictions require law enforcement officers, prosecutors or other persons concerned with conducting investigations into criminal offences to apply to a judicial or other competent authority seeking authorisation to exercise procedural powers. The trainer is required to explain that some jurisdictions require written applications whereas others require verbal requests seeking authorisation to undertake procedural or investigative measures. The trainer should also ensure that this lesson be delivered keeping in mind conditions and safeguards relating to Article 15 of the Budapest Convention. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 8 | These slides provide a recap of certain key aspects of the Budapest Convention that are relevant to the lesson. They include a list of the various procedural powers under the Budapest Convention. The trainer should also use these slides to refresh key concepts under Article 15 of the Budapest Convention. The trainer should also distinguish between the processes for seeking authorization to exercise procedural powers in different legal systems. This part also provides a brief introduction to Part 2, 3 & 4 of the session – the “what”, “how” and “why” of applications for exercise of procedural powers. | |
| 9 to 22 | These slides relate to the “what” of applications for exercise of procedural powers. They cover both the aspect of subject data and subject persons in relation to an application for procedural power. The slides refer to the investigation exercise case study to provide examples of how subject persons and subject data are identified. | |
| 23 to 54 | These slides relate to the “how” of applications for exercise of procedural powers. They explain how procedural powers are meant to be applied. In doing so, they cover both technical aspects of how procedural powers are to be applied (i.e. which procedural powers will be exercised in relation to different investigations, and what technical measures will be taken to exercise such powers), as well as protective aspects of how procedural powers are to be applied (i.e. conditions and safeguards at the application stage, at execution stage and post-execution stage). The slides refer to the investigation exercise case study to provide examples of technical and protective measures that may be stated in an application. | |
| 55 to 66 | These slides relate to the “why” of applications for exercise of procedural powers. This part of the session is focussed on explaining the grounds for exercise of procedural powers. The slides refer to the investigation exercise case study to provide examples of grounds that may be stated and further elaborated in an application. | |
| 67 to 77 | These slides explain certain formalities of written applications in different jurisdictions. The trainer may need to adapt these slides to align with local requirements. | |
| 78 to 80 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |

Lesson 2.3.4 (Requesting Procedural Powers)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.4 (Requesting Procedural Powers) | | Duration: 60 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The purpose of this lesson is to provide delegates with guidelines on applying for investigative or procedural powers corresponding to the Budapest Convention. This lesson will also provide information on what judicial officers or other competent authorities should expect from law enforcement or prosecutors applying for procedural powers. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Understand ways in which different legal systems enable applying for procedural powers * Recognize particular considerations relating to requesting procedural or investigative measures relating to electronic evidence * Understand some of the considerations and safeguards that should be kept in mind when requesting procedural powers | | |
| **Trainer Guidance**  Many jurisdictions require law enforcement officers, prosecutors or other persons concerned with conducting investigations into criminal offences to request a judicial or other competent authority seeking authorisation to exercise procedural powers. The trainer is required to explain that some jurisdictions require written applications whereas others require verbal requests seeking authorisation to undertake procedural or investigative measures. The trainer should also ensure that this lesson be delivered keeping in mind conditions and safeguards relating to Article 15 of the Budapest Convention. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 8 | These slides provide a recap of certain key aspects of the Budapest Convention that are relevant to the lesson. They include a list of the various procedural powers under the Budapest Convention. The trainer should also use these slides to refresh key concepts under Article 15 of the Budapest Convention. The trainer should also distinguish between the processes for seeking authorization to exercise procedural powers in different legal systems. This part also provides a brief introduction to Part 2, 3 & 4 of the session – the “what”, “how” and “why” of requests for exercise of procedural powers. | |
| 9 to 22 | These slides relate to the “what” of requests for exercise of procedural powers. They cover both the aspect of subject data and subject persons in relation to a request for exercise of procedural power. The slides refer to the investigation exercise case study to provide examples of how subject persons and subject data are identified. | |
| 23 to 49 | These slides relate to the “how” of requests for exercise of procedural powers. They explain how procedural powers are meant to be applied. In doing so, they cover both technical aspects of how procedural powers are to be applied (i.e. which procedural powers will be exercised in relation to different investigations, and what technical measures will be taken to exercise such powers), as well as protective aspects of how procedural powers are to be applied (i.e. conditions and safeguards at the request stage, at execution stage and post-execution stage). The slides refer back to the investigation exercise case study to provide examples of technical and protective measures. | |
| 50 to 61 | These slides relate to the “why” of requests for exercise of procedural powers. This part of the session is focussed on explaining the grounds for exercise of procedural powers. The slides refer to the investigation exercise case study to provide examples of grounds that may be stated and further elaborated in a request. | |
| 62 to 64 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |

Lesson 2.3.4 (Conducting Hearings and Drafting Orders)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.5 (Conducting Hearings and Drafting Orders) | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The purpose of this lesson is to provide delegates with the necessary guidance to assist them in conducting hearings on applications for exercise of procedural powers and draft orders enabling exercise of such powers. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Recognize various considerations with respect to conducting hearings on investigative powers * Explain relevant conditions and procedural safeguards that should be considered when conducting hearings * Identify important judicial skills that may be implemented to effectively conduct hearings * Understand key considerations with respect to orders enabling exercise of electronic evidence procedural powers | | |
| **Trainer Guidance**  Budapest Convention mandates states to implement adequate conditions and safeguards in regard to the exercise of procedural powers. Some jurisdictions require a law enforcement agent or a prosecutor to prepare a formal application and for an independent officer (usually judicial officer) to conduct a hearing of the application and prepare an appropriate order. Other jurisdictions require an independent officer (usually a judicial officer) to consider a request to apply procedural powers and issue a verbal authorization. This lesson aims to provide the necessary general skills to the delegates to hear such applications and draft orders. This lesson should be delivered keeping in mind that the delegates will undertake a practical exercise to involving conducting a hearing. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 7 | These slides provide a brief introduction to hearings including a brief description of how certain legal systems require hearings on applications for procedural powers while others may involve judges rendering authorizations without hearings. This part also recaps an overview of applicable conditions and safeguards. | |
| 8 to 25 | These slides relate to the entire hearing process from the preparation stage to the stage of asking questions and requesting further information. The trainer should explain the stages of a hearing (e.g. preparation, presentation, identification of issues, evidence, questioning and further information) to the participants. The slides refer back to the investigation exercise case study to provide relevant examples. | |
| 26 to 47 | These slides cover skills that are relevant to the process of conducting hearings. Given the sensitivity of this topic, the trainer should ensure that the participants are made aware that this part of the session is based upon existing best practice judicial skills identified by judges in the UK, but adapted appropriately to the specific nature of applications involving electronic evidence. This part also includes some practical examples of implementation of some judicial skills with respect to the investigation exercise case study. | |
| 48 to 72 | These slides relate to drafting of orders after completion of the hearing process. The slides build upon concepts covered during the hearing stage and specify various details that may be included in the order. The trainer should explain that the slides only provide certain non-specific heads of terms and examples, but that the content of any order relating to the exercise of procedural powers would depend entirely on the facts of the case at hand. | |
| 73 to 75 | The trainer should recap the session objectives with the delegates and give them an opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  After completion of the lesson, the delegates are expected to take part in a mock hearing. The delegates will be divided into small groups of even numbers of people. Each group will be provided with a mock application for search and seizure of computer data and will be divided into two sub-groups (e.g. law enforcement officials/prosecutors & judges). Each sub-group will conduct a mock hearing of the application, following which the sub-group of judges will be required to draft an order. After completion of this exercise, the sub-groups will switch roles and the exercise will be repeated.  Upon completion of the exercise, the trainer will be responsible for providing feedback to the delegates. The trainer will provide feedback as follows:   * Headline: Identify the features to be addressed * Playback: Re-enact the subject matter of the headline * Reason: Provide rationale based on which the headline was identified * Remedy: Explain how performance can be improved * Demonstration: Perform the remedy * Replay: Ask to repeat the headlined feature of performance | | |
| **Assessment/Knowledge Check**  The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. The knowledge of the delegates will be assessed in the practical exercise. | | |

Lesson 2.3.4 (Requesting Procedural Powers)

|  |  |  |
| --- | --- | --- |
| Lesson 2.3.5 (Requesting Procedural Powers) | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The purpose of this lesson is to provide delegates with guidelines on applying for investigative or procedural powers corresponding to the Budapest Convention. This lesson will also provide information on what judicial officers or other competent authorities should expect from law enforcement or prosecutors applying for procedural powers. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Understand ways in which different legal systems enable applying for procedural powers * Recognize particular considerations relating to requesting procedural or investigative measures relating to electronic evidence * Understand some of the considerations and safeguards that should be kept in mind when requesting procedural powers | | |
| **Trainer Guidance**  Many jurisdictions require law enforcement officers, prosecutors or other persons concerned with conducting investigations into criminal offences to request a judicial or other competent authority seeking authorisation to exercise procedural powers. The trainer is required to explain that some jurisdictions require written applications whereas others require verbal requests seeking authorisation to undertake procedural or investigative measures. The trainer should also ensure that this lesson be delivered keeping in mind conditions and safeguards relating to Article 15 of the Budapest Convention. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 8 | These slides provide a recap of certain key aspects of the Budapest Convention that are relevant to the lesson. They include a list of the various procedural powers under the Budapest Convention. The trainer should also use these slides to refresh key concepts under Article 15 of the Budapest Convention. The trainer should also distinguish between the processes for seeking authorization to exercise procedural powers in different legal systems. This part also provides a brief introduction to Part 2, 3 & 4 of the session – the “what”, “how” and “why” of requests for exercise of procedural powers. | |
| 9 to 22 | These slides relate to the “what” of requests for exercise of procedural powers. They cover both the aspect of subject data and subject persons in relation to a request for exercise of procedural power. The slides refer to the investigation exercise case study to provide examples of how subject persons and subject data are identified. | |
| 23 to 49 | These slides relate to the “how” of requests for exercise of procedural powers. They explain how procedural powers are meant to be applied. In doing so, they cover both technical aspects of how procedural powers are to be applied (i.e. which procedural powers will be exercised in relation to different investigations, and what technical measures will be taken to exercise such powers), as well as protective aspects of how procedural powers are to be applied (i.e. conditions and safeguards at the request stage, at execution stage and post-execution stage). The slides refer back to the investigation exercise case study to provide examples of technical and protective measures. | |
| 50 to 61 | These slides relate to the “why” of requests for exercise of procedural powers. This part of the session is focussed on explaining the grounds for exercise of procedural powers. The slides refer to the investigation exercise case study to provide examples of grounds that may be stated and further elaborated in a request. | |
| 62 to 64 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  No practical exercises are envisaged in this lesson. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. | | |

Lesson 2.4.2 (Feedback on Hearing Exercise)

|  |  |  |
| --- | --- | --- |
| Lesson 2.4.2 (Feedback on Hearing Exercise) | | Duration: 90 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The purpose of this lesson is to teach trainers how to review and provide feedback to participants on their performance in the exercise related to hearing of an application for exercise of investigative measures. | | |
| **Objectives:**  By the end of the lesson the delegates will be able to:   * Understand how to evaluate and review performance of delegates in exercise on conducting hearings/considering requests for investigative measures * Understand how to implement each of the six stages of the Review Process when giving feedback to participants | | |
| **Trainer Guidance**  The participants of the advanced judicial training course will undertake an exercise involving conducting a hearing of an application for exercise of investigative measures. Clear feedback and a review of performance is critical to the success of any such exercise. This module explains a best practice method to review the performance of the participants. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 3 to 5 | These slides provide an introduction to the feedback process that trainers should use following completion of the hearing exercise. The slides divide the review process into two legs (Feedback & Feedforward) and also list the six stages of the review process that are dealt with in more detail in the subsequent slides. | |
| 6 to 9 | These slides relate to the first leg of the review process which relate to providing feedback to the participants. Feedback involves reflecting back on the performance of the participants. This leg includes the “Headline”, “Playback” and “Reason” stages. The trainer is required to cover each of these stages. | |
| 10 to 15 | These slides relate to the second leg of the review process which relate to providing feedforward to the participants. Feedforward involves looking forward on how to address aspects of the performance of the participants that have been identified in the feedback. This leg includes the “Remedy”, “Demonstration” and “Replay” stages. The trainer is required to cover each of these stages. | |
| **Practical Exercises**  This module has been developed to provide training to trainers on how to provide feedback to trainees after a hearing exercise. Trainers will be required to practically conduct the review process after the hearing exercise of a particular training. | | |
| **Assessment/Knowledge Check**  The trainer is encouraged to check knowledge and understanding by asking relevant questions throughout the session. No formal assessment is required for this lesson. | | |

6. Evaluation

Evaluation is an important part of a training course and should be accorded the time it requires for delegates to provide considered feedback on their learning experience.

This course has been developed as a generic course and as such much of the teaching materials are PowerPoint based and without the level of practical exercises that may normally be associated with this type of course.

An evaluation from has been prepared and is provided as a template to be adapted to local conditions. Trainers are responsible for ensuring that the forms are completed and returned to the relevant national body in order that improvements may be made for further delivery of the course.

7. Assessment

No assessment has been requested for this course, however those delivering the materials in the future, especially those in countries where the course may be part of a programme that is assessed may reconsider this. If assessment is introduced, the methodologies in that country should be used.

1. The European Union/Council of Europe Joint Project CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime) is aimed at strengthening the capacities of criminal justice authorities of Western Balkans and Turkey to cooperate effectively against cybercrime. [↑](#footnote-ref-1)
2. \*This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence. [↑](#footnote-ref-2)