**INTRODUCTORY TRAINING COURSE FOR JUDGES AND PROSECUTORS**

1. **INTRODUCTORY TRAINING COURSE OUTLINE PROPOSAL**

This Introductory Training Course is an important and necessary course as it gives the very foundation of knowledge for judges, magistrates and prosecutors on Cybercrime. It must be able to give participants a good grasp on the basic concepts on cybercrime and other related topics. This course, more than anything, should provide a solid base for future courses such as the Advanced Course and other specialized courses. Just to reiterate this introductory course must serve as the building blocks for future trainings.

The 3 and ½ day Introductory Training Course on Cybercrime for Judges, Magistrates and Prosecutors as the name suggests should be a course where the bare essentials of subjects, concepts and topics relating to cybercrime are presented to the participants. The course should at onset titillate the minds of the participants and jump start their interest. This includes an introduction to cybercrime concepts and, if possible, the explanation of terminologies which is crucial in understanding and comprehending the provisions of the Budapest Convention, local legislation and concepts relating to Digital Evidence and International Cooperation.

The session on Public Private partnership is not included as it can be briefly discussed in the Introduction to International Cooperation

**1st DAY**

**9:00 1.OPENING REMARKS / WELCOME MESSAGES (30mins)**

Delivered by the following:

EU Delegation

Council of Europe – Project Manager

Local/National Authorities

**9:30 2. CAPACITY BUILDING ON CYBERCRIME BY THE COE (30 mins)**

***Delivered by CoE – Project Manager***

A session to inform participants of the efforts of CoE in capacity building on cybercrime thru its several projects such as the Glacy +

**10:00 3. INTRODUCTION TO THE COURSE AND LEVELLING-OFF**

**( 30 mins )**

***Delivered by CoE Expert***

Introduction and Levelling-off serves to present to the participants the objectives of the training and elicit their expectations as well as their concerns in handling cases involving cybercrime offenses.

The main goal of this session is to familiarize participants with the general overview of the course as well as its goals and objectives. Ground rules are also presented to the participants for a smooth flow of training

This is a perfect time to break the ice with the participants. Maybe let them briefly share their insights and some apprehensions on the training.

The trainer in this session is supposed to “sell” the training so that participants’ interest is captured right at the start.

**10:30 Coffee break**

**11:00 4. PRE-SURVEY AND QUESTION FORM**

**( 30 mins )**

A Question form is given to participants in order for them to have the opportunity to write their questions and concerns which will be answered by the experts later on in the course. This goes hand in hand with the Pre-survey which comes in the form of a pre-test (timed at 10 mins.) which gives the trainers an overview of how far the knowledge of participants go and give trainers an idea of how they would deliver their given topic.

A sample pre-test which we use in cyber warrants training is herein attached.

**11:30 5. INTERNET BASICS FOR JUDGES AND PROSECUTORS,**

**( 1.5 hr )**

***Delivered by CoE Expert or Local Trainer***

This session gives participants the information on the basics of the computer and the internet. Like an intro to tech session but stripped down to its basic points

Topics dealing with

1. Refresher on computer parts and functions
2. The internet and how it came to be
3. How the internet works and functions
4. Internet services and applications

Other topics may be added

Visual aids or videos may be presented to better explain and illustrate how the internet functions.

Interesting facts and statistics may be presented to the participants at the start of the session like global usage of internet and mobile phones and how it has impacted the world. Just so it may kick-off the discussion and draw their interest on the topic

**1:00 LUNCH BREAK**

**2:00 6. CYBERCRIME BASICS (An Introduction to Cybercrime)**

( 1.5 hr. )

The topic presents an overview of cybercrime.

At the end of the session, participants are expected to familiarize themselves with

1. Cybercrime, its basic concept
2. Terminologies that participants will encounter during the course like the different kinds of data *(Traffic, Content and Subscriber Information)*, computer system and network, service provider, etc. as it will find relevance in the course of the training and other future courses
3. Types of cybercrime and their global impact
4. Prevalent threats and challenges

In this session discussion on concrete cases that has impacted the world can be discussed so as to get the interest of the participants.

Regional cases if there are, are good examples to give as well. This is also a good opportunity to get the feel on what the cybercrime situation is in the particular country or region where the training is held.

Practical examples as well may prove to be helpful for better understanding

It is also encouraged that videos be presented on globally talked about cybercrime that has put several sectors of society of even governments at risk.

Statistics may be presented on the prevalent cybercrimes impacting the world such as its impact to global economy and security.

**3:30 COFFEE BREAK**

**4:00 7. THE BUDAPEST CONVENTION AN OVERVIEW**

**( 45 mins. )**

***Delivered by CoE Expert***

A short session of 45 mins to give participants a briefer of what the treaty is all about, the member states and efforts of countries who want to accede.

Will be discussed as well will be the treaties’ components such as the substantive, procedural and international cooperation aspect…**this can also be integrated in the cybercrime basics and not treated as a separate session.**

**4:45 END OF DAY 1**

**2nd DAY**

**9:00 8. OVERVIEW OF DIGITAL/ELECTRONIC EVIDENCE**

**( 1.5 hr )**

***Delivered by CoE Expert***

The goal is for participants to identify

1. what constitutes electronic evidence
2. types of electronic evidence
3. sources and
4. characteristics.

A distinction on the difference between physical and electronic evidence may be discussed.

This session would deal with the basic concepts such as hash values, preserving RAM, finding deleted files, etc.

**Videos** illustrating these concepts is also good to incorporate.

**Practical exercises** may be done, like generating a hash value which would be interesting to participants as one of them can be asked to do the demonstration.

An exercise presenting an illustration or picture of a crime scene where participants will be asked to identify potential electronic evidence may be done for the session to be interactive.

Introduction as to the contents of the CoE electronic evidence guide is proper at this time as primer for the electronic evidence course.

Basic concepts on admissibility may be inserted

Statistics may also be presented relating to how many people use computers and how many hours they spend per day. This is relevant in emphasizing that there are tons of electronic evidence that are stored and can be gathered or taken from one’s own electronic device.

This is not an in depth session as there will be a separate course on electronic evidence

**10:30 COFFEE BREAK**

**11:00 9. SUBSTANTIVE PROVISIONS OF THE BUDAPEST CONVENTION**

**( 1.5 hr )**

***Delivered by a CoE Expert***

Part 1 – Offenses against the Confidentiality, Integrity and Availability of Computer data

This section covers the substantive offences provisions under Chapter II, Section 1 Title 1 of the Budapest Convention.

Offences against the confidentiality, integrity and availability of computer data and systems

a. Illegal access (Article 2)

b. Illegal interception (Article 3)

c. Data interference (Article 4)

d. System interference (Article 5)

e. Misuse of devices (Article 6)

Each offence and its elements must be discussed and explained to participants.

It is good to integrate in the discussion some examples and actual cases for better understanding. Regional case examples are preferred so the participants can relate more.

We can also allow some interaction with the audience by giving them the opportunity to share some experience they may have on the topic.

**12:30 LUNCH BREAK**

**1:30 10. SUBSTANTIVE PROVISIONS OF THE BUDAPEST CONVENTION**

**( 1.5 hr )**

***Delivered by CoE Expert***

Part 2 – Content and Computer Related Offenses

This section covers the substantive offences provisions under Chapter II, Section 1 Titles 2, 3 and 4 of the Budapest Convention

Computer-related offences (Title 2)

a. Computer-related forgery (Article 7)

b. Computer-related fraud (Article 8)

Content-related offences (Title 3)

a. Offences related to child pornography (Article 9)

Offences related to infringements of copyright and related rights (Title 4)

a. Offences related to infringements of copyright and related rights (Article 10)

Each offence and its elements must be discussed and explained to participants.

It is good to integrate in the discussion some examples and actual cases for better understanding. Regional case examples are preferred so the participants can relate more.

We can also allow some interaction with the audience by giving them the opportunity to share some experience they may have on the topic.

**3:00 COFFEE BREAK**

**3:30 11. PROCEDURAL POWERS UNDER THE BUDAPEST CONVENTION**

**( 1.5 hr )**

***Delivered by CoE Expert***

Part 1 – Scope, Conditions and safeguards

Preservation and Production orders

This covers the procedural law provisions under Chapter II, Section 2 Titles 1, 2 and 3 of the Budapest Convention

The following topics will be discussed in this session:

1. Scope of procedural powers (Article 14)
2. Conditions and safeguards (Article 15)
3. Expedited preservation of stored computer data (Article 16)
4. Expedited preservation and partial disclosure of preserved traffic data (Article 17)
5. Production order (Article 18)

Key concepts and elements of each procedural power must be discussed and explained to participants.

Case examples may be given to further amplify and explain the concepts that may be new to some if not most of the participants. This would increase their understanding on the concepts

If there are regional and local cases that would be preferred as participants would relate more.

**5:00 END OF DAY 2**

**3RD DAY**

**9:00 12. PROCEDURAL POWERS UNDER THE BUDAPEST CONVENTION**

**( 1.5 hr )**

***Delivered by CoE Expert***

Part 2 – Search and seizure, real-time collection, interception

This covers the procedural law provisions under Chapter II, Section 2 Titles 4 and 5 of the Budapest Convention

a. Search and seizure of stored computer data (Article 19)

b. Real-time collection of traffic data (Article 20)

c. Interception of content data (Article 21)

In this session, the topic of jurisdiction under Section 3 Article 22 may also be discussed as it affects the procedural powers.

Case examples may be given to further amplify and explain the concepts that may be new to some if not most of the participants. This would increase their understanding on the concepts. Again local/regional scenarios are preferred as participants can relate more.

**10:30 COFFEE BREAK**

**11:00 13. BASIC CONCEPTS ON INTERNATIONAL COOPERATION**

**( 1.5 hr )**

***Delivered by CoE Expert***

This session gives the participants an overview of the basic concepts and principles of international cooperation.

The session can start with emphasizing anew the global dimension of cybercrime and its cross-border nature thus necessitating international cooperation.

Mechanisms on how international cooperation is carried out can be outlined together with an overview of MLA can be discussed as a tool for cooperation.

Discussion on various organizations, agencies and treaties that enable and facilitate international cooperation between states and their response mechanism can be discussed here.

A run thru on the articles on the Convention relating to International Cooperation

a. Spontaneous information (Article 26)

b. Expedited preservation of stored computer data (Article 29)

c. Expedited disclosure of preserved traffic data (Article 30)

d. Mutual assistance regarding accessing of stored computer data (Article 31)

e. Transborder access to stored computer data with consent or where publicly available (Article 32)

f. Mutual assistance regarding real time collection of traffic data (Article 33)

g. Mutual assistance regarding interception of content data (Article 34)

h. 24/7 Network (Article 35)

No in depth discussion should be made here as there is a specialized course on International Cooperation.

The concept of Public-Private Partnership can be introduced here and present its interplay with International cooperation. NO in depth discussion as a full session on Public-Private partnership can be included in the International Cooperation course.

**12:30 LUNCH BREAK**

**1:15 14. OVERVIEW OF CYBERCRIME INVESTIGATION (Govt agencies and law enforcement )**

**( 1 hr )**

***Delivered by local LEA and/or CoE EXPERT***

This session gives participants a briefer or general idea how law enforcement authorities do their work and what agencies of government are crucial in the investigation of cybercrime.

The session may be delivered by a representative from Local Law Enforcement giving the participants an outline or overview of how cybercrime investigation is conducted.

This can give the participants working knowledge on how a case prior to being filed in court, is investigated. This would include the process of case-build up, surveillance and how they eventually come to a conclusion that a case is ripe to be filed in court.

This knowledge is useful and handy for a magistrate, judge or prosecutor as they would know how evidence was gathered which would aid them during trial especially when asking questions to a witness. This would be helpful as well in the appreciation of pieces of evidence brought before them.

This session can also be given hand in hand with a CoE Expert who can share best practices done all over the world relating to cybercrime investigation.

**2:15 15. CYBERCRIME LEGISLATION (NATIONAL LEGISLATION)**

**( 1.5 hr )**

***Delivered by a Local Expert***

This session is where the local legislation on cybercrime is discussed and presented by a representative of the concerned country.

An overview of the cybercrime law and related laws of the country are discussed and parallel comparison with the Convention can be made.

An update on efforts done by the country to strengthen its laws in the fight. Against cybercrime can also be discussed here.

**3:45 COFFEE BREAK**

**4:00 16. SKILLS BUILDING IN CYBERCRIME**

**(1 hr)**

***Faciliated by a COE Expert***

Participants will be divided into maybe 3-4 groups. Each group will be given a case scenario where they are to answer questions relating to the topics discussed during the course. This serves to gauge their learning as well. This will take 1 hour

**5:00 END OF DAY 3**

**4th DAY**

**9:00 17. POST-SURVEY**

This post-test (same test given during the pre-test) is given to gauge whether participants understood the topics delivered. This will also take 10 minutes

**9:20 18. GROUP REPORTING**

***Facilitated by a COE Expert***

Each group will then report what they have discussed during the group discussion. They are to appoint a rapporteur to deliver the report.

The experts will be the panelists who will comment and critique on the answers given.

**10:30 COFFEE BREAK**

**11:00 19. OPEN FORUM (feedback mechanism)**

***Facilitated by a COE Expert***

In this session, the experts will answer the questions earlier propounded by the participants in the Question Form given. This session serves to clarify vague matters and further strengthen the knowledge and understanding of the participants relating to cybercrime.

**12:00 20. PRESENTATION OF POST-SURVEY RESULTS**

***Presented by COE Expert***

The results of the post-test will be announced vis-à-vis the pre-test to determine improvement.

**12:30 21. CLOSING REMARKS (20 mins)**

***Delivered by Project Manager of COE***

***Local Representative/Authorities***

This session should be flexible to how the local organizers would want it to be. This would involve delivery of closing remark and words of thanks from COE and the local organizer.

The manner or how the distribution of Certificates will be will depend on how locally the organizer does it. They can just be handed to the participants or a form of “graduation” ceremony may be made but should be kept short.

COE Experts must also remind participants in this session of filling up and evaluation form or feedback form on how the training went.

**1:00 END OF TRAINING**

Participants must be reminded of the evaluation form/feedback form.