**COURS INTRODUCTIF DE FORMATION POUR LES JUGES ET LES PROCUREURS**

**I. PROPOSITION DE PLAN DE COURS INTRODUCTIF DE FORMATION**

Cette formation introductive est un cours important et nécessaire car c'est le fondement même du savoir des juges, magistrats et procureurs sur la cybercriminalité. Ce cours doit permettre aux participants de bien saisir les concepts de base sur la cybercriminalité et autres sujets connexes. Ce cours devrait, plus que tout, constituer une base solide pour les futurs cours tels que le cours avancé et d'autres cours spécialisés. Pour rappel, ce cours introductif doit être la base des formations futures.

Comme son nom l'indique, le cours introductif de formation de 3 jours et ½ sur la cybercriminalité pour les juges, les magistrats et les procureurs, devrait être un cours où l'essentiel des sujets, concepts et thèmes relatifs à la cybercriminalité est présenté aux participants. Le cours devrait dès le début titiller l'esprit des participants et éveiller leur intérêt. Cela comprend une introduction aux concepts de la cybercriminalité et, si possible, l'explication de terminologies qui est cruciale pour comprendre et assimiler les dispositions de la Convention de Budapest, la législation locale et les concepts relatifs à la preuve numérique et à la coopération internationale.

La session sur le partenariat public-privé n'est pas incluse car elle peut être brièvement abordée dans l'introduction à la coopération internationale

**1er jour**

**9:00 1. ALLOCUTIONS D'OUVERTURE / MESSAGES DE BIENVENUE (30mins)**

Prononcés par :

La délégation de l'UE

Le Conseil de l'Europe - Chef de projet

Les autorités locales/nationales

**9:30 2. RENFORCEMENT DES CAPACITÉS SUR LA CYBERCRIMINALITÉ par le CdE (Conseil de l'Europe) (30 minutes)**

Animé par le Chef de projet

Une session pour informer les participants des efforts déployés par le Conseil de l'Europe pour renforcer les capacités en matière de cybercriminalité par le biais de ses différents projets, tels que le projet Glacy +

**10:00 3. INTRODUCTION AU COURS ET REMISE À NIVEAU**

**(30 minutes)**

***Présenté par un expert du CdE***

L'introduction et la remise à niveau servent à présenter aux participants les objectifs de la formation et à élucider leurs attentes ainsi que leurs préoccupations en ce qui concerne le traitement des affaires impliquant des délits de cybercriminalité.

Le but principal de cette session est de familiariser les participants avec les grandes lignes du cours ainsi que ses buts et objectifs. Les règles de base sont également présentées aux participants pour un déroulement harmonieux de la formation

C'est le moment idéal pour briser la glace, par exemple en laissant les participants partager brièvement leurs points de vue et quelques appréhensions sur la formation.

Pendant cette session, le formateur est censé être convaincant et susciter l'intérêt des participants dès le début de la formation.

**10:30 Pause café**

**11:00 4. PRE-ENQUETE ET QUESTIONNAIRE (30 minutes)**

Un formulaire est remis aux participants afin qu'ils puissent rédiger leurs questions et préoccupations, auxquelles les experts répondront plus tard dans le cours. Cela va de pair avec la pré-enquête qui se présente sous la forme d'un pré-test (chronométré à 10 minutes) qui donne aux formateurs un aperçu de l'étendue des connaissances des participants et leur donne une idée de la manière dont ils traiteraient le sujet donné.

Un exemple de pré-test que nous utilisons dans la formation sur les mandats électroniques est ci-joint.

**11:30 5. LES FONDAMENTAUX DE L'INTERNET POUR LES JUGES ET LES PROCUREURS, (1,5 h)**

Présenté par un expert du CdE ou un formateur local

Cette session donne aux participants des informations sur les notions de base de l'ordinateur et de l'internet. Telle une session d'introduction à la technologie, mais réduite à ses points essentiels

Sujets traitant de

a. Révision sur les composantes et les fonctions de l'ordinateur

b. L'internet et son évolution

c. Comment fonctionne l'internet

d. Services et applications Internet

D'autres sujets peuvent être ajoutés

Des supports visuels ou des vidéos peuvent être présentés pour mieux expliquer et illustrer le fonctionnement de l'internet.

Afin de lancer la discussion et susciter l'intérêt des participants pour le sujet, des faits et statistiques intéressants peuvent leur être présentés au début de la session, comme par exemple l'utilisation globale de l'internet et des téléphones portables et son impact sur le monde.

**1:00 PAUSE DEJEUNER**

**2:00 6. Notions de base de la cybercriminalité (Une introduction à la cybercriminalité)**

**(1,5 h)**

Le topic présente un aperçu de la cybercriminalité.

À la fin de la session, les participants sont censés se familiariser avec

a. La cybercriminalité : concept de base

b. Les terminologies que les participants rencontreront pendant le cours telles que les différents types de données (trafic, contenu et informations sur les abonnés), système et réseau informatiques, fournisseur de services, etc.

c. Les différentes formes de cybercriminalité et leur impact mondial

d. Les menaces et les défis actuels

Au cours de cette session, on peut discuter de cas concrets qui ont eu un impact sur le monde afin de stimuler l'intérêt des participants.

Les cas régionaux, s'il y en a, sont également de bons exemples à donner. C'est également une bonne occasion de se faire une idée de la situation de la cybercriminalité dans le pays ou la région où se tient la formation.

Des exemples pratiques peuvent aussi s'avérer utiles pour mieux comprendre

Il est également encouragé que soient présentées des vidéos sur la cybercriminalité dont on parle dans le monde entier et qui a mis en danger plusieurs secteurs de la société, voire même des gouvernements.

Des statistiques peuvent être présentées sur les cyber crimes les plus néfastes dans le monde, et leurs répercussions sur l'économie et la sécurité mondiales.

**3:30 PAUSE CAFÉ**

**4:00 7. LA CONVENTION DE BUDAPEST : UN APERÇU (45 minutes)**

**Présenté par un expert du Conseil de l'Europe**

Une courte session de 45 minutes pour donner aux participants un aperçu de la signification du traité, des États membres et des démarches des pays qui veulent y adhérer.

Seront également abordés les éléments du traité tels que le fond, la procédure et la coopération internationale... **Ce sujet peut également être intégré dans la session sur les notions de base de la cybercriminalité et ne pas être traité comme une session séparée.**

**4:45 FIN DE LA PREMIÈRE JOURNÉE**

**2eme JOUR**

**9:00 8. APERÇU GÉNÉRAL DES ÉLÉMENTS DE PREUVE NUMÉRIQUES/ÉLECTRONIQUES (1,5 h)**

Présenté par un expert du Conseil de l'Europe

L'objectif est que les participants identifient

a. ce qui constitue une preuve électronique

b. types de preuves électroniques

c. sources et

d. les caractéristiques.

Une discussion sur la différence entre les preuves physiques et électroniques peut être menée.

Cette session traiterait des concepts de base tels que les valeurs de hachage, la préservation de la mémoire vive, la recherche de fichiers supprimés, etc.

Des vidéos illustrant ces concepts sont également bonnes à intégrer.

Des exercices pratiques peuvent être effectués, comme la génération d'une valeur de hachage qui serait intéressante pour les participants car l'un d'entre eux peut être invité à en faire la démonstration.

Un exercice présentant une illustration ou une photo d'une scène de crime où les participants seront invités à identifier des preuves électroniques potentielles peut être fait pour que la session soit interactive.

Une introduction au contenu du guide des preuves électroniques du Conseil de l'Europe est appropriée à ce stade en tant qu'introduction au cours sur les preuves électroniques.

Des concepts de base sur les critères de recevabilité des preuves peuvent être insérés

Des statistiques peuvent également être présentées concernant le nombre de personnes qui utilisent un ordinateur et le nombre d'heures qu'elles y passent par jour. Ceci est pertinent pour souligner qu'il existe des tonnes de preuves électroniques qui sont stockées et qui peuvent être recueillies ou extraites de son propre appareil électronique.

Il ne s'agit pas d'une session approfondie car il y aura un cours séparé sur les preuves électroniques

**10:30 PAUSE CAFÉ**

**11:00 9. LES DISPOSITIONS DE FOND DE LA CONVENTION DE BUDAPEST (1,5h)**

**Présenté par un expert du Conseil de l'Europe**

**Partie 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données informatiques**

Cette section couvre les dispositions relatives aux infractions matérielles du chapitre II, section 1, titre 1, de la convention de Budapest.

Infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques

a. Accès illégal (article 2)

b. Interception illégale (article 3)

c. Interférence dans les données (article 4)

d. Interférences avec le système (article 5)

e. Utilisation abusive de dispositifs (article 6)

Chaque infraction et ses éléments doivent être discutés et expliqués aux participants.

Il est bon d'intégrer dans la discussion quelques exemples et cas réels pour une meilleure compréhension. Des exemples de cas régionaux sont préférables pour que les participants puissent mieux se faire une idée.

Nous pouvons également permettre une certaine interaction avec le public en lui donnant l'occasion de partager une certaine expérience qu'il peut avoir du sujet.

**12:30 PAUSE DEJEUNER**

**1:30 10. LES DISPOSITIONS DE FOND DE LA CONVENTION DE BUDAPEST**

**(1,5 h)**

**Présenté par un expert du Conseil de l'Europe**

**Partie 2 - Contenu et infractions informatiques**

La présente section couvre les dispositions relatives aux infractions substantielles prévues au chapitre II, section 1, titres 2, 3 et 4 de la convention de Budapest

Infractions informatiques (titre 2)

a. Falsification informatique (article 7)

b. Fraude informatique (article 8)

Infractions liées au contenu (titre 3)

1. Infractions liées à la pornographie enfantine (article 9)

Infractions liées aux violations des droits d'auteur et des droits voisins (titre 4)

a. Infractions liées aux violations des droits d'auteur et des droits connexes (article 10)

Chaque infraction et ses éléments doivent être discutés et expliqués aux participants.

Il est bon d'intégrer dans la discussion quelques exemples et cas réels pour une meilleure compréhension. Des exemples de cas régionaux sont préférables pour que les participants puissent mieux se faire une idée.

Nous pouvons également permettre une certaine interaction avec le public en lui donnant l'occasion de partager une certaine expérience qu'il peut avoir du sujet.

**3:00 PAUSE CAFÉ**

**3:30 11. POUVOIRS PROCÉDURAUX EN VERTU DE LA CONVENTION DE BUDAPEST (1,5 h)**

**Présenté par un expert du Conseil de l'Europe**

**Partie 1 - Champ d'application, conditions et garanties**

Ordres de conservation et de production

Il s'agit des dispositions de droit procédural du chapitre II, section 2, titres 1, 2 et 3 de la convention de Budapest

Les sujets suivants seront abordés lors de cette session :

a. Portée des pouvoirs de procédure (article 14)

b. Conditions et sauvegardes (article 15)

c. Conservation accélérée des données informatiques stockées (article 16)

d. Conservation accélérée et divulgation partielle des données relatives au trafic conservées (article 17)

e. Ordre de production (article 18)

Les concepts et éléments clés de chaque pouvoir procédural doivent être discutés et expliqués aux participants.

Des exemples de cas peuvent être donnés afin d'amplifier et d'expliquer davantage les concepts qui peuvent être nouveaux pour certains, voire pour la plupart des participants. Cela permettrait d'améliorer leur compréhension des concepts

S'ils existent, les cas régionaux et locaux seraient préférables car les participants s'y retrouveraient davantage.

**5:00 FIN DE LA 2eme JOURNÉE**

**3eme JOUR**

**9:00 12. POUVOIRS PROCÉDURAUX EN VERTU DE LA CONVENTION DE BUDAPEST (1,5 h)**

**Présenté par un expert du Conseil de l'Europe**

**Partie 2 - Perquisition et saisie, collecte en temps réel, interception**

Il s'agit des dispositions de droit procédural du chapitre II, section 2, titres 4 et 5 de la convention de Budapest

a. Perquisition et saisie de données informatiques stockées (article 19)

b. Collecte en temps réel des données relatives au trafic (article 20)

c. Interception des données relatives au contenu (article 21)

Au cours de cette session, le sujet de la compétence en vertu de la section 3 de l'article 22 peut également être discuté car il affecte les pouvoirs de procédure.

Des exemples de cas peuvent être donnés afin d'amplifier et d'expliquer les concepts qui peuvent être nouveaux pour certains, voire pour la plupart des participants. Cela permettrait d'améliorer leur compréhension des concepts. Là encore, des scénarios locaux/régionaux sont préférables, car les participants peuvent s'y retrouver plus facilement.

**10:30 PAUSE CAFÉ**

**11:00 13. CONCEPTS DE BASE SUR LA COOPÉRATION INTERNATIONALE (1,5 h)**

**Présenté par un expert du Conseil de l'Europe**

Cette session donne aux participants un aperçu des concepts et principes de base de la coopération internationale.

La session peut commencer par souligner à nouveau la dimension mondiale de la cybercriminalité et sa nature transfrontalière, ce qui nécessite une coopération internationale.

Les mécanismes de mise en œuvre de la coopération internationale peuvent être décrits et un aperçu du MLA peut être discuté en tant qu'outil de coopération.

On peut discuter ici des diverses organisations, agences et traités qui permettent et facilitent la coopération internationale entre les États et de leur mécanisme de réponse.

Un tour d'horizon des articles de la Convention relatifs à la coopération internationale :

a. Informations spontanées (article 26)

b. Conservation accélérée des données informatiques stockées (article 29)

c. Divulgation accélérée de données relatives au trafic conservées (article 30)

d. Assistance mutuelle concernant l'accès aux données informatiques stockées (article 31)

e. Accès transfrontalier à des données informatiques stockées avec le consentement du détenteur ou lorsqu'elles sont accessibles au public (article 32)

f. Assistance mutuelle concernant la collecte en temps réel de données relatives au trafic (article 33)

g. Assistance mutuelle en matière d'interception de données relatives au contenu (article 34)

h. Réseau 24/7 (article 35)

Il n'y a pas lieu d'approfondir ici, car il existe un cours spécialisé sur la coopération internationale.

Le concept de partenariat public-privé peut être introduit ici pour illustrer son interaction avec la coopération internationale. AUCUNE discussion approfondie ne peut être incluse dans le cours sur la coopération internationale car il existe une session complète sur le partenariat public-privé.

**12:30 PAUSE DÉJEUNER**

**1:15 14. VUE D'ENSEMBLE DE L'ENQUÊTE SUR LA CYBERCRIMINALITÉ (Organismes gouvernementaux et services de police) (1 heure)**

Présenté par l'ALE local et/ou l'EXPERT du CdE

Cette session donne aux participants une idée plus succincte ou générale de la manière dont les autorités judiciaires font leur travail et quelles agences gouvernementales sont cruciales dans les enquêtes sur la cybercriminalité.

La session peut être animée par un représentant des services judiciaires locaux qui donne aux participants un aperçu ou une vue d'ensemble de la manière dont les enquêtes sur la cybercriminalité sont menées.

Les participants peuvent ainsi acquérir des connaissances pratiques sur la manière dont une affaire est instruite avant d'être portée devant les tribunaux. Cela comprend le traitement des dossiers, la surveillance et la manière dont ils parviennent à la conclusion qu'une affaire est prête pour être portée devant les tribunaux.

Ces connaissances sont utiles et pratiques pour un magistrat, un juge ou un procureur car ils sauront comment les preuves ont été recueillies, ce qui les aidera pendant le procès, notamment lorsqu'ils poseront des questions à un témoin. Cela les aiderait également à apprécier les éléments de preuve qui leur sont présentés.

Cette session peut également être animée conjointement avec un expert du Conseil de l'Europe qui peut partager les meilleures pratiques appliquées dans le monde entier en matière d'enquêtes sur la cybercriminalité.

**2:15 15. LA LÉGISLATION SUR LA CYBERCRIMINALITÉ (LÉGISLATION NATIONALE) (1,5 h)**

Présenté par un expert local

C'est au cours de cette session que la législation locale sur la cybercriminalité est examinée et présentée par un représentant du pays concerné.

Un examen général de la loi sur la cybercriminalité et des lois connexes du pays est présenté et une comparaison parallèle avec la Convention peut être faite.

Une mise à jour des efforts déployés par le pays pour renforcer ses lois en matière de lutte contre la cybercriminalité. La lutte contre la cybercriminalité peut également être abordée ici.

**3:45 PAUSE CAFÉ**

**4:00 16. LE RENFORCEMENT DES CAPACITÉS EN MATIÈRE DE CYBERCRIMINALITÉ (1 heure)**

Avec l'aide d'un expert du Conseil de l'Europe

Les participants seront divisés en 3 ou 4 groupes. Chaque groupe recevra un scénario dans lequel il devra répondre à des questions relatives aux sujets abordés pendant le cours. Cela permet également d'évaluer leur apprentissage. Cette activité prendra 1 heure

**5:00 FIN DE LA TROISIEME JOURNEE**

**4eme JOURNÉE**

**9:00 17. EVALUATION APRÈS-SONDAGE**

Ce post-test (le même que celui effectué lors du pré-test) est donné pour évaluer si les participants ont compris les sujets abordés. Cela prendra également 10 minutes

**9:20 18. RAPPORT DE GROUPE**

Animé par un expert du Conseil de l'Europe

Chaque groupe rendra ensuite compte de ce dont il a discuté au cours de la discussion de groupe. Ils doivent désigner un rapporteur pour présenter le rapport.

Les experts seront les panélistes qui commenteront et critiqueront les réponses données.

**10:30 PAUSE CAFÉ**

**11:00 19. FORUM OUVERT (mécanisme de retour d'information)**

Animé par un expert du Conseil de l'Europe

Au cours de cette session, les experts répondront aux questions proposées par les participants dans le formulaire de questions. Cette session sert à clarifier des questions vagues et à renforcer les connaissances et la compréhension des participants en matière de cybercriminalité.

**12:00 20. PRÉSENTATION DES RÉSULTATS DE L'ENQUÊTE**

Présenté par l'expert du Conseil de l'Europe

Les résultats du post-test seront annoncés par rapport au pré-test afin de mesurer l'amélioration.

**12:30 21. REMARQUES DE CLÔTURE (20 minutes)**

Présenté par le chef de projet du Conseil de l'Europe

Représentants/autorités locales

Cette session devrait être flexible, selon les souhaits des organisateurs locaux. Cela impliquerait la présentation d'un mot de clôture et de remerciements de la part du Conseil de l'Europe et de l'organisateur local.

La manière dont les certificats seront distribués dépendra de la manière dont l'organisateur local le fera. Ils peuvent être simplement remis aux participants ou une forme de cérémonie de "remise des diplômes" peut être organisée, mais elle doit être courte.

Les experts du CdE doivent également rappeler aux participants à cette session de remplir un formulaire d'évaluation ou un formulaire de retour d'information sur le déroulement de la formation.

**1:00 FIN DE LA FORMATION**

Il faut rappeler aux participants de remplir et rendre le formulaire d'évaluation/feedback.