****

**GLACY+**

**Global Action on Cybercrime Extended**

**Action globale sur la cybercriminalité élargie**

|  |  |
| --- | --- |
| [www.coe.int/cybercrime](http://www.coe.int/cybercrime) | Projet de mars 2018 |

**Formation avancée sur la cybercriminalité et les preuves électroniques à destination**

**des juges et des procureurs**

**2018**

**Manuel de formation et kit de ressources**



**Table des matières**

[Introduction 3](#_Toc516009774)

[1. Aperçu général 5](#_Toc516009775)

[1.1 But du cours 5](#_Toc516009776)

[1.2 Pourquoi cette formation est-elle nécessaire ? 5](#_Toc516009777)

[1.3 Programme d’études 6](#_Toc516009778)

[2. Comment utiliser le Guide du formateur ? 7](#_Toc516009779)

[3. Aperçu du cours 9](#_Toc516009780)

[3.1 Combien de temps dure le cours et à qui s’adresse-t-il ? 9](#_Toc516009781)

[3.2 Qui donne le cours ? 9](#_Toc516009782)

[3.3 Comment le cours sera-t-il donné ? 9](#_Toc516009783)

[3.4 Objectifs du cours 9](#_Toc516009784)

[3.5 Groupes cibles de participants et de formateurs 9](#_Toc516009785)

[3.5.1 Participants 9](#_Toc516009786)

[3.5.2 Expérience préalable requise 10](#_Toc516009787)

[3.5.3 Formateurs 10](#_Toc516009788)

[3.5.4 Expérience préalable requise 10](#_Toc516009789)

[3.6 Ressources 10](#_Toc516009790)

[3.6.1 Ressources nécessaires au cours 10](#_Toc516009791)

[3.6.2 Personnalisation des ressources pédagogiques 11](#_Toc516009792)

[3.7 Évaluation 11](#_Toc516009793)

[3.8 Emploi du temps 12](#_Toc516009794)

[3.9 Objectifs du cours et des sessions 15](#_Toc516009795)

[4. Principaux contacts 18](#_Toc516009796)

[5. Plan des sessions 19](#_Toc516009797)

[6. Évaluation 57](#_Toc516009798)

[7. Appréciation 57](#_Toc516009799)

Introduction

Les sociétés du monde entier dépendant de plus en plus des technologies de l’information et de la communication, les juges et les procureurs doivent être en mesure de traiter les affaires relatives à la cybercriminalité et aux preuves électroniques. Si, dans de nombreux pays, les services répressifs ont été en mesure de renforcer leurs capacités en matière d’enquête sur la cybercriminalité et d’obtention de preuves électroniques, il semblerait que ce ne soit pas toujours le cas pour les juges et les procureurs. L’expérience montre que, la plupart du temps, ces derniers éprouvent des difficultés à se confronter aux nouvelles réalités du cyberespace. Il est donc nécessaire de déployer des efforts particuliers pour permettre aux intéressés de mener des poursuites et rendre des jugements dans les cas d’infraction relevant de la cybercriminalité ainsi que d’utiliser les preuves électroniques grâce à l’organisation de formations, la création de réseaux et la mise en place de spécialisations.

Au cours de l’année 2009, le Conseil de l’Europe a élaboré un concept visant à soutenir ces efforts dans le cadre du Projet sur la cybercriminalité, en coopération avec le Réseau de Lisbonne d’organes de formation judiciaire et avec un groupe de travail multipartite.

Le but de ce concept est d’aider les organes de formation judiciaire à mettre au point des programmes portant sur la cybercriminalité et les preuves électroniques à l’intention des juges et des procureurs et à intégrer ces cours à la fois dans les formations initiale et continue.

Les objectifs du concept de formation à l’intention des juges et des procureurs sont les suivants :

* permettre aux organes de formation de dispenser une formation initiale et continue relative à la cybercriminalité sur la base des normes internationales ;
* inculquer au plus grand nombre possible de juges et procureurs, en formation ou en exercice, les connaissances de base relatives à la cybercriminalité et aux preuves électroniques ;
* dispenser une formation avancée à un nombre significatif de juges et de procureurs ;
* soutenir la spécialisation et la formation technique continues des juges et des procureurs ;
* contribuer à l’enrichissement des connaissances des juges et des procureurs par l’établissement de réseaux entre eux ;
* faciliter l’accès aux différentes initiatives et réseaux de formation.

Dans le cadre du projet conjoint Union européenne/Conseil de l’Europe Cybercrime@IPA (Coopération régionale en matière de justice pénale : Renforcement des capacités dans la lutte contre la cybercriminalité)[[1]](#footnote-1), les organes de formation des régions visées par les projets (Albanie, Bosnie-Herzégovine, Croatie, Monténégro, Serbie, « l’ex-République yougoslave de Macédoine », Turquie et Kosovo[[2]](#footnote-2)) bénéficient d’un soutien pour la mise en œuvre du concept de formation.

Dans ce contexte, des supports didactiques ont été élaborés à l’usage des organes de formation, un « Programme de formation de formateurs » a été mis en œuvre et un centre régional, qui a son siège en Croatie, a été créé.

La dernière version mise à jour (2018) du cours a été établie pour veiller à ce que les supports rendent compte de l’évolution actuelle de la cybercriminalité et des vecteurs par lesquels sont commises les infractions, tout en garantissant la pertinence de ces facteurs pour d’autres régions du monde. Il est prévu que le matériel de formation actualisé permettra d’adapter le cas pratique, élément central du cours, pour qu’il puisse être présenté dans n’importe quelle partie du monde au cours de la phase de mise en œuvre du cours et lors de sa prochaine mise à jour. En outre, les présentations ont été renouvelées et revues pour s’assurer qu’elles correspondent aux objectifs d’apprentissage de chaque session, et que le contenu du cours soit mis à jour de manière à tenir compte des évolutions technologiques et des changements d’approche des cybercriminels d’aujourd’hui dans la perpétration de ces infractions pénales.

Dans le cadre du précédent projet GLACY, un document d’orientation intitulé « Lignes directrices pour la dispense des modules de formation judiciaire relatifs à la cybercriminalité et à la preuve électronique du Conseil de l’Europe » a été élaboré. Ce document devrait être disponible sur le site web du Conseil de l’Europe à l’adresse [www.coe.int/cybercrime](http://www.coe.int/cybercrime). La démarche adoptée par le CdE consiste à donner aux pays les moyens d’établir leur propre programme en leur fournissant les premiers niveaux de formation puis en les aidant à intégrer la formation disponible dans leurs programmes nationaux. Le présent document donne des informations sur la formation disponible pour qu’elle puisse être dispensée pendant et après l’engagement du CdE dans chaque pays. Il ne reprend pas le contenu des supports existants et fait référence à ces derniers pour que les lecteurs puissent les examiner conjointement avec les informations présentées ici. Ce document peut être utile pour les pays qui prévoient de dispenser une formation sur la cybercriminalité à l’échelle nationale.

Cette mise à jour du cours apporte des modifications importantes au matériel déjà existant relatif à la formation avancée. Une nouvelle étude de cas a été adoptée et une nouvelle approche a été définie pour aborder des sujets tels que l’entraide judiciaire, les requêtes, les audiences et les études de cas concernant la Convention de Budapest. De plus, des changements significatifs sont à signaler dans les domaines de la preuve électronique et des techniques actuelles employées par les cyberdélinquants. L’objectif de ces modifications est de faire acquérir aux participants un ensemble de compétences à jour, ce qui leur permettra non seulement de transférer ces connaissances au sein de leurs parquets et de leurs tribunaux respectifs, mais aussi de devenir des formateurs compétents pour les futurs programmes de formation au niveau local.

1. Aperçu général

## 1.1 But du cours

Le présent cours s’appuie sur le cours d’introduction à l’intention des juges et des procureurs élaboré par le projet GLACY du Conseil de l’Europe puis modifié et mis à jour par le projet GLACY+ en 2017. La formation a été conçue dans l’intention de permettre aux juges et aux procureurs d’approfondir leurs connaissances en matière de cybercriminalité et de preuves électroniques et d’avoir accès à une plus grande compréhension des techniques de pointe pour l’analyse juridique des éléments de preuves apportés lors de la phase préparatoire et de la phase principale du procès, tout en apprenant à mieux les utiliser. La formation fournira aux juges et aux procureurs des informations juridiques et pratiques sur les problématiques abordées et s’intéressera en particulier à leurs répercussions sur le travail quotidien des magistrats.

* *Le but de ce cours est de fournir aux juges et aux procureurs les connaissances et les compétences nécessaires pour remplir leur rôle dans les enquêtes et les procès liés à la cybercriminalité.*
* *Ce cours s’appuie sur les acquis de la formation de base sur la cybercriminalité à l’intention des juges et des procureurs et ne devrait être suivi que par des participants l’ayant achevée avec succès.*

Le cours couvrira les sujets suivants :

* *conduite d’une enquête ;*
* *identification des types d’infractions commises ;*
* *détermination des lieux dont proviennent les éléments de preuve, les témoins et les suspects ;*
* *monnaies traditionnelles et alternatives ;*
* *obtention de preuves d’une manière satisfaisante, quel que soit l’endroit où elles sont détenues ;*
* *préparation de perquisitions et de saisies concernant des preuves électroniques ;*
* *traitement des dispositifs numériques faisant partie de l’enquête ;*
* *communication d’informations aux spécialistes, notamment en criminalistique, dont le soutien est nécessaire lors de la phase d’enquête ;*
* *préparation des interrogatoires de suspects ;*
* *présentation des preuves en matière de cybercriminalité ;*
* *introduction des requêtes et conduite des audiences dans des affaires de cybercriminalité dans le cadre de la procédure pénale des systèmes juridiques de common law et de droit civiliste ;*
* *prise en compte des aspects pertinents au cours de la procédure judiciaire et du procès dans le but ultime de rendre une décision judicieuse.*

## 1.2 Pourquoi cette formation est-elle nécessaire ?

Les procureurs et les juges jouent un rôle central dans les enquêtes et les décisions de justice concernant des individus ou des groupes qui ont commis des infractions. Avec l’augmentation du nombre d’affaires relatives à des infractions comportant un élément numérique, il devient nécessaire que ces magistrats soient convenablement formés pour qu’ils comprennent la nature desdites infractions et qu’ils connaissent la législation en matière de coopération internationale ainsi que les instruments dont ils disposent pour traiter les affaires de cybercriminalité.

Les criminels et les groupes criminels ne limitent généralement pas leur action au territoire national. La cybercriminalité est un type de délinquance excluant la nécessité pour l’auteur de l’infraction de se déplacer localement ou de franchir des frontières pour commettre un crime, ce qui complique singulièrement la conduite des enquêtes et les poursuites. Cet état de fait explique la nécessité d’améliorer la coopération internationale et régionale, ainsi que la coopération interinstitutionnelle, dans le traitement des affaires de ce type.

Les affaires de cybercriminalité requièrent souvent une coopération internationale ou régionale rapide et très efficace afin de pouvoir, sans délai et de façon opportune, lancer une enquête et engager des poursuites. L’un des objectifs que les organes de formation devraient se fixer est de s’efforcer d’intégrer dans leurs programmes d’étude des modules qui présenteraient des connaissances sur les diverses possibilités, pour les professionnels du droit pénal, de traiter ces affaires ; il conviendrait en outre d’accorder une plus grande importance à la formation concernant les outils procéduraux majeurs, comme les instruments de coopération internationale pouvant être utilisés pour enquêter sur les affaires de cybercriminalité, notamment le recours à des points de contact disponibles 24 heures sur 24 et 7 jours sur 7, les procédures et instruments d’entraide judiciaire, les activités et les plates-formes de coopération judiciaire, etc.

## 1.3 Programme d’études

Ce programme d’études est un outil à prendre en considération par les organes de formation lorsqu’ils dispensent un enseignement sur la cybercriminalité. L’objectif du présent document est de mettre l’accent sur l’élaboration et la production de cours ou de modules harmonisés qui seront utilisés dans les pays/régions couverts par le projet en vue d’assurer la formation avancée des juges et procureurs appelés à connaître des affaires de cybercriminalité.

Le modèle proposé pour le module de formation doit servir uniquement de base à la formation des juges et des procureurs et non d’objectif final à ladite formation. Les pays/régions concernés par le projet devraient discuter de leurs besoins au niveau national et demander à bénéficier d’une formation spécifique supplémentaire dans les domaines de la cybercriminalité qu’ils jugent les plus décisifs.

Les leçons qui ont été préparées fournissent des titres/sujets de présentations/conférences ainsi que des explications détaillées à répercuter par les formateurs. Le cours est conçu pour être modifié de manière à répondre aux exigences nationales, tout en garantissant que son but et ses objectifs soient atteints. Cette méthodologie permettra d’assurer la cohérence des modules de formation par-delà les frontières. Les formateurs devraient envisager d’introduire un certain nombre d’exercices/de discussions qui amélioreront l’expérience d’apprentissage des participants dans chaque pays.

Ce module de formation avancée est conçu de manière à permettre aux juges et aux procureurs qui ont suivi le module d’introduction d’améliorer leur connaissance de la nature de la cybercriminalité, ainsi que des termes et des technologies propres à ce domaine, en traitant un cas pratique qui porte sur l’ensemble de la procédure depuis la plainte initiale jusqu’au procès, en passant par l’enquête ; ils devront s’appuyer sur des fondements juridiques et des éléments de preuve suffisants pour parvenir à une décision de justice satisfaisante.

Ce module a été créé dans le but de fournir aux juges et aux procureurs les connaissances supplémentaires qui pourront leur être utiles dans la pratique sur le fonctionnement des ordinateurs et des réseaux, la nature de la cybercriminalité, la législation en la matière, les questions de compétence, les moyens d’enquête et les preuves électroniques, la coopération internationale , ainsi que les requêtes et les audiences.

Ce cours a été conçu comme l’association d’enseignements magistraux et d’un cas pratique, qui traitent l’ensemble de la procédure depuis le premier signalement de l’infraction jusqu’à la préparation de l’affaire pour qu’elle soit jugée. Les présentations complètent l’apprentissage engagé dans le cadre de l’étude du cas pratique. Ce dernier correspond à un calendrier précis et devra être mis à jour pour qu’il soit pertinent par rapport à la période au cours de laquelle il est présenté. Il peut également être adapté pour que le siège de l’entreprise victime se situe dans le pays où le cours est dispensé, afin de rendre la réglementation pénale et procédurale plus pertinente, bien que des efforts aient été faits pour que le scénario du cas pratique traite de pays et d’organismes neutres/fictifs afin d’éviter d’éventuels litiges pour des motifs politiques et des questions de propriété intellectuelle.

2. Comment utiliser le Guide du formateur ?

Le présent guide a pour but de fournir aux formateurs des informations sur la structure et le contenu du cours. Les objectifs de chaque leçon décrivent les informations à traiter. La méthodologie de ce cours a été soigneusement élaborée et toutes les aides à la formation pertinentes devraient être accompagnées du présent kit de formation. L’objectif du guide est de maintenir le caractère standard du cours et d’assurer une cohérence pendant la prestation.

Il est recommandé aux concepteurs de formations de veiller à ce que les supports qu’ils préparent soient aussi à jour que possible et tiennent compte des dernières évolutions technologiques au fur et à mesure que celles-ci influent sur les comportements des auteurs d’infractions, ainsi que sur les règles juridiques, procédurales et de preuve en vigueur dans la juridiction où la formation doit être dispensée. Il est important de prendre ces questions en considération dans les programmes de formation et il convient d’inclure ces changements au fur et à mesure que leur utilisation se généralisera.

Comme pour chaque programme, toute formation élaborée à l’intention des juges et des procureurs doit avoir des objectifs clairs conformes à la méthode SMART (spécifiques, mesurables, atteignables, pertinents et limités dans le temps). Le respect de cette condition est essentiel pour garantir l’accomplissement des objectifs. Ainsi, il convient d’éviter d’utiliser des termes comme « comprendre » ou « connaître », car ils ne remplissent pas les critères. Comment évaluer par exemple si l’objectif de « connaître » un sujet est atteint ? Il est préférable d’utiliser des mots comme « répertorier » ou « identifier » qui ont l’avantage d’être mesurables.

Le rôle déterminant du concepteur d’une formation consiste à s’assurer que la finalité globale de toute activité pédagogique et que les objectifs spécifiques soient atteints. Le présent chapitre donne quelques éléments pour faciliter ce processus.

Bien que ce cours ait été conçu comme un programme générique et non spécifique à un pays, il est important que les formateurs personnalisent leur matériel didactique pour assurer une diffusion plus efficace des supports. L’utilisation d’études de cas visant à éclairer l’apprentissage est considérée comme adaptée à ce type de formation et correspond davantage aux modes d’apprentissage des adultes qu’à un enseignement purement didactique.

Pour la mise à jour 2017/2018, les documents de preuve portent sur des pays, des villes et des personnes physiques et morales fictifs. Cette approche vise à définir un environnement générique qui permettra aux participants de se concentrer sur le déroulé des affaires en analysant les résultats des enquêtes et les éléments de preuve, avant d’examiner les problèmes de droit révélés à la fois par l’enquête et la procédure judiciaire, qui se termine par l’adoption d’une décision de justice.

Toutefois, cette méthode n’exclut pas la possibilité d’adapter les supports aux besoins des institutions locales de formation judiciaire en introduisant notamment des composantes géographiques réelles, pour permettre aux participants d’acquérir une expérience plus localisée.

3. Aperçu du cours

3.1 Combien de temps dure le cours et à qui s’adresse-t-il ?

Ce cours est conçu comme un programme de quatre jours destiné aux juges et aux procureurs dans le cadre de leur programme de formation initiale ou continue lorsqu’ils n’ont pas bénéficié auparavant de cette formation.

3.2 Qui donne le cours ?

Le cours a été conçu pour être dispensé par des formateurs internes dans les établissements de formation des magistrats des différents pays. Le cas échéant, il est conseillé de faire appel à des spécialistes pour traiter de sujets techniques spécifiques si ces institutions ne disposent pas de l’expertise nécessaire. Pour ce cours, il est particulièrement important de faire intervenir des formateurs ayant une certaine expérience de ce type d’enquête et de procédure pénale.

3.3 Comment le cours sera-t-il dispensé ?

Le cours, tel qu’il est actuellement structuré, devrait être dispensé en salle de cours en appliquant un système de formation idoine et en proposant des exercices sur papier. Néanmoins, il est fortement recommandé d’utiliser du matériel informatique, en particulier des équipements mobiles comme des ordinateurs portables et des tablettes. Il est également souhaitable de diviser les participants en groupes de travail de 5 personnes maximum pour l’ensemble du cours. Comme indiqué plus haut, dans la partie 1, les formateurs devraient envisager d’adapter les exercices et les autres méthodes d’enseignement dans le programme au niveau national. Ce cours est très interactif et exigera beaucoup de travail d’investigation de la part des participants ainsi qu’un soutien sans faille des formateurs du cours.

3.4 Objectifs du cours

Les objectifs du cours ont été rédigés de manière traditionnelle, ce qui permettra aux formateurs d’utiliser diverses méthodes pédagogiques pour les atteindre. Pour ce faire, ils répondent tous aux critères SMART, c’est-à-dire que chacun d’entre eux correspond aux caractéristiques ci-après, d’où leur nom :

* **Spécifique** – Chaque objectif doit indiquer le but précis à atteindre.
* **Mesurable** – Vous devez pouvoir mesurer si l’objectif a été atteint ou pas.
* **Atteignable** – Chaque objectif est-il réalisable et atteignable ?
* **Réaliste** – Pouvez-vous atteindre les objectifs de façon réaliste avec les ressources dont vous disposez ?
* **limité dans le Temps** – Quand voulez-vous atteindre l’objectif fixé ?

Sur cette base, les objectifs de cours ci-après ont été fixés et doivent être lus conjointement avec le but général du cours.

3.5 Groupes cibles de participants et de formateurs

### 3.5.1 Participants

Ce cours est conçu pour être dispensé aux juges et aux procureurs pendant leur période de formation initiale ou continue pour ceux qui n’ont pas suivi ce cours auparavant.

### 3.5.2 Expérience préalable requise

Ce cours est conçu pour être suivi uniquement par des personnes qui ont déjà achevé la formation d’introduction sur la cybercriminalité et les preuves électroniques conçue par le Conseil de l’Europe ou par un module équivalent au niveau national.

### 3.5.3 Formateurs

Les établissements de formation des magistrats devraient employer des formateurs pour assurer ce cours, parmi lesquels devraient figurer des personnes expérimentées dans la conduite d’enquêtes en matière de cybercriminalité, ainsi que des magistrats responsables d’engager des poursuites ou de rendre des jugements dans ce type d’affaires.

### 3.5.4 Expérience préalable requise

Les formateurs devraient avoir une bonne connaissance des problèmes/tendances propres à la cybercriminalité et de la législation pertinente dans leur pays d’origine. Une expérience préalable en tant que formateur avec des connaissances théoriques et pratiques de l’enseignement est exigée.

3.6 Ressources

### 3.6.1 Ressources nécessaires au cours

Pour assurer cette formation en salle de cours, il est nécessaire de disposer des ressources suivantes :

* une salle suffisamment grande pour accueillir le nombre de participants prévu. Il conviendrait de mettre en place une table ronde par équipe, si possible selon une disposition de base de 5 participants par groupe ;
* un PC/portable fonctionnant sous Windows 7, 8 ou 10 et équipé de MS Office Professional ;
* un projecteur et un écran ;
* un accès à internet (si possible) ;
* des exemplaires de la Convention du Conseil de l’Europe sur la cybercriminalité ;
* des exemplaires de la version 2 du Guide du Conseil de l’Europe sur la preuve électronique ;
* un tableau blanc pour chaque groupe ;
* des feutres pour tableau blanc (au moins deux pour chacune des couleurs suivantes : bleu, noir, rouge et vert) pour chaque groupe ;
* un chevalet à feuilles mobiles avec assez de papier pour chaque groupe ;
* des blocs-notes et des stylos ;
* une agrafeuse, une perforatrice et des ciseaux pour chaque groupe ;
* de la Patafix ou un produit analogue pour coller provisoirement des documents aux murs pour chaque groupe ;
* un ordinateur portable pour chaque groupe, avec une configuration similaire à celle du PC du formateur et un accès à internet permettant de faire des recherches d’informations ;
* tous les supports pédagogiques fournis dans le kit de formation.

Les ressources ci-après ont été mises au point pour servir de support à la mise en œuvre du cours. Ils sont présentés sous forme électronique, car ils sont volumineux. Le CdE fournira toutes les ressources aux pays.

### 3.6.2 Personnalisation des ressources pédagogiques

Le cours traite des questions juridiques qui se posent dans l’utilisation du cadre des conventions et traités internationaux pertinents (comme les conventions du Conseil de l’Europe de Budapest et de Varsovie). Il sera nécessaire que le formateur identifie les dispositions de sa législation nationale en la matière, afin de les intégrer aux supports pédagogiques. Il sera également nécessaire de présenter des exemples de décisions, de formulaires, de documents types, etc., provenant des tribunaux nationaux et portant sur des affaires qui ont donné lieu à des perquisitions, des saisies et des confiscations de produits du crime.

3.7 Évaluation

Aucun contrôle des connaissances des participants n’a été demandé ni fourni dans le cadre de ce cours pilote. Les pays qui mettent en œuvre cette formation au niveau national souhaiteront peut-être instaurer une procédure d’évaluation. En tout état de cause, les formateurs devraient vérifier les connaissances des participants pendant le cours, en posant des questions, en invitant les intéressés à remplir des questionnaires ou en utilisant d’autres méthodes pour s’assurer que les objectifs d’apprentissage soient bien atteints.

3.8 Emploi du temps



3.9 Objectifs du cours et des sessions

|  |  |  |
| --- | --- | --- |
| **Numéro de la session** | **Intitulé** | **Objectifs** |
| 2.1.1 | **Introduction au cours et prise de contact** | Prendre connaissance du programme et des domaines abordés dans la formation avancée sur la cybercriminalité à destination des juges et des procureurs 2018  Expliquer aux participants la nécessité de la formation, son but et ses objectifs  Veiller à leur donner suffisamment d’informations sur le programme d’activités et l’emploi du temps  Leur communiquer des informations relatives à l’hygiène et à la sécurité, ainsi que les modalités administratives de la formation  Faire un tour de table pour que les formateurs et les participants se présentent |
| 2.1.2 | **Rappels sur la Convention de Budapest et nouveaux éléments** | Convention de Budapest : aspects substantiels, procéduraux et de coopération internationale de la STE 185 et de son Protocole additionnel sur la xénophobie et le racisme  Lignes directrices et avis  État d’avancement du deuxième Protocole additionnel  Nouveaux éléments sur les activités connexes |
| 2.1.3 | **Technologies et cybercriminalité** | Présenter les différentes manières de compromettre les courriels professionnels  Identifier les menaces que représente l’internet des objets (IDO)  Faire la distinction entre les différentes couches d’internet  Expliquer comment les transactions en monnaie virtuelle sont effectuées |
| 2.1.4 | **Étude de cas sur la Convention de Budapest** | Rappeler les dispositions de la Convention de Budapest relatives au droit substantiel, au droit procédural et à la coopération internationale étudiées dans le cadre du module d’introduction  Présenter le champ d’application et l’importance des dispositions de la Convention de Budapest relatives au droit substantiel, au droit procédural et à la coopération internationale  Appliquer les dispositions de la Convention de Budapest et des législations nationales correspondantes aux études de cas portant sur le droit substantiel, le droit procédural et le droit relatif à la coopération internationale |
| 2.2.1  2.2.2 | **Introduction à l’étude de cas**  **Simulation d’enquête** | Identifier les personnes morales et physiques impliquées dans le scénario  Présenter l’affaire et exposer les éléments saillants du dossier  Suivre et expliquer le déroulement et l’évolution de l’enquête  Expliquer comment l’acte criminel a été perpétré et qui en sont les principaux acteurs  Décrire comment et où l’enquête criminelle devrait commencer et quelle direction elle devrait prendre |
| 2.3.1 | **Défis liés aux preuves électroniques** | Identifier les méthodes de validation des preuves électroniques  Examiner les questions liées à l’admissibilité des preuves électroniques dans le cadre du procès  Examiner et expliquer les atouts que présentent les fichiers contenant des preuves électroniques |
| 2.3.2 | **Entraide judiciaire – Coopération internationale** | Apprendre ou se remémorer les principes fondamentaux de l’entraide judiciaire appliquée à la cybercriminalité  Identifier les bonnes pratiques dans la préparation et la rédaction d’une requête  Adopter un point de vue constructif sur les requêtes étrangères reçues pour exécution |
| 2.3.3 | **Rédaction de requêtes**  **ou**  **Demande d’autorisation** | Reconnaître les considérations particulières relatives à la rédaction de requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique  Comprendre le contenu d’une requête type, y compris sa portée et sa durée, ainsi que d’autres requêtes  Comprendre les éléments qu’il faut rechercher dans une requête visant à obtenir l’exercice de pouvoirs procéduraux en matière de preuve électronique  Comprendre certaines des considérations et des garanties qu’il convient de prendre en compte lors de la rédaction et de l’examen des requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique |
| 2.3.4 | **Conduite d’audiences et rédaction d’ordonnances**  **ou**  **Examen de demandes d’autorisation**  **Préparation de la simulation d’audience**  **ou**  **Préparation de la simulation d’examen de demandes d’autorisation** | Reconnaître les diverses considérations relatives à la conduite d’audiences sur les requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique  Expliquer les conditions et les garanties procédurales qui s’appliquent aux requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique  Identifier les compétences judiciaires importantes qui peuvent être mises en œuvre pour mener efficacement une audience sur les pouvoirs procéduraux en matière de preuve électronique  Comprendre les éléments essentiels à prendre en compte dans la rédaction d’une ordonnance judiciaire permettant l’exercice de pouvoirs procéduraux en matière de preuve électronique |
| 2.3.5 | **Préparation de la simulation d’audience**  **ou**  **Examen de demandes d’autorisation** | Travail de groupe sur le module précédent |
| 2.4.1 | **Simulation d’audience**  **ou**  **Simulation d’examen de demandes d’autorisation** | Reconnaître les diverses considérations relatives à la conduite d’audiences sur les requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique  Expliquer les conditions et les garanties procédurales qui s’appliquent aux requêtes concernant l’exercice de pouvoirs procéduraux en matière de preuve électronique  Identifier les compétences judiciaires importantes qui peuvent être mises en œuvre pour mener efficacement une audience sur les pouvoirs procéduraux en matière de preuve électronique  Comprendre les éléments essentiels à prendre en compte dans la rédaction d’une ordonnance judiciaire permettant l’exercice de pouvoirs procéduraux en matière de preuve électronique |
| 2.4.2 | **Retour d’informations sur la simulation d’audience**  **ou**  **Retour d’informations sur la simulation d’examen de demandes d’autorisation** | Retour d’informations par les participants et les formateurs sur la simulation d’audience ou de demande d’autorisation |
| 2.4.3 | **Clôture du cours** | Donner un retour approprié sur la formation et son efficacité  Distribution du formulaire d’évaluation  Remplir les formulaires d’évaluation de la formation  Identifier le palier d’apprentissage suivant dont ils ont besoin pour approfondir leurs connaissances et améliorer leurs compétences dans le domaine  Observations finales et perspectives |

4. Principaux contacts

Les personnes suivantes doivent être contactées pour toute demande ou question concernant le cours et son contenu :

|  |
| --- |
| Alexander Seger  Chef de la division Cybercriminalité  Direction générale des droits de l’homme et de l’État de droit (DG-I)  Conseil de l’Europe  F-67075 Strasbourg Cedex  Tél. : +33 3 88 41 21 03  Fax : +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int)  Matteo Lucchetti  Directeur de programme  Bureau de programme sur la cybercriminalité (C-PROC), division de la Cybercriminalité  Direction générale des droits de l’homme et de l’État de droit (DG-I)  Conseil de l’Europe  Bucarest, Roumanie  Tél. : +40 (21) 201 78 30  [matteo.lucchetti@coe.int](mailto:matteo.lucchetti@coe.int) |

5. Plan des sessions

Leçon 2.1.1 (Ouverture du cours et introduction)

|  |  |  |
| --- | --- | --- |
| Leçon 2.1.1 (Ouverture du cours et introduction) | | Durée : 30 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Cette session vise à présenter aux participants le déroulement de la formation et les thèmes et domaines qui seront abordés. | | |
| **Objectifs :**  À l’issue de cette session, les participants seront en mesure :   * d’avoir des connaissances de base sur le programme et les domaines abordés dans la formation avancée sur la cybercriminalité à destination des juges et des procureurs 2018 ; * de comprendre la nécessité de la formation, son but et ses objectifs ; * de disposer de suffisamment d’informations sur le programme d’activités et l’emploi du temps ; * d’avoir des informations relatives à l’hygiène et à la sécurité, ainsi que de connaître les modalités administratives de la formation ; * de connaître les formateurs et les autres participants. | | |
| **Conseils pour le formateur**  Cette présentation est de nature introductive et devrait donner une vue d’ensemble et une première idée de la formation et des compétences qui seront développées dans le cadre du cours. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. Les questions de santé et de sécurité seront également abordées. | |
| 4 | Cette diapositive présente le contexte de la formation. Le titre de celle-ci est « Formation avancée sur la cybercriminalité et les preuves électroniques à destination des juges et des procureurs ». Elle a été élaborée dans le cadre du Projet conjoint Union européenne/Conseil de l’Europe sur la coopération régionale en matière de cybercriminalité dans les pays concernés par l’IAP. Les derniers ajouts sont le fruit des travaux menés dans le cadre des projets GLACY et GLACY+. | |
| 5 | Cette diapositive fournit des informations sur la nécessité de la formation, qui s’explique par le fait que les juges et les procureurs jouent un rôle important dans les enquêtes et les procès concernant des individus ou des groupes ayant commis des infractions.  Avec l’augmentation du nombre d’affaires relatives à des infractions comportant un élément propre à la cybercriminalité, il est de plus en plus nécessaire que ces magistrats soient convenablement formés pour qu’ils comprennent la nature desdites infractions et qu’ils connaissent la législation en matière de coopération internationale et les instruments dont ils disposent pour traiter les affaires de cybercriminalité. | |
| 7 | Le but général de la formation est expliqué aux participants dès le départ. Cela leur permettra de comprendre la raison plus globale de leur présence. Le but de ce cours est de fournir les connaissances et les compétences nécessaires pour permettre aux juges et aux procureurs de remplir leur rôle dans les enquêtes sur la cybercriminalité.  Ce cours s’appuie sur les acquis de la formation de base sur la cybercriminalité à l’intention des juges et des procureurs et ne devrait être suivi que par des participants l’ayant achevée avec succès. | |
| 8 | Objectifs de la session | |
| 10 | Cette diapositive est laissée vide pour que chaque pays indique le nom des formateurs qui dispensent le cours. | |
| 12 | La diapositive sur la méthodologie devrait fournir des informations sur le contenu ultérieur de la formation qui se présentera sous la forme d’un assortiment d’exposés et d’exercices basés sur un scénario. Il est structuré de cette façon à la suite des demandes reçues pendant le cours de base qui réclamaient plus d’informations sur les affaires et la criminalistique numérique.  Ce cours permettra aux participants non seulement d’assister à des présentations par des experts, mais aussi de travailler eux-mêmes sur une enquête en s’appuyant sur les informations qui leur seront fournies pendant le cours. | |
| 13 | À ce stade, il conviendra d’expliquer l’emploi du temps aux participants. Devraient y figurer les horaires des sessions de formation, le déjeuner et d’autres pauses ainsi qu’une brève description de chaque session.  C’est également à ce stade qu’il conviendra d’évoquer une évaluation éventuelle, auquel cas on expliquera de manière détaillée en quoi elle consiste, notamment pour ce qui est des attentes des participants en matière d’apprentissage. | |
| 15 | Cette diapositive permet, dans un deuxième temps, de présenter les formateurs et les participants Il est important de profiter de cette première occasion pour les amener à interagir entre eux et avec les formateurs. Il devra être demandé aux participants de s’associer en binôme à une personne du groupe qu’ils ne connaissent pas déjà. Il conviendra ensuite de leur donner pour tâche de partager des informations entre « partenaires » sur les questions suivantes :  nom et pays ;  lieu de travail ;  activité professionnelle ;  expérience de formateur ;  autres éléments personnels intéressants.  Les membres des binômes devront s’échanger les mêmes questions. Ils devront ensuite présenter leur « nouveau collègue » au reste du groupe. Le formateur devra prendre note de ces informations pour les aider à mieux connaître les participants. | |
| 16 | Le formateur devra récapituler/tester les connaissances sur les différents points pour s’assurer que l’auditoire a compris les objectifs d’apprentissage de la session. Au cours de la session, il conviendra de ménager à intervalles réguliers des plages de temps suffisamment longues pour les questions. | |
| **Exercices pratiques**  Aucun exercice pratique obligatoire n’est prévu. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. On attendra des participants qu’ils s’impliquent activement dans la session. | | |

Leçon 2.1.2 (Mise à jour sur la Convention de Budapest – Accès aux preuves électroniques dans le cloud et Protocole additionnel)

|  |  |  |
| --- | --- | --- |
| Leçon 2.1.2 (Mise à jour sur la Convention de Budapest – Accès aux preuves électroniques dans le cloud et Protocole additionnel) | | Durée : 60 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Cette session vise à présenter aux participants le déroulement de la formation et les thèmes et domaines qui seront abordés. | | |
| **Objectifs :**  À l’issue de cette session, les participants seront en mesure :   * d’avoir une représentation à jour de la portée de la Convention de Budapest ; * d’énumérer les principaux problèmes rencontrés lors de l’accès aux preuves électroniques dans le cloud ; * de connaître les solutions actuellement envisagées dans le contexte de la législation internationale. | | |
| **Conseils pour le formateur**  Cette présentation devrait fournir une mise à jour aux participants sur les dernières évolutions concernant la Convention du Conseil de l’Europe sur la cybercriminalité (STE 185) et les projets de renforcement des capacités élaborés par le Conseil et mis en œuvre par le Bureau de programme sur la cybercriminalité.  Elle devrait également présenter les derniers développements dans la manière dont sont perpétrées à l’heure actuelle les infractions pénales dans le domaine de la cybercriminalité. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-5 | Ces diapositives donnent des informations sur les principaux défis actuels concernant la compréhension et la mise en œuvre pratique du droit substantiel, procédural et international dans le domaine de la cybercriminalité. | |
| 6 | Cette diapositive donne des informations sur la Convention de Budapest, sa mise en œuvre et ses articles. Les formateurs devront avoir à disposition le texte de la Convention accompagné de notes explicatives. | |
| 7 | Diapositive sur la portée géographique de la Convention. Plus de 130 pays ont ratifié ou signé la Convention, ou la mettent en œuvre de différentes manières. | |
| 8 | Diapositive sur le champ d’application de la Convention. Comportement des auteurs d’infractions, outils procéduraux et articles de la Convention portant sur la coopération internationale présentés sous forme de graphiques en mettant l’accent sur les moyens et les besoins d’harmonisation. | |
| 9 | Cette diapositive présente les défis posés par la preuve dans le cadre de l’utilisation de l’informatique en nuage et la manière dont la Convention sur la cybercriminalité est applicable à ces questions. | |
| 10-11 | Ces diapositives présentent l’organisation et les travaux du Groupe de travail sur les preuves dans le cloud (GPC) du T-CY, notamment en ce qui concerne les problèmes qui ont été recensés et pour lesquels le T-CY devrait recommander des solutions réalisables et efficaces. | |
| 12 | Cette diapositive établit une comparaison entre les données relatives aux abonnés, au trafic et au contenu. | |
| 13 | Cette diapositive fournit des informations sur l’entraide judiciaire et les défis à relever actuellement pour mettre en place une coopération continue et réussie en matière de cybercriminalité. | |
| 13 | Cette diapositive fournit des informations sur l’entraide judiciaire et les défis à relever actuellement pour mettre en place une coopération continue et réussie en matière de cybercriminalité. | |
| 13 | Cette diapositive fournit des informations sur l’entraide judiciaire et les défis à relever actuellement pour mettre en place une coopération continue et réussie en matière de cybercriminalité. | |
| 14-15 | Diapositive sur la perte de la localisation des données. Le formateur devra avoir connaissance des défis présentés lors des réunions du T-CY à cet égard et des solutions mises en œuvre jusqu’à présent par les différentes juridictions nationales. | |
| 16-18 | Ces diapositives donnent un aperçu plus précis de la coopération public-privé, à savoir, en l’occurrence, entre les autorités de justice pénale compétentes et les fournisseurs d’accès à internet. Différents aspects sont examinés à cet égard, tels que la présence des FAI, l’offre de services, la divulgation volontaire d’informations sur leur bilan et sur les données relatives au trafic par les FAI dans certains pays (ou non), etc.  Des statistiques de 2015 pour certaines entreprises et certains pays sont également présentées. | |
| 19-20 | Ces diapositives portent sur les procédures d’urgence menées dans le cadre de l’entraide judiciaire et de la coopération directe, ainsi que la protection des données et d’autres garanties. | |
| 21-28 | Ces diapositives concernent les solutions identifiées par le Groupe de travail sur les preuves dans le cloud du Conseil de l’Europe, qui reposent notamment sur une entraide judiciaire plus efficace, une note d’orientation sur l’article 18 de la Convention de Budapest, les règlementations nationales relatives aux injonctions de produire, des mesures pratiques de coopération avec les fournisseurs et des protocoles additionnels à la Convention de Budapest. | |
| **Exercices pratiques**  Aucun exercice pratique obligatoire n’est prévu. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. On attendra des participants qu’ils s’impliquent activement dans la session. | | |

Leçon 2.1.3 (Technologies et cybercriminalité)

|  |  |  |
| --- | --- | --- |
| Leçon 2.1.3 (Technologies et cybercriminalité) | | Durée : 150 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  L’objectif de cette session est d’informer les participants des nouveaux types d’infractions et des nouvelles menaces véhiculées par les nouvelles technologies. Bien que certains des sujets aient été abordés brièvement dans le cours d’introduction, ils sont traités plus en détail dans cette session. | | |
| **Objectifs:**  À l’issue de cette session, les participants seront en mesure :   * de connaître les différentes manières de compromettre les courriels professionnels ; * d’identifier les menaces que représente l’internet des objets (IDO) ; * de faire la distinction entre les différentes couches d’internet ; * de comprendre comment les transactions en monnaie virtuelle sont effectuées. | | |
| **Conseils pour le formateur**  Cette session présente les dernières technologies qui ont des effets sur le comportement des auteurs d’infractions. L’Évaluation de la menace en ligne sur internet (IOCTA) 2017 a été publiée en septembre 2017 et est utilisée dans certaines diapositives car il s’agit des informations disponibles les plus à jour. Les formateurs devront revoir ces informations à mesure que de nouveaux rapports et de nouvelles données seront disponibles. Les vidéos utilisées au cours de cette session sont authentifiées et peuvent être téléchargées et utilisées gratuitement. Le formateur peut souhaiter s’appuyer sur la démonstration comme méthode d’enseignement, par exemple au cours de la session sur le Darknet, en utilisant le navigateur TOR pour montrer aux participants comment accéder aux outils de lutte contre la criminalité en ligne. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-18 | Ces diapositives donnent des informations sur l’influence d’internet, à l’échelle mondiale (diapositives 5 à 12) et spécifiquement pour le pays où le cours est dispensé (diapositives 13 à 18). Le formateur devra s’assurer que ces diapositives sont pertinentes pour le pays où se tient la formation et les utiliser pour discuter des effets d’internet au sein de ce pays et dans le contexte mondial. | |
| 19-30 | Ces diapositives fournissent des informations sur les infractions récentes qui ont des répercussions significatives. Le formateur devra se familiariser avec ces infractions et présenter celles qui sont pertinentes pour la région où la formation est dispensée. Le formateur pourra souhaiter substituer à certains cas prévus des affaires spécifiques au pays. | |
| 31-32 | Ces diapositives présentent des informations issues de l’IOCTA 2017 en rapport avec la compromission de courriels professionnels. | |
| 33 | Le formateur devra poser aux participants la question figurant dans la diapositive. En l’absence de réponse, il poursuivra la présentation. S’il y a des exemples, il conviendra d’accorder du temps aux participants pour qu’ils développent leurs explications et d’utiliser les informations données pour établir des comparaisons avec les éléments fournis dans la présentation. | |
| 34-42 | Ces diapositives et les vidéos proviennent des informations et des données de Trend Micro/Europol et donnent une très bonne explication des méthodologies et des mesures de prévention relatives à la compromission des courriels professionnels (BEC). La vidéo finale présente la compromission des processus professionnels (BPC) comme une variante de la BEC. | |
| 43-44 | Ces diapositives constituent une introduction au sujet de l’internet des objets (IDO). Le formateur devra inviter les participants à partager toute connaissance ou expérience qu’ils pourront avoir de l’IDO.  Veuillez noter que la diapositive 45 est une vidéo qui donne un très bon exemple de la façon dont un véhicule à moteur peut être connecté à plusieurs services par l’IDO et comment ces services peuvent présenter de grands avantages pour un client. Le formateur pourra également s’intéresser à la disponibilité des preuves électroniques grâce à ces connexions. | |
| 45 | Cette vidéo donne un très bon exemple de la façon dont un véhicule à moteur peut être connecté à plusieurs services par l’IDO et comment ces services peuvent présenter de grands avantages pour un client. Le formateur pourra également s’intéresser à la disponibilité des preuves électroniques grâce à ces connexions. | |
| 46 | Cette diapositive offre l’occasion de présenter la version 6 de l’IP comme la plate-forme qui permet à l’IDO de fonctionner. | |
| 47 | Cette diapositive permet au formateur d’aborder les problèmes de sécurité posés par les dispositifs de l’IDO et le fait que leurs concepteurs ne sont pas des experts en sécurité. Du point de vue de la sécurité, les dispositifs de l’IDO sont des bombes à retardement. Le formateur pourra développer les points évoqués en fonction de sa propre connaissance du sujet. | |
| 48-49 | Ces diapositives présentent d’autres informations à jour tirées du rapport de l’IOCTA 2017. Elles étayent les points abordés dans la diapositive 20. | |
| 50-57 | Ces diapositives donnent des informations sur les dispositifs de l’IDO et sur certains des problèmes qu’ils posent. Les formateurs sont encouragés à utiliser des exemples qu’ils connaissent et en particulier s’il y a des problèmes de sécurité avec eux, comme c’est le cas avec l’e-Kettle. | |
| 58-60 | Ces diapositives marquent le début de la session sur le Darknet et les services. Elles définissent le contexte de l’IOCTA pour lancer le sujet. | |
| 61-67 | Ces diapositives présentent le Darknet, ses usages et services criminels, ainsi que certains succès rencontrés dans la fermeture de sites utilisés pour des activités criminelles. Le formateur est encouragé à s’appuyer sur des démonstrations en direct de l’accès au Darknet le cas échéant et lorsque la connexion internet le permet. | |
| 68-77 | Ces diapositives constituent principalement un rappel des questions soulevées dans le module d’introduction, comprenant un support vidéo supplémentaire et, comme pour d’autres sujets, les informations les plus récentes issues du rapport IOCTA 2017. | |
| 78-79 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Il n’y a pas d’exercices pratiques obligatoires, bien que les formateurs soient encouragés à faire une démonstration en direct de l’accès au Darknet, le cas échéant. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. On attendra des participants qu’ils s’impliquent activement dans la session. | | |

Leçon 2.1.4 (Étude de cas sur la Convention de Budapest)

|  |  |  |
| --- | --- | --- |
| Leçon 2.1.4 (Étude de cas sur la Convention de Budapest) | | Durée : 60 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants * Des exemplaires de l’étude de cas et de la Convention de Budapest pour les participants | | |
| **But de la session :**  Le but de cette session est de donner aux participants l’occasion de développer des aspects pratiques de leur connaissance de la Convention de Budapest en travaillant sur une étude de cas qui porte sur le droit substantiel, les pouvoirs procéduraux, l’entraide judiciaire et d’autres formes de coopération internationale rendues possibles par la Convention de Budapest. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de se remémorer les dispositions de la Convention de Budapest relatives au droit substantiel, au droit procédural et à la coopération internationale étudiées dans le cadre du module d’introduction ; * de connaître le champ d’application et l’importance des dispositions de la Convention de Budapest relatives au droit substantiel, au droit procédural et à la coopération internationale ; * d’appliquer les dispositions de la Convention de Budapest et des législations nationales correspondantes aux études de cas portant sur le droit substantiel, le droit procédural et le droit relatif à la coopération internationale. | | |
| **Conseils pour le formateur**  La Convention de Budapest est le premier traité international traitant spécifiquement de la cybercriminalité, des pouvoirs procéduraux relatifs à ce type d’infractions et aux preuves électroniques, ainsi que de la coopération internationale entre les parties. Cette leçon avancée se présente sous la forme d’une brève étude de cas qui couvre tous les aspects de la Convention de Budapest, en s’appuyant sur les notions abordées dans les modules d’introduction relatifs au droit substantiel, aux pouvoirs procéduraux, à l’entraide judiciaire et à la coopération public-privé. L’étude de cas est divisée en quatre parties et la présentation qui l’accompagne, qui comprend une introduction à l’étude de cas, comporte cinq parties. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-18 | Ces diapositives présentent aux participants les faits abordés et les questions posées dans le cadre de l’étude de cas sur laquelle ils devront travailler. Le formateur devra expliquer les éléments en détail aux participants et en particulier se concentrer sur les aspects essentiels des faits qui sont importants pour répondre aux questions. Le formateur devra permettre aux participants de poser des questions sur les faits ou sur n’importe quel aspect à ce stade préliminaire avant de leur donner le temps de résoudre l’étude de cas. | |
| **Étude de cas** | | |
| 19-35 | Ces diapositives couvrent les questions relatives au droit substantiel. Il est prévu de permettre aux participants de tenter de répondre aux questions pertinentes. Le formateur devra revoir les faits pertinents et traiter ensuite chaque question individuellement. Les diapositives sont organisées de la façon suivante : chaque question est suivie d’une ou plusieurs diapositives mettant en évidence les faits relatifs à la question, puis d’une ou plusieurs diapositives montrant les parties pertinentes des dispositions de la Convention de Budapest, qui sont finalement suivies des réponses et explications nécessaires.  Le formateur devra permettre dans une large mesure aux participants de répondre aux questions à l’oral. Ces diapositives sont destinées à tester la compréhension de la Convention de Budapest par les participants à la fois dans ses aspects théoriques et pratiques, et en particulier des notions liées aux articles 2 (Accès illégal), 5 (Atteinte à l’intégrité du système) et 6 (Abus de dispositifs) de la Convention. | |
| 36-51 | Ces diapositives couvrent les questions relatives aux pouvoirs procéduraux. Il est prévu de permettre aux participants de tenter de répondre aux questions pertinentes. Le formateur devra revoir les faits pertinents et traiter ensuite chaque question individuellement. Les diapositives sont organisées de la façon suivante : chaque question est suivie d’une ou plusieurs diapositives mettant en évidence les faits relatifs à la question, puis d’une ou plusieurs diapositives montrant les parties pertinentes des dispositions de la Convention de Budapest, qui sont finalement suivies des réponses et explications nécessaires.  Le formateur devra permettre dans une large mesure aux participants de répondre aux questions à l’oral. Ces diapositives sont destinées à tester la compréhension, par les participants, des aspects théoriques et pratiques des pouvoirs procéduraux énoncés dans la Convention de Budapest et leurs compétences s’agissant de déterminer les pouvoirs procéduraux à exercer en fonction des faits établis. En particulier, les notions liées à l’article 16 (Conservation rapide de données informatiques stockées), 18.1.a. et 18.1.b. (Injonction de produire des données relatives aux abonnés et des données informatiques) de la Convention de Budapest sont examinées dans cette partie. | |
| 52-64 | Ces diapositives couvrent les questions relatives aux autres formes de coopération internationale. Elles portent en particulier sur les formes de coopération internationale permises par la Convention de Budapest qui n’exigent pas de formuler des demandes d’entraide judiciaire. Il est prévu de permettre aux participants de tenter de répondre aux questions pertinentes. Le formateur devra revoir les faits pertinents et traiter ensuite chaque question individuellement. Les diapositives sont organisées de la façon suivante : chaque question est suivie d’une ou plusieurs diapositives mettant en évidence les faits relatifs à la question, puis d’une ou plusieurs diapositives montrant les parties pertinentes des dispositions de la Convention de Budapest, qui sont finalement suivies des réponses et explications nécessaires.  Le formateur devra permettre dans une large mesure aux participants de répondre aux questions à l’oral. Ces diapositives sont destinées à tester la compréhension, par les participants, des aspects théoriques et pratiques des formes de coopération prévues par la Convention de Budapest. En particulier, les notions relatives à l’article 18.1.b. (injonctions de produire transfrontières visant à obtenir des informations relatives aux abonnés) et à l’article 32 (accès transfrontière à des données avec consentement) font l’objet des questions posées dans cette partie. | |
| 65-79 | Ces diapositives couvrent les questions relatives à l’entraide judiciaire. Il est prévu de permettre aux participants de tenter de répondre aux questions pertinentes. Le formateur devra revoir les faits pertinents et traiter ensuite chaque question individuellement. Les diapositives sont organisées de la façon suivante : chaque question est suivie d’une ou plusieurs diapositives mettant en évidence les faits relatifs à la question, puis d’une ou plusieurs diapositives montrant les parties pertinentes des dispositions de la Convention de Budapest, qui sont finalement suivies des réponses et explications nécessaires.  Le formateur devra permettre dans une large mesure aux participants de répondre aux questions à l’oral. Ces diapositives sont destinées à tester la compréhension, par les participants, des aspects théoriques et pratiques des dispositions de la Convention de Budapest relatives à l’entraide judiciaire et leurs compétences s’agissant de déterminer les dispositions de ce domaine à invoquer en fonction des faits établis. En particulier, les notions relatives à l’article 29 (Conservation rapide de données informatiques stockées), à l’article 30 (Divulgation rapide de données relatives au trafic conservées), à l’article 31 (Entraide concernant l’accès aux données stockées) et à l’article 33 (Entraide dans la collecte en temps réel de données relatives au trafic) sont examinées dans cette partie. | |
| 80-82 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Il est prévu que les participants terminent l’étude de cas incluse dans cette leçon une fois que le formateur aura présenté les diapositives 1 à 18. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. On attendra des participants qu’ils s’impliquent activement après avoir terminé l’exercice de cas pratique. | | |

Leçon 2.2.1 (Introduction à l’étude de cas)

|  |  |  |
| --- | --- | --- |
| Leçon 2.2.1 (Introduction à l’étude de cas) | | Durée : 30 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de présenter les concepts de base de l’étude de cas. La session devrait également présenter une conclusion de cette première partie du cours, qui servira pour les présentations suivantes sur les systèmes de compromission de courriels professionnels, les monnaies virtuelles et la Convention de Budapest. | | |
| **Objectifs :**  À la fin de la session, les participants devront être en mesure :   * d’identifier les personnes morales et physiques impliquées dans le scénario ; * de présenter l’affaire et d’exposer les éléments saillants du dossier ; * de suivre et d’expliquer le déroulement et l’évolution de l’enquête ; * d’expliquer comment l’acte criminel a été perpétré et qui en sont les principaux acteurs ; * de décrire comment et où l’enquête criminelle devrait commencer et quelle direction elle devrait prendre. | | |
| **Conseils pour le formateur**  Cette session a été préparée pour permettre aux participants d’avoir une première présentation des principaux éléments de l’affaire. Elle comprend cinq parties. La première partie contient une introduction et présente les principales parties à l’affaire. La deuxième partie présente les principaux éléments de l’affaire. La troisième partie aborde la perpétration de l’infraction pénale. La quatrième partie pose les bases du début de l’enquête et des travaux que les participants devront réaliser. La cinquième partie résume les informations présentées précédemment. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-9 | Ces diapositives fournissent une introduction dans le monde fictif de pays qui n’existent pas en réalité, mais qui ont ratifié la Convention de Budapest, aux fins de la formation. Les participants découvriront la Federal Bank of Atlantis, United Bank Printing et la Docklands Securitas Bank of Norland.  Le scénario du cas pratique commence par la description de la Federal Bank of Atlantis (FBA) comme une banque internationale renommée, bien établie et réputée depuis longtemps. Ces caractéristiques devraient amener les participants à penser que ce genre de banque ne devrait pas être impliquée dans des problèmes de quelque nature que ce soit, et encore moins rencontrer des difficultés du type de celles qui seront décrites plus loin.  Les participants devront identifier les faits principaux et les divisions et acteurs essentiels dans l’entreprise afin de comprendre la portée et l’organisation du cercle d’affaires dans lequel d’autres faits seront exposés. | |
| 10-14 | Aux fins de la présente formation, des pays et des entreprises fictifs ont été créés. Il s’agit de l’Atlantide, du Norland, de l’Ostland, du Westland, etc. Pour l’exercice, tous ont ratifié la Convention du Conseil de l’Europe sur la cybercriminalité (« Convention de Budapest »).    Cette approche vise à faciliter le transfert de la formation d’une juridiction à l’autre, sans qu’il soit nécessaire d’apporter des changements majeurs au matériel didactique.  La configuration financière devrait indiquer que le transfert bancaire initial s’est déroulé sans problème et que la mention des comptes SWIFT et IBAN signifie que le transfert d’argent est de nature internationale et non nationale. | |
| 21-25 | Ces diapositives présentent le début de l’enquête. L’enquête devra débuter dans les groupes de travail, les chefs de groupe et les membres commençant à travailler sur l’affaire à partir des informations de base fournies dans le dossier.  Les preuves électroniques devront être examinées et utilisées en tant qu’outil essentiel pour le lancement et la conclusion de l’enquête, ainsi que pour la préparation du procès. | |
| 26-27 | Résumé  Il est recommandé de répéter toutes les étapes principales en donnant aux participants un peu plus de temps pour poser des questions et traiter la « réalité » du cas pratique.  Les formateurs devront être très bien informés à la fois sur le cas pratique et les mécanismes utilisés pour sa création, pour être prêts à répondre aux participants et à les aider. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. | | |

Leçon 2.2.2 (Examen des preuves dans l’étude de cas et simulation d’enquête)

|  |  |  |
| --- | --- | --- |
| Leçon 2.2.2 (Examen des preuves dans l’étude de cas et simulation d’enquête) | | Durée : 360 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de présenter les concepts de base des preuves dans l’étude de cas. Seules les parties importantes devraient être présentées, sans entrer dans trop de détails révélateurs afin de ne pas enlever toute difficulté à l’exercice. | | |
| **Objectifs :**   * À la fin de la session, les participants devront être en mesure : * de comprendre l’introduction aux preuves et les premiers éléments de preuve de l’affaire ; * de comprendre l’évolution de l’affaire en analysant les preuves électroniques et matérielles présentées ; * de suivre la perpétration réelle et les autres faits énoncés dans les déclarations des témoins ; * de trouver des informations supplémentaires sur les principaux termes et définitions relatifs au cyberespace et aux outils permettant de commettre une infraction et utilisés dans cette affaire. | | |
| **Conseils pour le formateur**  Cette session a été préparée pour permettre aux participants d’avoir une première présentation des principaux éléments de preuve de l’affaire. Elle comprend cinq parties. La première partie présente une introduction des premiers éléments de preuve prévus dans le scénario du cas pratique. La deuxième partie présente les principaux éléments de l’affaire. La troisième partie aborde la perpétration de l’infraction pénale. La quatrième partie posera les bases du début de l’enquête et des travaux que les participants devront réaliser. La cinquième partie résume les informations présentées précédemment. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-9 | Ces diapositives constituent une introduction au scénario qui commence par la description de la Federal Bank of Atlantis (FBA) comme une banque internationale renommée, bien établie et réputée depuis longtemps. Ces caractéristiques devraient amener les participants à conclure que ce genre de banque ne devrait pas être impliquée dans des problèmes de quelque nature que ce soit, et encore moins rencontrer des difficultés du type de celles qui seront décrites plus loin dans ce document.  Profil des entreprises en cause dans le cas pratique : trois fichiers MS Word différents au format 97-2003 figurent parmi les ressources proposées. Ils devraient être mis à la disposition des participants sur papier ou, si les circonstances le permettent et que tous les participants ont un accès personnel à un ordinateur, sous forme électronique.  Divers documents d’appui sont fournis pour aborder le cas pratique : trois fichiers différents aux formats MS Word 97-2003 et Adobe Reader figurent parmi les ressources proposées. Ils devraient être mis à la disposition des participants sur papier ou, si les circonstances le permettent et que tous les participants ont un accès personnel à un ordinateur, sous forme électronique. | |
| 10-13 | Le développement de l’affaire porte sur 10 courriels qui sont des courriels réguliers faisant suite à un échange entre la FBA et le personnel d’UBP chargé des différents contrats et transactions pour l’impression d’obligations d’anniversaire.  Un contrat entre FBA et UBP est conclu à la suite de cet échange de courriels et met en perspective les grandes lignes du cadre commercial de l’opération. Il fixe également des étapes capitales pour la poursuite du développement de l’affaire.  Les relevés bancaires des entreprises suivent étroitement l’évolution des évènements dans cette affaire. Les participants pourront adopter l’approche consistant à « suivre l’argent à la trace » en analysant les relevés bancaires de la FBA et d’UBP.  Une facture pro forma authentique a été émise par UBP à la FBA pour que celle-ci règle une avance de 100 000. | |
| 14-16 | Diapositives sur le glossaire  L’enquête devra débuter dans les groupes de travail, les chefs de groupe et les membres commençant à travailler sur l’affaire à partir des informations de base fournies dans le dossier. | |
| 22 | Résumé  Il est recommandé de répéter toutes les étapes principales en donnant aux participants un peu plus de temps pour poser des questions et traiter la « réalité » du cas pratique.  Les formateurs devront être très bien informés à la fois sur le cas pratique et les mécanismes utilisés pour sa création, pour être prêts à répondre aux participants et à les aider. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. | | |

Leçon 2.3.1 (Défis liés aux preuves électroniques)

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.1 (Défis liés aux preuves électroniques) | | Durée : 90 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants * Un exemplaire papier du fichier de preuves mail11.doc et du fichier supplémentaire mail11(hash).doc pour chaque participant * Des exemplaires du Guide de la preuve électronique et du Guide du laboratoire forensique numérique du CdE | | |
| **But de la session :**  Le but de cette session est de donner aux participants l’occasion d’examiner les défis liés à l’utilisation des preuves électroniques présentées dans l’étude de cas sur la compromission des courriels professionnels. | | |
| **Objectifs :**  À l’issue de cette session, les participants seront en mesure :   * d’identifier les méthodes de validation des preuves électroniques ; * d’examiner les questions liées à l’admissibilité des preuves électroniques dans le cadre du procès ; * d’examiner et d’expliquer les atouts que présentent les fichiers contenant des preuves électroniques. | | |
| **Conseils pour le formateur**  L’objectif primordial de cette session est d’amener les participants à identifier les principaux problèmes d’admissibilité concernant les preuves électroniques et à comprendre qu’il est important qu’ils puissent les examiner dans la perspective de leur acceptation ou de leur rejet. Les participants sont initiés à la possibilité de vérifier les preuves en validant les empreintes numériques de différents fichiers. Certaines limites s’imposent au développement de la capacité à évaluer différents types de preuves, car les preuves provenant de courriels sont créées dans des fichiers MS Word et il n’y a pas de véritables objets à examiner. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-5 | Ces diapositives donnent des définitions des preuves électroniques et énoncent certaines de leurs spécificités. Il conviendra de rappeler aux participants que ces questions leur ont été présentées de manière plus détaillée dans le cadre du module d’introduction. | |
| 6-11 | Ces diapositives exposent, de manière plus détaillée que dans le module d’introduction, les considérations relatives à l’admissibilité des preuves électroniques. Le formateur devra s’assurer qu’il traite tous les aspects des diapositives. | |
| 12-13 | Ces diapositives rappellent aux participants que leur législation et leur pratique nationales priment sur les autres réglementations, et que le Conseil de l’Europe met à leur disposition des documents qui portent sur la question des preuves électroniques. Il conviendra d’encourager les participants à se les procurer. | |
| 14 | Le formateur devra poser les questions sur la diapositive et être prêt à examiner des exemples réels avant de passer aux preuves de l’étude de cas du cours. | |
| 15-16 | Ces diapositives énumèrent les documents utilisés dans l’étude de cas. Il conviendra de demander aux participants s’ils ont décelé des problèmes d’admissibilité concernant l’un de ces documents et le formateur devra engager une discussion à ce sujet. | |
| 17-22 | Ces diapositives sont le support de la démonstration de hachage de fichiers et de la façon dont ce processus permet d’identifier une petite modification apportée à un fichier. L’utilisation des fichiers mail11.doc et mail11(hash).doc est fondamentale dans cette session. Il est recommandé que le formateur fasse une démonstration du hachage et de la comparaison de deux fichiers entre lesquels il n’y a qu’une différence mineure. | |
| 23 | Cette diapositive présente certains des avantages des preuves électroniques, la manière dont elles peuvent être validées et des questions que les juges peuvent poser. | |
| 24-25 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  L’exercice pratique est abordé dans les diapositives 16 à 21. Le formateur devra envisager de faire une démonstration en direct de hachage sur les lignes affichées. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. On attendra des participants qu’ils s’impliquent activement dans la session. | | |

Leçon 2.3.2 – Demandes d’entraide judiciaire : modalités pratiques

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.2 – Demandes d’entraide judiciaire : modalités pratiques | | Durée : 90 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un tableau blanc * Des feutres pour tableau blanc (au moins deux pour chacune des couleurs suivantes : bleu, noir, rouge et vert) * Deux chevalets à feuilles mobiles équipés d’une réserve suffisante de papier * Des blocs-notes et des stylos pour les participants * Si possible, des exemples locaux de demandes d’entraide judiciaire (pour faciliter la visualisation et/ou la discussion sur les bonnes et les mauvaises pratiques) | | |
| **But de la session :**  L’objectif général de cette session est d’apporter des connaissances de base sur les principes de l’entraide judiciaire d’un point de vue pratique aux participants qui ne sont peut-être pas familiarisés à l’utilisation des demandes d’entraide judiciaire. Elle vise en outre à partager des conseils pratiques et des bonnes pratiques applicables quel que soit le pays d’origine du participant ou l’endroit où il a l’intention d’envoyer une demande d’entraide judiciaire.  Cette leçon s’intéressera à toutes les étapes de l’élaboration d’une requête, de la préparation à la rédaction, ainsi qu’à la façon d’aborder une demande étrangère afin de permettre son exécution.  Cette leçon devrait donner aux participants les outils de base et les réflexes nécessaires avant l’exercice de rédaction au cours duquel on leur demandera de rédiger un projet de demande d’entraide judiciaire dans une affaire de cybercriminalité. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de connaître ou de se rappeler les principes fondamentaux de l’entraide judiciaire appliquée à la cybercriminalité ; * d’identifier les bonnes pratiques dans la préparation et la rédaction d’une requête ; * d’adopter un point de vue constructif sur les requêtes étrangères reçues pour exécution. | | |
| **Conseils pour le formateur**  Cette session vise à préparer les participants à l’exercice de rédaction. Elle peut aussi être mise en œuvre comme un cours général adressé à tous les participants. Cette session ne présentera pas les règles juridiques de l’entraide judiciaire, qui dépendent de chaque pays, mais se concentrera sur les aspects pratiques ou les conseils qui peuvent aider les participants à rédiger leurs requêtes pour en garantir une meilleure exécution. Bien que la cybercriminalité et l’entraide judiciaire soient souvent liées, les juges ou les procureurs spécialisés en cybercriminalité ne connaissent pas toujours les règles qui régissent l’entraide judiciaire, et vice versa. Cette session vise à permettre aux participants de se faire une idée concrète de l’entraide judiciaire dans les affaires de cybercriminalité, qui peut être complétée par l’étude des règles théoriques applicables au pays concerné (en dehors de ce cours). | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3  obligatoires | Les premières diapositives exposent le programme et les objectifs de la session. Les objectifs de cette session sont expliqués aux participants et correspondent aux notions que ceux-ci devront avoir assimilées à la fin de ladite session. Ces objectifs peuvent être utilisés pour tester les connaissances acquises et permettre aux participants d’évaluer la formation. | |
| 4-7  obligatoires | Ces diapositives rappellent aux participants les principes généraux de l’entraide judiciaire et tentent de mettre en perspective ces principes généraux et les défis posés par les aspects technologiques. | |
| 8  facultative | Ce tableau tente de résumer les principales différences qui existent entre une « infraction traditionnelle » et une infraction commise dans le monde numérique, et les enjeux que cela représente. | |
| 9  obligatoire | Cette diapositive résume le défi posé par l’opposition entre souveraineté (principe) et efficacité/vitesse (absolument nécessaire en matière de cybercriminalité). | |
| 10  facultative | Cette diapositive détaille les enjeux de la situation décrite dans la diapositive 9. | |
| 11  obligatoire | Temps consacré aux questions et aux échanges avec les participants. | |
| 12-20  obligatoires  (sauf 19) | Ces diapositives traitent des étapes utiles à suivre pour mieux préparer une demande d’entraide judiciaire, notamment de l’utilisation des articles 29 et 35 de la Convention de Budapest (réseau 24/7 pour les demandes de conservation rapide). | |
| 21-52  obligatoires (sauf 23, 24, 26 to 40, 44, 45, 47 et 48) | Ces diapositives examinent les différentes étapes à respecter lors de la phase de rédaction d’une requête. Elles présentent des exemples régionaux (diapositives facultatives 23 et 24 concernant la décision d’enquête européenne dans l’Union européenne) ainsi qu’un modèle de formulaire de demande d’entraide judiciaire établi par le Conseil de l’Europe (diapositives facultatives 26 à 39), afin que les participants puissent visualiser un exemple de requête (il n’y a pas de modèle universel et obligatoire). Cette partie pourrait être complétée par d’autres exemples d’initiatives régionales ou locales.  Les diapositives ci-après passent en revue les différentes parties d’une requête à rédiger, à savoir le fondement juridique, les coordonnées utiles, le résumé des faits, les demandes spécifiques (diapositives 41 à 44). Des conseils sont donnés pour chacune de ces rubriques.  Ensuite, les diapositives 44 et 46 présentent des requêtes envoyées aux États-Unis.  Les diapositives 46 à 49 donnent d’autres conseils pour améliorer la rédaction. | |
| 53-61  obligatoires  (sauf 57, 58) | Ces diapositives visent à donner des conseils sur la façon d’examiner une demande étrangère dans la pratique, indépendamment des règles juridiques nationales applicables.  Les diapositives 59 à 61 (vides) devront être utilisées pour détailler certaines des règles nationales spécifiques concernant l’exécution des demandes étrangères. | |
| 62-64 | Ces diapositives présentent un résumé des objectifs qui devront être atteints à la fin de la leçon et proposent un temps de discussion avec les participants pendant lequel ils pourront poser des questions. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Le formateur est encouragé à vérifier les connaissances et la compréhension des participants en posant des questions pertinentes tout au long de la session, par exemple en citant des exemples locaux. | | |

Leçon 2.3.3 (Rédaction de requêtes)

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.3 (Rédaction de requêtes) | | Durée : 60 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de fournir aux participants des lignes directrices sur les requêtes concernant l’exercice de pouvoirs d’enquête ou de pouvoirs procéduraux prévus par la Convention de Budapest. Cette leçon présentera également des informations sur ce que les magistrats ou les autres autorités compétentes devraient attendre des services répressifs ou des procureurs qui déposent une requête relative à des pouvoirs procéduraux. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de comprendre la manière dont les différents systèmes juridiques permettent de solliciter l’exercice de pouvoirs procéduraux ; * de reconnaître les considérations particulières relatives à la rédaction de requêtes concernant l’exercice de pouvoirs procéduraux ou de pouvoirs d’enquête en matière de preuve électronique ; * de comprendre certaines des considérations et des garanties qu’il convient de prendre en compte lors d’une demande concernant l’exercice de pouvoirs procéduraux. | | |
| **Conseils pour le formateur**  De nombreuses juridictions exigent que les agents des services répressifs, les procureurs ou d’autres personnes chargées d’enquêter sur des infractions pénales s’adressent à une autorité judiciaire ou à une autre autorité compétente pour lui demander l’autorisation d’exercer des pouvoirs procéduraux. Le formateur sera tenu d’expliquer que certaines juridictions exigent des demandes écrites alors que d’autres attendent des demandes orales pour obtenir l’autorisation de mettre en œuvre des mesures procédurales ou d’enquête. Il devra également veiller à ce que cette leçon soit dispensée en gardant à l’esprit les conditions et les garanties prévues à l’article 15 de la Convention de Budapest. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-8 | Ces diapositives présentent un résumé de certains aspects fondamentaux de la Convention de Budapest qui sont pertinents pour la leçon. Elles comprennent une liste des différents pouvoirs procéduraux prévus par la Convention de Budapest. Le formateur devra également utiliser ces diapositives pour rappeler les notions énoncées à l’article 15 de la Convention de Budapest. Il devra par ailleurs faire la distinction entre les processus de demande d’autorisation d’exercice de pouvoirs procéduraux dans différents systèmes juridiques. Cette partie prévoit également une brève introduction aux parties 2, 3 et 4 de la session – l’objet (« quoi ? »), la manière (« comment ? ») et le motif (« pourquoi ? ») en ce qui concerne les demandes d’exercice de pouvoirs procéduraux. | |
| 9-22 | Ces diapositives portent sur l’objet (« quoi ? ») des demandes d’exercice de pouvoirs procéduraux. Elles traitent à la fois de la question des données et de celle des personnes visées par une demande d’exercice de pouvoirs procéduraux. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de la manière dont les personnes et les données qui font l’objet d’une demande sont identifiées. | |
| 23-54 | Ces diapositives portent sur la manière (« comment ? ») de formuler des demandes d’exercice de pouvoirs procéduraux. Elles expliquent comment les pouvoirs procéduraux sont censés être appliqués. Ce faisant, elles couvrent à la fois les aspects techniques de la manière dont les pouvoirs procéduraux doivent être appliqués (c’est-à-dire quels pouvoirs procéduraux seront exercés dans le cadre de différentes enquêtes et quelles mesures techniques seront prises pour exercer ces pouvoirs) et les aspects relatifs à la protection (c’est-à-dire les conditions et les garanties au moment de la demande, pendant l’exécution et après l’exécution). Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de mesures techniques et de protection qui peuvent être énoncées dans une requête. | |
| 55-66 | Ces diapositives portent sur le motif (« pourquoi ? ») des demandes d’exercice de pouvoirs procéduraux. Cette partie de la session est axée sur l’explication des motifs pour lesquels des demandes d’exercice de pouvoirs procéduraux sont formulées. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de motifs qui peuvent être énoncés et détaillés par la suite dans une requête. | |
| 67-77 | Ces diapositives présentent certaines formalités à respecter pour déposer des requêtes écrites dans différentes juridictions. Le formateur pourra envisager d’adapter ces diapositives pour s’aligner sur les exigences locales. | |
| 78-80 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. | | |

Leçon 2.3.4 (Demande d’exercice de pouvoirs procéduraux)

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.4 (Demande d’exercice de pouvoirs procéduraux) | | Durée : 60 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de fournir aux participants des lignes directrices sur les requêtes concernant l’exercice de pouvoirs d’enquête ou de pouvoirs procéduraux prévus par la Convention de Budapest. Cette leçon présentera également des informations sur ce que les magistrats ou les autres autorités compétentes devraient attendre des services répressifs ou des procureurs qui déposent une requête relative à des pouvoirs procéduraux. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de comprendre la manière dont les différents systèmes juridiques permettent de solliciter l’exercice de pouvoirs procéduraux ; * de reconnaître les considérations particulières relatives à la rédaction de requêtes concernant l’exercice de pouvoirs procéduraux ou de pouvoirs d’enquête en matière de preuve électronique ; * de comprendre certaines des considérations et des garanties qu’il convient de prendre en compte lors d’une demande concernant l’exercice de pouvoirs procéduraux. | | |
| **Conseils pour le formateur**  De nombreuses juridictions exigent que les agents des services répressifs, les procureurs ou d’autres personnes chargées d’enquêter sur des infractions pénales s’adressent à une autorité judiciaire ou à une autre autorité compétente pour lui demander l’autorisation d’exercer des pouvoirs procéduraux. Le formateur sera tenu d’expliquer que certaines juridictions exigent des demandes écrites alors que d’autres attendent des demandes orales pour obtenir l’autorisation de mettre en œuvre des mesures procédurales ou d’enquête. Il devra également veiller à ce que cette leçon soit dispensée en gardant à l’esprit les conditions et les garanties prévues à l’article 15 de la Convention de Budapest. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-8 | Ces diapositives présentent un résumé de certains aspects fondamentaux de la Convention de Budapest qui sont pertinents pour la leçon. Elles comprennent une liste des différents pouvoirs procéduraux prévus par la Convention de Budapest. Le formateur devra également utiliser ces diapositives pour rappeler les notions énoncées à l’article 15 de la Convention de Budapest. Il devra par ailleurs faire la distinction entre les processus de demande d’autorisation d’exercice de pouvoirs procéduraux dans différents systèmes juridiques. Cette partie prévoit également une brève introduction aux parties 2, 3 et 4 de la session – l’objet (« quoi ? »), la manière (« comment ? ») et le motif (« pourquoi ? ») en ce qui concerne les demandes d’exercice de pouvoirs procéduraux. | |
| 9-22 | Ces diapositives portent sur l’objet (« quoi ? ») des demandes d’exercice de pouvoirs procéduraux. Elles traitent à la fois de la question des données et de celle des personnes visées par une demande d’exercice de pouvoirs procéduraux. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de la manière dont les personnes et les données qui font l’objet d’une demande sont identifiées. | |
| 23-49 | Ces diapositives portent sur la manière (« comment ? ») de formuler des demandes d’exercice de pouvoirs procéduraux. Elles expliquent comment les pouvoirs procéduraux sont censés être appliqués. Ce faisant, elles couvrent à la fois les aspects techniques de la manière dont les pouvoirs procéduraux doivent être appliqués (c’est-à-dire quels pouvoirs procéduraux seront exercés dans le cadre de différentes enquêtes et quelles mesures techniques seront prises pour exercer ces pouvoirs) et les aspects relatifs à la protection (c’est-à-dire les conditions et les garanties au moment de la demande, pendant l’exécution et après l’exécution). Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de mesures techniques et de protection qui peuvent être énoncées dans une requête. | |
| 50-61 | Ces diapositives portent sur le motif (« pourquoi ? ») des demandes d’exercice de pouvoirs procéduraux. Cette partie de la session est axée sur l’explication des motifs pour lesquels des demandes d’exercice de pouvoirs procéduraux sont formulées. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de motifs qui peuvent être énoncés et détaillés par la suite dans une requête. | |
| 62-64 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. | | |

Leçon 2.3.4 (Conduite d’audiences et rédaction d’ordonnances)

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.4 (Conduite d’audiences et rédaction d’ordonnances) | | Durée : 90 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de fournir aux participants les directives nécessaires pour les aider à conduire des audiences sur des demandes d’exercice de pouvoirs procéduraux et de rédiger des ordonnances permettant d’exercer ces pouvoirs. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de reconnaître les diverses considérations relatives à la conduite d’audiences sur l’exercice de pouvoirs d’enquête ; * d’expliquer les conditions et les garanties procédurales applicables qui devraient être prises en compte lors des audiences ; * d’identifier les compétences judiciaires importantes qui peuvent être mises en œuvre pour mener efficacement les audiences ; * de comprendre les considérations essentielles relatives aux ordonnances autorisant l’exercice de pouvoirs procéduraux en matière de preuve électronique. | | |
| **Conseils pour le formateur**  La Convention de Budapest charge les États de mettre en œuvre des conditions et des garanties adéquates en ce qui concerne l’exercice des pouvoirs procéduraux. Certaines juridictions exigent qu’un agent des services répressifs ou qu’un procureur dépose une demande officielle et qu’un agent indépendant (en général un magistrat) tienne une audience pour examiner cette requête et établisse une ordonnance en conséquence. D’autres juridictions imposent qu’un agent indépendant (en général un magistrat) examine une demande d’application des pouvoirs procéduraux et délivre une autorisation verbale. Le but de cette session est de fournir aux participants les compétences générales qui leur permettront de statuer sur ces requêtes et d’établir des ordonnances. Cette leçon devra être dispensée en gardant à l’esprit que les participants se prêteront à un exercice pratique qui impliquera la tenue d’une audience. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-7 | Ces diapositives présentent une courte introduction aux audiences, qui comprend une brève description de la façon dont certains systèmes juridiques imposent que des audiences soient tenues sur les demandes d’exercice de pouvoirs procéduraux, alors que d’autres peuvent permettre à des juges d’accorder des autorisations sans conduire d’audience. Cette partie présente également un rappel des conditions et des garanties applicables. | |
| 8-25 | Ces diapositives portent sur l’ensemble du processus d’audience, de la préparation à la phase d’interrogation et de demande de renseignements supplémentaires. Le formateur devra présenter aux participants les différentes phases d’une audience (préparation, présentation, identification des problèmes, éléments de preuve, interrogation et recherche de renseignements supplémentaires, par exemple). Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples pertinents. | |
| 26-47 | Ces diapositives portent sur des compétences qui concernent le processus de conduite des audiences. Compte tenu de la sensibilité de ce sujet, le formateur devra s’assurer que les participants sont informés que cette partie de la session se fonde sur les bonnes pratiques judiciaires identifiées par les juges au Royaume-Uni, mais adaptées à la nature spécifique des requêtes relatives à des preuves électroniques. Cette partie comprend également des exemples pratiques de mise en œuvre de certaines compétences judiciaires dans le cadre de l’étude de cas sur la simulation d’enquête. | |
| 48-72 | Ces diapositives portent sur la rédaction d’ordonnances à l’issue du processus d’audience. Elles s’appuient sur les concepts abordés à l’étape de l’audience et précisent divers détails qui peuvent être inclus dans l’ordonnance. Le formateur devra expliquer que les diapositives ne fournissent que certains exemples et conditions non spécifiques, mais que le contenu de toute ordonnance relative à l’exercice de pouvoirs procéduraux dépendra entièrement des éléments de l’affaire en question. | |
| 73-75 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Une fois la leçon terminée, il est attendu que les participants se prêtent à une simulation d’audience. Ils seront divisés en petits groupes d’un nombre pair de personnes. Chaque groupe se verra attribuer une requête fictive pour la perquisition et la saisie de données informatiques et sera divisé en deux sous-groupes (les agents des services répressifs, les procureurs et les juges, par exemple). Chaque sous-groupe tiendra une audience simulée pour examiner cette requête, à l’issue de laquelle le sous-groupe de juges devra rédiger une ordonnance. Une fois cet exercice terminé, les sous-groupes inverseront les rôles et l’exercice sera répété.  À l’issue de l’exercice, le formateur sera chargé de communiquer un retour d’informations aux participants. Il prendra la forme suivante :   * Sujet abordé : identifier les éléments à prendre en compte * Retour en arrière : revenir sur le thème désigné * Motif : justifier le choix du thème désigné * Solution : expliquer comment améliorer les performances * Démonstration : mise en œuvre de la solution * Reproduction : demander de renouveler l’exercice sur le thème désigné | | |
| **Évaluation/Contrôle des connaissances**  Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. Les connaissances des participants seront examinées dans le prochain exercice. | | |

Leçon 2.3.4 (Demande d’exercice de pouvoirs procéduraux)

|  |  |  |
| --- | --- | --- |
| Leçon 2.3.4 (Demande d’exercice de pouvoirs procéduraux) | | Durée : 90 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est de fournir aux participants des lignes directrices sur les requêtes concernant l’exercice de pouvoirs d’enquête ou de pouvoirs procéduraux prévus par la Convention de Budapest. Cette leçon présentera également des informations sur ce que les magistrats ou les autres autorités compétentes devraient attendre des services répressifs ou des procureurs qui déposent une requête relative à des pouvoirs procéduraux. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de comprendre la manière dont les différents systèmes juridiques permettent de solliciter l’exercice de pouvoirs procéduraux ; * de reconnaître les considérations particulières relatives à la rédaction de requêtes concernant l’exercice de pouvoirs procéduraux ou de pouvoirs d’enquête en matière de preuve électronique ; * de comprendre certaines des considérations et des garanties qu’il convient de prendre en compte lors d’une demande concernant l’exercice de pouvoirs procéduraux. | | |
| **Conseils pour le formateur**  De nombreuses juridictions exigent que les agents des services répressifs, les procureurs ou d’autres personnes chargées d’enquêter sur des infractions pénales s’adressent à une autorité judiciaire ou à une autre autorité compétente pour lui demander l’autorisation d’exercer des pouvoirs procéduraux. Le formateur sera tenu d’expliquer que certaines juridictions exigent des demandes écrites alors que d’autres attendent des demandes orales pour obtenir l’autorisation de mettre en œuvre des mesures procédurales ou d’enquête. Il devra également veiller à ce que cette leçon soit dispensée en gardant à l’esprit les conditions et les garanties prévues à l’article 15 de la Convention de Budapest. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 4-8 | Ces diapositives présentent un résumé de certains aspects fondamentaux de la Convention de Budapest qui sont pertinents pour la leçon. Elles comprennent une liste des différents pouvoirs procéduraux prévus par la Convention de Budapest. Le formateur devra également utiliser ces diapositives pour mettre à jour les notions énoncées à l’article 15 de la Convention de Budapest. Il devra par ailleurs faire la distinction entre les processus de demande d’autorisation d’exercice de pouvoirs procéduraux dans différents systèmes juridiques. Cette partie prévoit également une brève introduction aux parties 2, 3 et 4 de la session – l’objet (« quoi ? »), la manière (« comment ? ») et le motif (« pourquoi ? ») en ce qui concerne les demandes d’exercice de pouvoirs procéduraux. | |
| 9-22 | Ces diapositives portent sur l’objet (« quoi ? ») des demandes d’exercice de pouvoirs procéduraux. Elles traitent à la fois de la question des données et de celle des personnes visées par une demande d’exercice de pouvoirs procéduraux. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de la manière dont les personnes et les données qui font l’objet d’une demande sont identifiées. | |
| 23-49 | Ces diapositives portent sur la manière (« comment ? ») de formuler des demandes d’exercice de pouvoirs procéduraux. Elles expliquent comment les pouvoirs procéduraux sont censés être appliqués. Ce faisant, elles couvrent à la fois les aspects techniques de la manière dont les pouvoirs procéduraux doivent être appliqués (c’est-à-dire quels pouvoirs procéduraux seront exercés dans le cadre de différentes enquêtes et quelles mesures techniques seront prises pour exercer ces pouvoirs) et les aspects relatifs à la protection (c’est-à-dire les conditions et les garanties au moment de la demande, pendant l’exécution et après l’exécution). Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de mesures techniques et de protection qui peuvent être énoncées dans une requête. | |
| 50-61 | Ces diapositives portent sur le motif (« pourquoi ? ») des demandes d’exercice de pouvoirs procéduraux. Cette partie de la session est axée sur l’explication des motifs pour lesquels des demandes d’exercice de pouvoirs procéduraux sont formulées. Les diapositives s’appuient sur l’étude de cas sur la simulation d’enquête pour donner des exemples de motifs qui peuvent être énoncés et détaillés par la suite dans une requête. | |
| 62-64 | Le formateur devra récapituler les objectifs de la session avec les participants et leur donner la possibilité de poser toutes les questions relatives au matériel abordé dans cette session. | |
| **Exercices pratiques**  Aucun exercice pratique n’est prévu pour cette session. | | |
| **Évaluation/Contrôle des connaissances**  Aucun contrôle formel des connaissances n’est prévu pour cette session. Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. | | |

Leçon 2.4.2 (Retour d’informations sur la simulation d’audience)

|  |  |  |
| --- | --- | --- |
| Leçon 2.4.2 (Retour d’informations sur la simulation d’audience) | | Durée : 90 minutes |
| **Matériel nécessaire :**   * Un PC/portable équipé de versions de logiciels compatibles avec le matériel préparé * Un projecteur et un écran * Un accès à internet (si possible) * Des blocs-notes et des stylos pour les participants | | |
| **But de la session :**  Le but de cette session est d’enseigner aux formateurs comment examiner et donner un retour d’informations aux participants sur leurs performances lors de l’exercice de simulation d’audience portant sur une demande d’exercice de mesures d’enquête. | | |
| **Objectifs :**  À la fin de la leçon, les participants seront en mesure :   * de comprendre comment évaluer et examiner les performances des participants lors de l’exercice de simulation d’audience et d’examen des demandes d’exercice de mesures d’enquête ; * de comprendre comment mettre en œuvre chacune des six phases du processus d’examen lorsque l’on communique un retour d’informations aux participants. | | |
| **Conseils pour le formateur**  Les participants à la formation judiciaire avancée se prêteront à un exercice impliquant la tenue d’une audience portant sur une demande d’exercice de mesures d’enquête. Un retour d’informations clair et un examen des performances sont essentiels au succès d’un tel exercice. Ce module présente une méthode issue des bonnes pratiques pour évaluer le niveau de performance des participants. | | |
| **Contenu de la session** | | |
| **No des diapositives** | **Contenu** | |
| 1-3 | Les premières diapositives présentent la structure et les objectifs de cette session. Les participants auront l’occasion de poser des questions préliminaires sur la structure et les objectifs de la session. | |
| 3-5 | Ces diapositives présentent une introduction au processus de retour d’informations que les formateurs devront mettre en œuvre à l’issue de la simulation d’audience. Les diapositives divisent le processus d’examen en deux volets (retour d’informations et suggestions constructives) et énumèrent également les six étapes du processus qui sont traitées plus en détail dans les diapositives suivantes. | |
| 6-9 | Ces diapositives se rapportent au premier volet du processus d’examen, qui consiste à fournir un retour d’informations aux participants. Cette étape consiste à revenir sur les performances des participants. Ce volet est composé des phases intitulées « sujet abordé », « retour en arrière » et « motif ». Il est demandé au formateur de traiter chacun de ces stades. | |
| 10-15 | Ces diapositives se rapportent au second volet du processus d’examen, qui consiste à proposer des suggestions constructives aux participants. Elles consistent en une réflexion prospective sur la façon de traiter les aspects relatifs aux performances des participants qui ont été évoqués dans le retour d’informations. Ce volet est composé des phases intitulées « solution », « démonstration » et « reproduction ». Il est demandé au formateur de traiter chacun de ces stades. | |
| **Exercices pratiques**  Ce module a été mis au point pour fournir une formation aux formateurs sur la manière de communiquer un retour d’informations aux participants après une simulation d’audience. Les formateurs seront tenus de mener à bien dans la pratique le processus d’examen à l’issue de la simulation d’audience de chaque formation. | | |
| **Évaluation/Contrôle des connaissances**  Le formateur est encouragé à vérifier l’acquisition des connaissances et la compréhension en posant des questions pertinentes tout au long de la session. Aucune évaluation formelle n’est requise pour cette session. | | |

6. Évaluation

L’évaluation est une partie importante de toute formation et, à ce titre, devrait se voir attribuer une tranche de temps suffisante pour que les participants puissent communiquer un retour d’informations sur leur expérience d’apprentissage.

Le présent cours a été conçu comme un cours générique et, par conséquent, une grande partie du matériel didactique se base sur PowerPoint sans faire appel à une pléthore d’exercices pratiques comme c’est normalement le cas pour ce type d’apprentissage.

Un formulaire d’évaluation a été élaboré et est fourni comme modèle pouvant être adapté à la situation locale. Les formateurs devront s’assurer que les formulaires sont remplis et transmis aux organismes nationaux compétents afin que des améliorations puissent être apportées dans la dispense des futurs cours.

7. Appréciation

Aucune appréciation n’a été demandée pour ce cours, mais ceux qui le dispenseront à l’avenir, en particulier dans les pays où le cours est susceptible de faire partie d’un programme qui prévoit ce type de procédure, pourraient reconsidérer la question. À supposer qu’un système d’appréciation soit instauré, il conviendrait de respecter la méthodologie en usage dans le pays concerné.

1. Le projet conjoint Union européenne/Conseil de l’Europe Cybercrime@IPA (Coopération régionale en matière de justice pénale : Renforcement des capacités dans la lutte contre la cybercriminalité) vise à renforcer les capacités des autorités de justice pénale dans les Balkans occidentaux et en Turquie pour coopérer efficacement dans la lutte contre la cybercriminalité. [↑](#footnote-ref-1)
2. Cette désignation ne préjuge en rien des positions concernant le statut du territoire et est conforme à la Résolution 1244 du Conseil de sécurité des Nations Unies ainsi qu’à l’Avis de la Cour internationale de justice sur la Déclaration d’indépendance du Kosovo. [↑](#footnote-ref-2)