Le Centre Africain de Recherche en Intelligence Artificielle (CARIA) et la Commission Economique des Nations Unies pour l'Afrique (UNCEA)

Orgnisent

Le seminaire de formation des corps judiciaire et de répression sur la Cybercriminalité et les techniques fondamentales d'enquête criminelle dans le Numérique

Brazzaville, 8-10 octobre 2024 /
Langue: Français

NOTE CONCEPTUELLE

I. Contexte et Justification

L'Afrique a connu une transformation numérique significative au cours de la dernière décennie, portée par l'adoption généralisée du mobile, une connectivité Internet améliorée et un secteur technologique florissant. À l'échelle mondiale, l'économie numérique représente désormais plus de 15 % du PIB, avec une croissance 2,5 fois plus rapide que l'économie traditionnelle au cours de la dernière décennie . McKinsey prédit que le secteur fintech africain générera près de 30 milliards de dollars de revenus d'ici 2025 . En outre, les projections de la Coopération financière internationale et de Google suggèrent que l'économie Internet de l'Afrique pourrait contribuer à son PIB à hauteur de 180 milliards de dollars d'ici 2025, et qu'elle pourrait atteindre 712 milliards de dollars d'ici 2050 . L'Accord de libre-échange continental africain (ZLECAf), qui couvre 55 pays avec un PIB combiné de 3 400 milliards de dollars, vise à établir la plus grande zone de libre-échange au monde. Il a le potentiel de sortir 30 millions de personnes de la pauvreté et de contribuer à hauteur de 459 milliards de dollars au PIB de l'Afrique .

Cependant, la numérisation rapide de l'Afrique l'expose également à une cybercriminalité importante. Des mesures inadéquates ont rendu le continent vulnérable aux cybermenaces, la cybercriminalité à elle seule aurait réduit le PIB de plus de 10 % en 2021, équivalant à une perte de 4,12 milliards de dollars . La sophistication croissante des cybermenaces, notamment les ransomwares et les malwares, constitue un défi de taille . Ce problème est particulièrement aigu dans des pays comme le Nigeria, le Kenya et l'Afrique du Sud, qui ont subi des pertes substantielles dues aux cyberattaques . Ces statistiques soulignent l'importance cruciale pour les pays de donner la priorité aux investissements dans des mesures globales de cybersécurité et de cybercriminalité, notamment des infrastructures solides, des programmes d'éducation et de formation.

Au niveau mondial, le Comité ad hoc sur la cybercriminalité, créé par l'Assemblée générale des Nations Unies, négocie actuellement une convention internationale globale visant à lutter contre l'utilisation des technologies de l'information et des communications (TIC) à des fins criminelles. Cette initiative vise à

créer un cadre juridique unifié qui répond à la menace croissante de la cybercriminalité, en harmonisant les efforts entre les différentes juridictions.

La cybercriminalité transcende souvent les frontières nationales, ce qui nécessite une collaboration transparente entre les services répressifs du monde entier. Cette coopération doit être étayée par une compréhension approfondie des lois et protocoles transfrontaliers. De plus, les enquêtes numériques doivent donner la priorité à la protection des droits et libertés des individus.

Pour lutter efficacement contre la cybermenace croissante, il est crucial de doter les forces de l'ordre et le pouvoir judiciaire des compétences et des connaissances nécessaires pour répondre à cette préoccupation croissante. Cela nécessite de leur fournir une formation complète et des ressources pour rester au courant des dernières tendances et techniques en matière de cybercriminalité, ainsi que de s'assurer qu'ils comprennent les cadres et procédures juridiques nécessaires pour enquêter et poursuivre efficacement les cybercriminels.

Pour y parvenir, les enquêteurs ont besoin d'une formation complète pour garantir qu'ils respectent les procédures légales et minimiser le risque de violations des droits humains. En outre, la nature en constante évolution des technologies numériques exige une formation continue pour que les enquêteurs se tiennent au courant des dernières tactiques et techniques de cybercriminalité, alors que les cybercriminels s'adaptent et innovent continuellement pour échapper à la détection.

Dans ce contexte, sous les auspices de la Déclaration de Lomé sur la cybersécurité et la lutte contre la cybercriminalité, cet atelier vise à doter les membres du corps judiciaire et des forces de l'ordre des connaissances et des compétences nécessaires pour lutter efficacement contre la cybercriminalité.

II. Objectif:

Cet atelier de formation vise à fournir au corps judiciaire et aux forces de l'ordre les compétences et connaissances essentielles pour faire face aux complexités de la cybercriminalité. En favorisant une approche collaborative et éclairée, nous pouvons améliorer notre capacité collective à protéger les espaces numériques et à garantir la justice ;

- **Améliorer la compréhension de la cybercriminalité** : fournir un aperçu complet des différents types de cybercriminalité, de leurs méthodologies et de leurs impacts.
- **Cadre juridique** : discutez des cadres juridiques nationaux et internationaux régissant la cybercriminalité, en vous concentrant sur les développements récents, notamment l'AHC sur la cybercriminalité et les études de cas.
- **Techniques d'enquête** : présenter des techniques et des outils avancés pour enquêter sur la cybercriminalité, y compris la collecte de preuves, la criminalistique numérique et l'analyse de données.
- **Coordination et collaboration inter-agences** : Promouvoir une coordination et une collaboration efficaces entre les organes judiciaires, les organismes chargés de l'application de la loi et les autres parties prenantes. Apprendre les mécanismes de partage d'informations et de coordination des enquêtes transfrontalières
- **Soutien aux victimes** : mettez en avant les stratégies visant à soutenir les victimes de la cybercriminalité et à garantir la protection de leurs droits et intérêts.

III. Resultats Attendus

- **Compétences techniques améliorées :** le pouvoir judiciaire et les forces de l'ordre acquerront une compréhension approfondie des TIC, permettant une analyse efficace et précise des preuves numériques.
- **Capacité à mener des enquêtes numériques :** les forces de l'ordre apprendront des techniques d'enquête sur les délits numériques, telles que la collecte de preuves numériques, l'analyse des journaux de serveur et la surveillance des réseaux, tout en respectant les procédures juridiques et les meilleures pratiques internationales.
- **Renforcement de la collaboration interinstitutionnelle :** les participants développeront des compétences pour travailler en collaboration avec des agences nationales et internationales, facilitant l'échange d'informations et la coordination des enquêtes transfrontalières.
- **Sensibilisation aux aspects juridiques :** L'organe judiciaire acquerra une connaissance des lois et réglementations spécifiques à la cybercriminalité, permettant un meilleur traitement des dossiers avec une compréhension des nuances techniques et juridiques.
- **Préservation des preuves :** les enquêteurs apprendront des techniques pour collecter, préserver et présenter des preuves électroniques au tribunal, garantissant ainsi leur admissibilité et leur intégrité.
- **Réduction de la criminalité numérique :** grâce à des compétences accrues, les forces de l'ordre interviendront plus rapidement et plus efficacement pour prévenir et résoudre les incidents de cybercriminalité, réduisant ainsi leur fréquence et leur impact.
- **Protection des droits et libertés :** les enquêtes numériques respecteront les droits et libertés des individus, réduisant ainsi les risques de violations des droits de l'homme.
- **Confiance renforcée dans le système judiciaire :** Une meilleure gestion des affaires de cybercriminalité augmentera la confiance du public dans la capacité du système judiciaire à protéger les citoyens contre les menaces numériques.
- **Développement des capacités institutionnelles :** les institutions judiciaires et les organismes chargés de l'application de la loi développeront de solides capacités internes pour gérer les cybermenaces de manière autonome et durable.
- **Adaptation aux évolutions technologiques :** La formation continue permettra aux participants de rester à jour avec les dernières technologies et méthodes utilisées par les cybercriminels, garantissant une réponse adaptée et proactive. Comprendre et interpréter les lois nationales sur la cybercriminalité, adopter la culture du partage des connaissances et s'engager dans une conversation mondiale sur la cybercriminalité ;

IV. Bénéficiaires Ciblés :

- Membres du corps judiciaire (juges, procureurs, conseillers juridiques) ;
- Agents chargés de l'application des lois (police, enquêteurs, unités de cybercriminalité) ;
- Des représentants des agences gouvernementales compétentes telles que le ministère de la Justice ;
- Les professionnels de la cybersécurité et les acteurs de la justice en général , tels que les assistants techniques, les experts commis d'office et les assistants juridiques ;
- Formateurs des institutions nationales de formation judiciaire (formation de formateurs).

V. Méthodologie :

- **Cours Théoriques :** Sessions interactives couvrant les aspects légaux, techniques et pratiques de la cybercriminalité.
- **Ateliers Pratiques :** Exercices pratiques et études de cas pour une application concrète des connaissances.
- **Experts Invités :** Interventions de professionnels expérimentés dans le domaine de la cybercriminalité.
- **Évaluations et Feedback :** Tests et évaluations pour mesurer l'acquisition des compétences et retour d'expérience pour améliorer la formation continue.

VI. Format de l'atelier :

Jour 1 : Comprendre la cybercriminalité et les cadres juridiques

- **Séance d'ouverture :** Mot de bienvenue et présentations
- **Discours d'ouverture :** L'importance cruciale de la cybersécurité dans le monde d'aujourd'hui
- **Session 1 :** Aperçu de la cybercriminalité – types, tendances, impacts et prévention
- **Session 2** : Cadres juridiques nationaux, sous-régionaux, continentaux et internationaux pour lutter contre la cybercriminalité
- **Exercice théorique** : Études de cas sur les poursuites en matière de cybercriminalité – défis et bonnes pratiques

Jour 2 : Techniques et outils d'enquête

- **Session 3** : Forensique numérique - outils, techniques et méthodologies
- **Session 4** : Analyse des données et collecte de preuves dans les enquêtes sur la cybercriminalité
- **Atelier pratique** : Utiliser un logiciel médico-légal pour l'analyse des données et la collecte de preuves
- **Exercice de simulation** : Enquêtes sur la cybercriminalité - exercices basés sur des scénarios

Jour 3 : Collaboration

- **Session 5 :** Collaboration inter-agences et partage d'informations dans les enquêtes sur la cybercriminalité
- **Session 6 :** Protéger les droits et les intérêts des victimes de la cybercriminalité – implications juridiques et sociales
- **Activité de groupe :** Développer un cadre collaboratif pour la prévention et la réponse à la cybercriminalité
- **Séance de clôture :** résumé et voie à suivre - mise en œuvre des enseignements tirés et des meilleures pratiques

VII. Contacts

Mme Sorene ASSEFA,
United Nations Economic Commission for Africa
Téléphone : +27(78)505 4834
Email : sorene@un.org

Dr Eric Armel NDOUMBA,
Telecommunications Advisor to the Minister and Technical Coordinator of the African Artificial Intelligence Research Center
Téléphone : +242 06 455 5663
Email : eric.ndoumba@postetelecom.gouv.cg
Email : eric.ndoumba@caria.cg