

DEUXIÈME FORUM AFRICAIN SUR LA CYBERCRIMINALITE

Politiques et législation en matière de
cybercriminalité, enquêtes,
coopération internationale

Programme de la conférence

En ligne, du 28 au 29 juin 2021

Organisé et financé par :



Financé
par l'Union européenne
et le Conseil de l'Europe



Mis en œuvre
par le Conseil de l'Europe

Aperçu

Contexte et justification

À mesure que le monde évolue vers une nouvelle "normalité", l'utilisation des technologies de l'information et la dépendance à leur égard sont de plus en plus répandues dans la société. Le ciblage et l'exploitation illégale des systèmes informatiques et des logiciels malveillants sont également devenus de plus en plus courants. La pandémie mondiale de COVID-19 a entraîné une augmentation sans précédent des activités illégales liées à la cybercriminalité¹. Les infractions impliquant des ordinateurs ont connu une croissance rapide, tant en nombre qu'en sophistication, et de manière encore plus alarmante depuis le début de la pandémie.

Conformément à cette tendance mondiale, le continent africain - la région du monde qui connaît la croissance la plus rapide en termes de pénétration de l'internet et d'utilisation des services financiers mobiles - est devenu une zone de plus en plus attrayante pour les cybercriminels. L'élaboration de contre-mesures efficaces s'est avérée difficile dans le contexte mondial, tout comme l'alignement de la législation, des stratégies et des politiques de manière cohérente et harmonisée. Comme le montrent des rapports récents^{2,3,4} l'hétérogénéité des cadres juridiques, l'absence de stratégies nationales et les infrastructures d'information encore peu sécurisées dans un certain nombre de pays ont fait de la région africaine une cible vulnérable pour les activités cybercriminelles. Ces activités ont un impact direct non seulement sur les citoyens, mais aussi - et c'est le plus inquiétant - sur la stabilité sociale des États.

De nombreux pays d'Afrique ont fait de l'élaboration de lois et de politiques en matière de cybercriminalité une priorité de haut niveau, capables de criminaliser efficacement ces actes illégaux et de permettre une coopération internationale efficace entre les autorités de justice pénale, conformément aux normes internationales. Dans cet effort, un point d'attention majeur a été la nécessité de respecter les droits fondamentaux des individus - qu'ils soient suspects ou victimes, tout en assurant la nécessité et la proportionnalité dans l'application de la justice pénale. Dans un tel contexte, les agents des services répressifs, les procureurs, les magistrats et les juges sont appelés à exercer leurs rôles dans des environnements de plus en plus complexes, qui nécessitent des compétences actualisées et des outils adéquats, tant techniques que juridiques.

Ces dernières années, un nombre croissant d'organisations internationales et régionales ont apporté leur soutien à cette entreprise. Cette coopération indispensable est impérative. Il est devenu essentiel d'unir nos forces entre nous et avec les autorités nationales, de développer des synergies de manière cohérente et de mettre en place des initiatives efficaces de renforcement des capacités.

Les avantages d'une telle approche coopérative ont été reconfirmés à l'occasion du premier Forum africain sur la cybercriminalité, organisé en octobre 2018 par la Commission de l'Union africaine à Addis-Abeba, et soutenu de manière substantielle par le Conseil de l'Europe, INTERPOL, l'Union européenne, l'UNODC, le Secrétariat du Commonwealth, le FCO du Royaume-Uni, le Département d'État des États-Unis et le Département de la justice des États-Unis.

Les plus de 50 pays africains qui ont participé à cet événement ont convenu de la nécessité d'encourager la poursuite de la coopération et l'échange d'expériences au sein du continent africain, établissant ainsi le Forum africain sur la cybercriminalité comme une initiative récurrente, qui sera organisée tous les deux ans. Le deuxième Forum africain sur la cybercriminalité s'appuiera sur les

¹ Microsoft Exploitant une crise : comment les cybercriminels se sont comportés pendant l'épidémie. [EN] <https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/>

² Nir Kshetri (2019) " Cybercrime and Cybersecurity in Africa" *Journal of Global Information Technology Management*, 22:2, 77-81

³ Africa Portal, 5 février 2020. [EN] [Cyber crime and data privacy: how Africa can up its game](#)

⁴ CGTN, [EN] [Unveiling the Cost of Cybercrime in Africa](#), 27 octobre 2020

conclusions tirées en 2018 et visera à promouvoir le dialogue mutuel entre les institutions nationales et les organisations internationales. Le Forum sera l'occasion d'évaluer les progrès accomplis par les nombreux pays africains qui ont initié des réformes législatives et politiques dans le domaine de la cybercriminalité et de faciliter l'échange de connaissances et d'expériences pratiques issues d'opérations réussies menées ces dernières années.

Le Forum est organisé par la Commission de l'Union africaine, l'Union européenne et le Conseil de l'Europe (projets GLACY+ et Octopus) en partenariat avec d'autres partenaires et vise à réaffirmer l'engagement commun à travailler ensemble pour trouver de nouvelles modalités de renforcement de la coopération internationale contre toutes les formes de cybercriminalité.

Le Forum sera organisé comme un événement en ligne de deux jours, se concentrant respectivement sur :

- Politiques et mises à jour législatives en matière de cybercriminalité en Afrique
- Coopération internationale en matière de cybercriminalité et de preuves électroniques

Hubs

Parallèlement à la participation en ligne à l'événement, les pays et/ou les organisations intéressés peuvent organiser des « hubs » pour diffuser tout ou partie des sessions du Forum.

Si les contre-mesures COVID-19 en place le permettent, les hubs du Forum devraient accueillir des rassemblements physiques d'homologues locaux en tant qu'événements parallèles à la conférence principale en ligne, en diffusant en continu un certain nombre de ses sessions.

Ces événements parallèles pourraient se concentrer sur des sujets liés aux principaux courants du Forum et pourraient être organisés sous la forme d'événements hybrides, avec une durée et un format variables, à décider sous la direction des organisateurs locaux.

Les centres du Forum sont encouragés à assurer une large couverture médiatique nationale.

Le soutien organisationnel, y compris la mise à disposition du lieu et d'autres services qui pourraient être nécessaires, peut être couvert par le Conseil de l'Europe et d'autres institutions de soutien ou initiatives de partenariat.

Le Conseil de l'Europe accueillera un pôle latéral consacré aux enquêtes sur la cybercriminalité en pratique. Il devrait réunir des intervenants de plusieurs organisations internationales et de pays africains et faciliter le partage d'expériences entre les participants sur les nouvelles tendances en matière de cybercriminalité et les moyens de lutter contre ce phénomène aux niveaux régional et international.

Interpol accueillera les hubs régionaux par l'intermédiaire de ses quatre bureaux à Harare (Zimbabwe), Nairobi (Kenya), Yaoundé (Cameroun) et Abidjan (Côte d'Ivoire).

Organisations / institutions de soutien

Le Forum africain sur la cybercriminalité est organisé par la **Commission de l'Union Africaine** et soutenu par un certain nombre d'organisations partenaires :

- **Le Conseil de l'Europe ;**
- **L'Union européenne ;**
- **INTERPOL ;**
- **Département de la Justice des États-Unis ;**
- **Ministère des Affaires étrangères des États-Unis.**

Un certain nombre d'organisations régionales seront également invitées à participer au Forum, notamment : la Communauté économique des États d'Afrique centrale (**CEEAC**) ; le Marché commun de l'Afrique orientale et australe (**COMESA**) ; l'Autorité intergouvernementale pour le développement (**IGAD**) ; la Communauté de développement de l'Afrique australe (**SADC**) ; le Nouveau partenariat pour le développement de l'Afrique (**NEPAD**) ; la Communauté économique des États de l'Afrique de l'Ouest (**CEDEAO**) ; la Commission économique de l'Afrique de l'Est (**CAE**) ; l'Union du Maghreb arabe (**UMA**) ; le Mécanisme de l'Union africaine pour la coopération policière (**AFRIPOL**) et le Centre africain d'études et de recherches sur le terrorisme (**CAERT**).

Résultats attendus

La 2^e édition du Forum africain devrait s'appuyer sur les résultats obtenus à la suite du 1^{er} Forum africain en contribuant à :

- Partager ses expériences entre les participants sur les nouvelles tendances en matière de cybercriminalité et les moyens de lutter contre la cybercriminalité au niveau régional et international ;
- Parvenir à une compréhension commune des lois sur la cybercriminalité dans les pays africains, identifier les lacunes potentielles et lancer une discussion sur les meilleures pratiques ;
- Faciliter la coopération internationale entre les autorités de justice pénale des pays africains, renforcer les cybercapacités et promouvoir l'adoption de normes internationales dans ce domaine.

La participation des délégations nationales et les contributions sur les sujets de discussion sont attendues et encouragées. Il est prévu que la conférence produise des recommandations et des conclusions pour un suivi ultérieur avec les pays individuels.

Participants

Les pays seront invités à désigner 10 participants chacun, notamment des décideurs et des législateurs, des représentants du secteur de la justice pénale (procureurs, juges, forces de l'ordre), des délégués des ministères chargés de la mise en œuvre des politiques de cybercriminalité et de cybersécurité, et d'autres parties prenantes nationales jouant un rôle actif dans le domaine de la cybercriminalité.

Plate-forme en ligne

Les ateliers se tiendront à distance via une plateforme de vidéoconférence. Le format de l'atelier est une réponse à la pandémie actuelle de COVID-19, qui interdit les voyages internationaux et la participation physique à des événements en grands groupes sans mettre en danger la santé publique.

Interprétation

L'interprétation simultanée EN/FR/PT/AR sera assurée.

Projet d'ordre du jour

Le Forum sera composé de 2 sessions en ligne de 3h30 chacune, organisées sur une période de deux jours. Le 30 juin, le Conseil de l'Europe (CdE) organisera un événement distinct lié au thème principal du Forum, avec la participation attendue de plusieurs organisations internationales. Vous trouverez ci-dessous l'ordre du jour proposé.

Premier jour - 28 juin 2021

GMT	SESSION 1 : Politiques et mises à jour législatives en matière de cybercriminalité en Afrique
09h00	<p>Accueil de haut niveau et remarques d'ouverture</p> <ul style="list-style-type: none"> Hilde HARDEMAN, Chef du Service des instruments de politique étrangère (FPI) de la Commission européenne Alexander SEGER, Chef de la Division Cybercriminalité du Conseil de l'Europe et Secrétaire exécutif du Comité de la Convention sur la cybercriminalité (TCY) Baronne Beeban Tania KIDRON, Membre de la Chambre des Lords, Parlement du Royaume-Uni SE. Dr Amani Abou-Zeid, Commissaire Infrastructure & Energie, Commission de l'Union africaine (CUA)
9h15	<p>Présentation du contexte et des objectifs de l'événement</p> <ul style="list-style-type: none"> Adbul-Hakeem AJIJOLA, président de l'AUCSEG
09h20	<ul style="list-style-type: none"> Législation sur la cybercriminalité en Afrique - Actualités pertinentes Amabélia CHUQUELA, Coordinatrice du Département Spécialisé pour le Domaine Pénal, Bureau du Procureur Général, Mozambique Dr. Mabahig Habib, Conseiller juridique, Ministère de la justice, Soudan <p>Session modérée par AUCSEG et le CdE Session de questions-réponses animée par la CUA - AUCSEG et le CdE</p>
10h00	<p>Lutte contre la cybercriminalité et protection des droits de l'homme en Afrique - Assurer un équilibre approprié grâce aux politiques et à la législation</p> <ul style="list-style-type: none"> Nnenna IFEANY-AJUFO, Nigeria et AUCSEG <p>Session de questions-réponses animée par La CUA - AUCSEG et le CdE</p>
10h30	Pause
10h45	<p>Mises à jour des politiques en matière de cybersécurité et de cybercriminalité</p> <ul style="list-style-type: none"> Proposé par: ECOWAS, intervenant* Tunisie et Bénin* <p>Session de questions-réponses animée par la CUA et le OCWAR-C</p>

11h15	<p>L'absence de législation sur la protection des données comme facteur favorisant la cybercriminalité</p> <ul style="list-style-type: none"> • Michael ILISHEBO, Zambie <p>Session de questions-réponses animée par la CUA et l'AUCSEG</p>
11h45	<p>La législation sur la protection des données, un facteur favorable aux plans d'innovation numérique</p> <ul style="list-style-type: none"> • Irene KABUA, Juriste principal, Commission de réforme du droit, Kenya • Sanusi DRAMMEH, Responsable principal des TIC, Ministère de l'infrastructure de l'information et de la communication, Gambie <p>Session de questions-réponses animée par la CUA</p>
12h15	<p>Conclusions et points essentiels à retenir</p> <ul style="list-style-type: none"> • Commission de l'Union africaine • Conseil de l'Europe
12h30	Fin du premier jour

**interventions à confirmer*

2e jour - 29 juin 2021

GMT	SESSION 2 : Coopération internationale en matière de cybercriminalité et de preuves électroniques
09h00	<p>Lutte contre la cybercriminalité et poursuite dans le cadre de la coopération internationale : Perspectives et défis</p> <ul style="list-style-type: none">• T. George-Maria TYENDEZWA, CFE, Directeur adjoint Unité des poursuites en matière de cybercriminalité, ministère fédéral de la Justice, Nigéria• Maroc* <p>Session modérée par la CUA et le CdE Session de questions-réponses facilitée par la CUA</p>
09h45	Pause
10h00	<p>Lutte contre la cybercriminalité et poursuite dans le cadre de la coopération internationale : Sécurité des enfants en ligne</p> <ul style="list-style-type: none">• Intervenant de l'AUCSEC*• Dr Sherif HASHEM, AUCSEG• Nina LICHTNER, Conseil de l'Europe <p>Session modérée par la CUA – Adil SULIEMAN Session de questions-réponses facilitée par la CUA</p>
11h00	<p>Coopération renforcée en matière de cybercriminalité et de preuves électroniques - le deuxième protocole additionnel à la Convention de Budapest</p> <ul style="list-style-type: none">• Papa Assane TOURE*, Magistrat, Secrétaire Général Adjoint du Gouvernement, Sénégal• Alexander SEGER, Chef de la Division Cybercriminalité du Conseil de l'Europe et Secrétaire exécutif du Comité de la Convention sur la cybercriminalité (T-CY) <p>Session de questions-réponses facilitée par le CdE</p>
11h45	<p>Créer des synergies pour une approche coordonnée du renforcement des capacités en Afrique</p> <ul style="list-style-type: none">• Panel avec des organisations internationales (attendus : CUA, INTERPOL, CdE, UNODC*, DoJ* américain, ComSec*) <p>Facilitée par le GFCE</p>

12h30	Panel sur la voie à suivre - Résolutions du deuxième Forum africain sur la cybercriminalité CUA
13h00	Fin de la conférence

**interventions à confirmer*

Contacts

A la Commission de l'Union africaine :

Adil SULIEMAN

Chargé de mission principal,
Département des infrastructures et de
l'énergie, Télécommunications et TIC,
Commission de l'Union africaine
Courriel : Suliemana@africa-union.org

Au Conseil de l'Europe :

Catalina STROE

Bureau du programme sur la cybercriminalité du
Conseil de l'Europe (C-PROC) Bucarest, Roumanie
Tel : +40 21 201 78 30
Courriel : Catalina.stroe@coe.int

Nina LICHTNER

Bureau du programme sur la cybercriminalité du
Conseil de l'Europe (C-PROC) Bucarest, Roumanie
Courriel: Nina.LICHTNER@coe.int