FORMULAIRE DE SOUMISSION DES CONTRIBUTIONS

Forum de développement régional pour l'Afrique 2020 (RDF-AFR)

La transformation numérique pour accélérer la réalisation des ODD – Développement numérique, partenariats et financement

6-7 octobre 2020, 12:00 –15:00 CAT (réunion virtuelle)
avec des sessions préparatoires le 5 octobre 2020 (12h00 – 13h30 heure du CAT

CONTRIBUTION DE ECOWAS

TITRE: **Agenda Cybersécurité de la CEDEAO**

DUREE PREVUE DE LA PRESENTATION: [5 minutes]

CONTACT: Dr Raphael Koffi, Directeur par intérim Economie Numérique et des Postes, rkoffi@ecowas.int , +234 706 690 6280]

❖ **Initiatives régionales pour l'Afrique : [Sélectionnez l'Initiative(s) régionale(s) pertinente(s) pour votre contribution]**

[Non] Initiative régionale AFR 1 – Construire des économies numériques et favoriser l'innovation en Afrique

[Non] Initiative régionale AFR 2 – Promotion des nouvelles technologies à large bande

[Oui] Initiative régionale AFR 3 – Renforcer la confiance et la sécurité dans l'utilisation des technologies des télécommunications et de l'information et de la communication

[Non] Initiative régionale AFR 4 – Renforcement des capacités humaines et institutionnelles

[Non] Initiative régionale AFR 5 – Gestion et surveillance du spectre des radiofréquences et transition vers la radiodiffusion numérique

❖ **Thème de développement de l'UIT connexe : [Sélectionnez la ou les thématiques pertinentes pour votre contribution]**

[Non] Réseaux et infrastructures numériques

[Oui] Cyber sécurité

[Non] Télécommunications d'urgence

[Non] Environnement

[Non] Politique et réglementation du numérique

[Non] Développement des capacités

[Non] Services et applications numériques

[Non] Inclusion numérique

[Non] Écosystèmes d'innovation numérique

[Non] Statistiques et données sur la prise de décisions fondées sur des données probantes

❖ **Année(s) de mise en œuvre : [Sélectionnez l'année(s) pour laquelle votre action/projet/initiative est pertinent]**

[Oui] 2018	[Oui] 2019	[Oui] 2020	[Oui] 2021	[**Oui**] autres. C'est un processus continu qui ira au-delà de 2021

❖ **Lien de l'initiative à la réponse COVIDE-19: [Veuillez indiquer si votre action/projet/initiative est pertinent pour la réponse COVIDE-19].**

[Oui] Initiative liée à la réponse COVIDE-19 ?

La COVID-19 a augmenté la connectivité des individus, entreprises, organisations et gouvernements avec le travail et les services en ligne. Par conséquent, la cybersécurité et la protection des données deviennent des enjeux capitaux. En effet, les statistiques selon un rapport d'Interpol montrent que depuis l'avènement de la COVID-19, le nombre des activités cybercriminelles a augmenté de façon très significative. Toujours selon Interpol, avec le déploiement rapide, par les organisations et les entreprises, de systèmes distants et de réseaux permettant le télétravail du personnel, les malfaiteurs exploitent également des vulnérabilités accrues en matière de sécurité pour dérober des données, générer des profits et provoquer des perturbations.

Contexte [max 300 mots]

Les Technologies de l'Information et de la Communication (TIC) font partie intégrante de la société et facilitent le développement socio-économique. Les TIC ont le potentiel d'accélérer les efforts d'intégration régionale et favorisent le développement d'une gamme de services innovants tels que le gouvernement électronique, le commerce électronique, l'éducation et e-Santé et qui contribuent au bien-être des citoyens de la CEDEAO.

Toutefois, cette révolution technologique, qui se traduit par des réseaux toujours interconnectés et une pénétration croissante d'Internet dans les États membres, s'est accompagnée du développement de nouvelles menaces appelées cyber menaces et d'une nouvelle forme de criminalité qui est la cybercriminalité.

Partout en Afrique de l'Ouest les cybercriminels prospèrent avec des dommages variés sur l'économie de nos pays. Outre les pertes financières qui se chiffrent en millions de dollars américains, les cyberattaques peuvent aussi conduire a de l'espionnage politique, au dysfonctionnement des infrastructures essentielles telles que les hôpitaux, les aéroports, les centrales électriques ou les réseaux de télécommunications.

C'est dans ce contexte que la CEDEAO a initié l'Agenda cybersécurité de la CEDEAO qui a pour objectif le Renforcement de la cybersécurité dans la région ouest africaine. Il vise à soutenir les États membres dans le renforcement de leurs capacités en matière de cybersécurité et de cybercriminalité pour mieux répondre aux cyber menaces pour assurer une meilleure protection de leur infrastructure nationale, y compris les infrastructures critiques de l'information, ce qui va

rendre l'Internet plus sûr et protéger ainsi les utilisateurs d'Internet, et maximiser ainsi les avantages socio-économiques des TIC.

L'Agenda a deux (2) piliers :

- Renforcer de la cybersécurité
- Lutte contre la cybercriminalité

Ces deux (2) principaux piliers de l'Agenda sont accompagnés des cinq (5) lignes d'action clés suivantes: (i) Gestion de la cybercriminalité ; (ii) La Politique et la Législation; (iii) la Cyber-résilience ; (iv) Le Renforcement des capacités ; et (v) la Coopération internationale

Proposition [max 400 mots]

La Commission de la CEDEAO a donc très tôt pris conscience de l'enjeu des cyber-menaces et la nécessité d'y faire face. C'est dans ce cadre qu'elle a lancé son Agenda de Cybersécurité. Des Textes Communautaires ont été déjà adoptés pour une harmonisation du cadre règlementaire et des renforcements des capacités ont été conduits pour les parties prenantes impliquées dans le renforcement de la cybersécurité et la lutte contre la cybercriminalité dans l'espace CEDEAO avec l'appui de différents partenaires.

Pour soutenir la mise en œuvre du programme de cybersécurité de la CEDEAO, la Commission de la CEDEAO et l'Union européenne ont signé un accord de partenariat pour la mise en œuvre le projet Crime organisé: Réponse de l'Afrique de l'Ouest à la cybersécurité et lutte contre la cybercriminalité» (OCWAR - C) dans le cadre du 11eme Fonds européen de développement (FED) avec Expertise France en tant qu'agence d'exécution. L'objectif global du projet est de contribuer à améliorer la sécurité dans les pays de la CEDEAO, en les aidant à améliorer leur environnement de cybersécurité et à lutter contre la cybercriminalité. Le projet se déroulera jusqu'en 2023 et Expertise France a été désignée comme partenaire de mise en œuvre.

Une évaluation de la maturité de cybersécurité de tous les Etats Membres a été effectuée. Une stratégie régionale de cybersécurité et de lutte contre la cybercriminalité ainsi qu'une politique régionale de protection des services essentiels et des infrastructures critiques ont été élaborées et en cours d'adoption. Un plan d'action régional et par pays a été également élaboré.

Les prochaines grandes activités pour l'implémentation de l'Agenda de cybersécurité de la CEDEAO porteront, entre autres :

Sur la Composante 1: Renforcer la cybersécurité

- Améliorer le cadre stratégique
- Sensibiliser les usagers à la cybersécurité et les décideurs à leurs responsabilités dans la sécurisation du cyberespace
- Améliorer la capacité à gérer les incidents de sécurité (mise en place de Computer Security Incident Response Team dans tous les pays suivi de formations)
- Analyser le cadre d'établissement d'une PKI nationale
- Renforcer la conformité aux droits de l'Homme et aux principes de l'État de droit

Sur la Composante 2: Combattre la cybercriminalité

- Améliorer le cadre légal de la lutte contre la cybercriminalité
- Renforcer la capacité de réponse à la cybercriminalité (mise en place de laboratoires d'investigation numérique dans tous les pays suivi de formations)

Il faut donc des ressources supplémentaires pour poursuivre le renforcement des capacités de toutes les parties prenantes, adopter des politiques/stratégies appropriées au niveau mational, mettre en place les structures nécessaires pour renforcer la résilience des réseaux et du cyber espace dans sa globalité, adopter et mettre en œuvre des cyber législations pour renforcer la coopération internationale en matière de cybercriminalité, etc.

VEUILLEZ SOUMETTRE LA CONTRIBUTION AVANT LE 15 SEPTEMBRE
A ITU-RO-AFRICA@ITU.INT