Common Market
for Eastern and Southern Africa

International Telecommunication Union

Date: 9 juin 2008 **Page 1/4** Ref: **DM-154**

A: Etats Membres du COMESA, Etats Membres de l'UIT, Membres du Secteur et Associés de l'Afrique de l'Est et de l'Afrique australe.

Fax: Voir la liste annexée.

Pour répondre:

Contact: M. Marcelino Tayob
Bureau de zone de l'UIT à Harare (Zimbabwe)

E-mail: marcelino.tayob@itu.int
Fax: +263 4 775939 Tél.: + 263 4 771257

M. Abu Sufian E Dafalla
Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA)

E-mail: ADafalla@comesa.int
Fax: +260 211 229725 Tél.: +260 211 225107

Mme Christine Sund
Division des applications TIC et de la cybersécurité
Département des politiques et stratégies du BDT/UIT

E-mail: cybmail@itu.int
Fax: +41 22 730 5484 Tél.: +41 22 730 5203

Objet: **Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe à Lusaka (Zambie), 25-28 août 2008**

Madame, Monsieur,

Nous avons l'honneur de vous inviter à participer au prochain **Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe**, organisé conjointement par le Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA) et l'Union internationale des télécommunications (UIT). Ce Forum se tiendra sous les auspices de la Communications Authority of Zambia (CAZ) (République de Zambie) du 25 au 28 août 2008 au Protea Hotel Safari Lodge, à environ 35 km de Lusaka (République de Zambie).

L'objet du Forum est de déterminer les principaux enjeux auxquels font face les pays de la région dans l'élaboration de cadres applicables à la cybersécurité et à la protection des infrastructures essentielles de l'information (CIIP), ainsi que d'analyser les bonnes pratiques, d'échanger des informations sur les activités de développement entreprises par l'UIT et par d'autres entités et d'examiner le rôle des différents partenaires pour promouvoir une culture de la cybersécurité. Le Forum vise à réunir les représentants des Etats, les acteurs de l'industrie et d'autres groupes intéressés dans les pays de l'Afrique de l'Est et de l'Afrique australe afin qu'ils puissent discuter, partager des informations et collaborer à l'élaboration et à la mise en œuvre de cadres politiques, réglementaires et d'application nationaux pour la cybersécurité et la CIIP. Par ailleurs, ce Forum intéressera les spécialistes de l'information et de la communication des ministères de la justice et autres départements publics; les institutions et départements chargés des politiques, de la législation et de la mise en en oeuvre dans le domaine de la cybersécurité et les représentants des opérateurs, fabricants, fournisseurs de services, industriels et associations des consommateurs s'intéressant à la promotion d'une culture de la cybersécurité.

Pendant les quatre jours que durera le Forum, les participants examineront les problèmes de cybersécurité nés de la dépendance croissante des sociétés modernes à l'égard des technologies de l'information et de la communication (TIC), interconnectées sur le plan mondial. Cette interconnectivité crée des relations d'interdépendance et expose à des risques auxquels il faut faire face aux niveaux national, régional et international. Au niveau national, chaque pays devrait envisager de s'organiser pour prendre des mesures concertées afin de prévenir les incidents en matière de cybersécurité, de s'y préparer, d'y réagir et, enfin, de rétablir la situation. Ces mesures nécessitent une coopération et une coordination entre les participants de chaque pays, y compris ceux des secteurs public et privé et d'autres organisations ainsi que des utilisateurs individuels qui développent, possèdent, fournissent, gèrent, entretiennent et utilisent les systèmes et réseaux d'information. L'établissement et la mise en œuvre par tous les pays d'un cadre national de cybersécurité et de protection des infrastructures essentielles de l'information (CIIP) représentent une première étape dans le traitement lié à l'interconnexion mondiale des infrastructures TIC.

Ce Forum, qui s'inscrit dans une série de manifestations régionales mises sur pied par l'UIT-D, est organisé conformément à la Résolution 130 (Rév. Antalya, 2006) de la Conférence de plénipotentiaires: **Renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication** et au Plan d'action établi en 2006 par la Conférence mondiale de développement des télécommunications de Doha définissant une nouvelle Question 22/1 devant être étudiée par les Commissions d'études de l'UIT-D: **Sécurisation des réseaux d'information et de communication: meilleures pratiques pour créer une culture de la cybersécurité**.

Dans le cadre de cette activité, l'UIT-D est en train de rédiger un rapport sur les meilleures pratiques recommandées pour une approche nationale de la cybersécurité dans lequel est présenté un cadre pour l'établissement de méthodes nationales de cybersécurité identifiant cinq grands éléments, comme suit: 1) élaborer une stratégie nationale de la cybersécurité; 2) établir une collaboration au niveau national entre les secteurs public et privé; 3) créer au niveau national un dispositif de gestion des incidents; 4) prévenir la cybercriminalité; et 5) promouvoir une culture nationale de la cybersécurité. Ce cadre vise à identifier les principaux partenaires de la cybersécurité dans un pays donné, leurs rôles et moyens de coordination, leurs interactions et modalités de coopération. Parmi ces partenaires, on distingue des organismes et institutions chargés:

– d'encadrer les mesures interinstitutions en matière de cybersécurité et de fournir des orientations pratiques;
– de communiquer avec le secteur privé sur la question de la cybersécurité, qu'il s'agisse de la cybercriminalité, de la gestion des incidents ou de l'élaboration de mesures techniques ou de politique générale;
– d'élaborer et de faire appliquer des lois dans le domaine de la cybersécurité;
– de coordonner les mesures à prendre pour prévenir les incidents en matière de cybersécurité, s'y préparer, y réagir et, enfin, rétablir la situation;
– de promouvoir une culture nationale de la cybersécurité et notamment de sensibiliser les individus, les petites entreprises et d'autres utilisateurs.

Les participants du Forum examineront en outre les initiatives susceptibles d'être prises aux niveaux régional et international pour accroître la coopération et la coordination entre les différentes parties prenantes. Le programme du Forum comportera une session interactive sur le Guide pratique UIT pour l'autoévaluation nationale en matière de cybersécurité/CIIP et nous comptons sur la participation active des délégués à cet égard.

Le Forum se tiendra en anglais et en français, avec interprétation simultanée. La participation au Forum est ouverte à tous les Etats Membres de l'UIT et/ou du COMESA, aux Membres du Secteur, aux Associés et aux autres parties prenantes intéressées, dont les représentants des organisations régionales ou internationales. Un projet de calendrier du Forum est joint à la présente lettre qui contient aussi des informations plus détaillées sur la manifestation: inscription, bourses et calendrier des sessions (voir les annexes). Pour obtenir davantage d'informations sur le Forum, prière de consulter le site web à l'adresse: www.itu.int/ITU-D/cyb/events/2008/lusaka/. Nous vous encourageons à consulter ce site et notamment les informations relatives au Guide pratique UIT pour l'autoévaluation nationale en matière de sécurité/CIIP, avant le Forum.

Nous nous réjouissons de votre participation active et de votre précieuse contribution.

Nous vous prions, Madame, Monsieur, de croire à l'assurance de notre haute considération.

Pour le COMESA	Pour l'UIT
[*Original signé*] Sindiso Ngwenya Secrétaire général, a. i.	[*Original signé*] Sami Al Basheer Al Morshid Directeur du Bureau de développement des télécommunications

Annexes: 2

Annexe 1

Inscription préalable et demande de bourses

La participation au Forum est ouverte à l'ensemble des Etats Membres de l'UIT et/ou du COMESA, aux Membres du Secteur, aux Associés et aux autres parties prenantes intéressées, dont les représentants des organisations régionales ou internationales.

Le formulaire de préinscription en ligne et de demande de bourses se trouve à l'adresse suivante: www.itu.int/ITU-D/cyb/events/2008/lusaka/registration.

Nous avons le plaisir de vous informer que, sous réserve du budget disponible, l'UIT accordera une bourse pour participer à ce Forum. Elle sera accordée à un candidat d'un pays éligible, dûment autorisé par son Administration appartenant à la catégorie des pays les moins avancés (PMA) de la région de l'Afrique de l'Est et de l'Afrique australe. En outre, le COMESA accordera une bourse à chaque Etat Membre éligible du COMESA. La bourse comprend un billet d'avion aller-retour en classe économique et une indemnité journalière pour la durée du Forum. Les bourses sont destinées principalement aux autorités de réglementation et aux ministères chargés des TIC. Les candidats à l'obtention d'une bourse devront régler eux-mêmes toutes les dépenses additionnelles afférentes notamment aux nuits d'hôtel passées en transit et aux visas d'entrée. Nous vous prions de bien vouloir adresser vos demandes avant le **31 juillet 2008** en utilisant le formulaire de demande de bourses en ligne disponible à l'adresse: **www.itu.int/ITU-D/cyb/events/2008/lusaka/registration/**.

Le nombre de délégués de chaque pays qui participera aux travaux du Forum n'est pas limité mais chaque délégué supplémentaire devra prendre à sa charge l'ensemble des coûts de sa participation. Idéalement parlant, un pays enverra des représentants pour chacune des principales fonctions de cybersécurité énoncées (voir plus haut). Chaque délégation devrait en principe être parfaitement au courant des initiatives déployées dans leur pays en matière de cybersécurité.

Les demandes d'inscription et de bourses devraient être présentées dès que possible et le 31 juillet 2008 au plus tard.

Les pays qui ont besoin d'une assistance pour participer au Forum sont priés de prendre contact avec M. Marcelino Tayob au Bureau de zone de l'UIT à Harare (Zimbabwe): Tél.: +263 4 775939 ou e-mail: marcelino.tayob@itu.int avec copie à cybmail@itu.int. Pour tout complément d'information sur le Forum, prière de s'adresser à M. Abu Sufian E Dafalla (e-mail: ADafalla@comesa.int) ou à Mme Christine Sund (e-mail: christine.sund@itu.int).

Contributions

Des contributions électroniques portant sur votre propre expérience au niveau national sont demandées. Nous vous encourageons à envoyer ces contributions à l'adresse suivante: cybmail@itu.int avant le **31 juillet 2008**.

Projet d'ordre du jour du Forum

On trouvera l'ordre du jour complet avec une brève description du contenu de chaque session à l'adresse suivante: **www.itu.int/ITU-D/cyb/events/2008/lusaka/agenda.html**.

Informations pratiques pour les participants

Les informations pratiques pour les participants sont disponibles à l'adresse: **www.itu.int/ITU-D/cyb/events/2008/lusaka/practical-information.html**.