# ANNEX 1 : GROUPE DE TRAVAIL 1

Common Market for Eastern and Southern Africa

Union internationale des télécommunications

## Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe

## Lusaka (Zambie), 25-28 août 2008[38]

**Doc. RFL/2008/WG01-F**

**29 août 2008**

**Original: anglais**

## Groupe de travail 1: Approche régionale pour l'élaboration de stratégies nationales de cybersécurité

### Recommandations du Groupe de travail ad hoc du Forum concernant une approche régionale pour l'élaboration de stratégies nationales de cybersécurité

Il est nécessaire d'élaborer une stratégie nationale type de cybersécurité permettant d'assurer la cybersécurité au niveau national. Une telle stratégie peut servir de mécanisme de coordination pour la région. Etant donné que les capacités nationales existantes varient et que les menaces évoluent en permanence, elle devrait prévoir une approche souple susceptible d'aider les nations de la région à évaluer et améliorer les institutions, les politiques et les capacités dont elle dispose actuellement pour assurer la cybersécurité et à passer en revue et renforcer leurs relations dans ce domaine. Elle devrait permettre d'appuyer les activités nationales et régionales de cybersécurité et les politiques nationales dans le domaine des technologies de l'information, contribuer à atteindre d'autres objectifs nationaux et régionaux de politique générale et favoriser le respect des principes de liberté d'expression, de libre circulation de l'information et d'application régulière de la loi.

Cette stratégie devrait favoriser une approche nationale globale de la cybersécurité et permettre de prendre les mesures requises dans les domaines clés, notamment:

- promouvoir une culture nationale de la cybersécurité;
- avoir un effet dissuasif en ce qui concerne les cyberdélits;
- créer des capacités nationales de gestion des incidents; et
- établir une collaboration secteur public-secteur privé au niveau national.

Cette stratégie devrait être souple et permettre de faire face à un environnement où les risques évoluent constamment. Elle devrait être issue de la coopération, grâce à la consultation de représentants de tous les groupes participants concernés, y compris les organismes publics, le secteur privé, les universités et les associations intéressées. En outre, elle devrait énoncer des objectifs et contenir des dispositions relatives au fonctionnement et à la mise en oeuvre. Ces dispositions seraient les suivantes:

1) reconnaître l'importance des technologies de l'information et de la communication pour la nation;

2) reconnaître qu'il est nécessaire d'assurer la cybersécurité et qu'il s'agit d'un processus permanent, et non d'un but à atteindre;

3) au niveau national, sensibiliser les responsables politiques et toutes les parties prenantes aux questions de cybersécurité et au besoin d'agir sur le plan national et de coopérer à l'échelle régionale et internationale;

4) justifier la nécessité d'agir au niveau national afin de faire face aux menaces qui pèsent sur les cyberinfrastructures des pays et d'éliminer les points où celles ci sont vulnérables, et demander que, sur le plan politique, des débats aient lieu et que des mesures soient prises afin d'atteindre les objectifs fixés dans la présente déclaration de politique générale relative à la cybersécurité;

---

38 Site web du Forum régional UIT sur la cybersécurité : http://www.itu.int/ITU-D/cyb/events/2008/lusaka/.

5) souligner la nécessité de participer aux activités régionales et internationales dans le domaine de la cybersécurité;

6) identifier les risques encourus, fixer des objectifs pour la politique de cybersécurité et déterminer les manières d'atteindre ces objectifs;

7) délimiter les rôles et les responsabilités, identifier les priorités et déterminer où et dans quels délais se fera la mise en oeuvre;

8) identifier une personne et une institution de premier plan chargées de coordonner l'ensemble des activités nationales et désigner des institutions et des partenaires de coopération principaux pour chaque élément de la stratégie nationale;

9) décider de l'emplacement, de la fonction et du rôle d'un organe national de veille, d'alerte et d'intervention chargé de coordonner les activités;

10) définir et établir des modalités et des mécanismes de coopération entre tous les participants ainsi qu'entre pouvoirs publics et secteur privé;

11) identifier des homologues aux niveaux international et régional et encourager les activités internationales et régionales visant à instaurer la cybersécurité, notamment l'échange d'informations et l'assistance;

12) demander la mise en place d'un processus de gestion intégrée des risques afin d'identifier et de hiérarchiser les mesures de protection pour ce qui est de la cybersécurité;

13) demander une réévaluation régulière de la stratégie nationale et de sa mise en oeuvre;

14) fixer ou demander que soient fixées des priorités pour les activités nationales de cybersécurité;

15) identifier les besoins de formation et les moyens d'y répondre;

16) recenser les ressources, les compétences et les budgets disponibles ainsi que les besoins de financement;

17) demander un premier grand examen général afin de déterminer si les pratiques nationales actuelles sont adéquates et l'évaluation du rôle de toutes les parties prenantes (autorités gouvernementales, secteur privé et citoyens) engagées dans ce processus;

18) faire connaître les présentes dispositions auprès des responsables gouvernementaux afin de favoriser la coopération de tous les participants;

19) prévoir des possibilités d'adaptation de ces dispositions et ajuster les approches sur le plan national, local et des communautés en fonction des besoins et des contextes nationaux.

_____