Common Market for Eastern and Southern Africa

Union internationale des télécommunications

Forum régional UIT sur la cybersécurité 2008 Lusaka (Zambie)

Document RFL/2008/01-F

29 août 2008

Original: anglais

Projet de compte rendu de la réunion:

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

Lusaka (Zambie), 25-28 août 2008[1]

Veuillez adresser vos observations éventuelles sur ce projet de compte rendu à l'adresse suivante: cybmail@itu.int

Objet du présent compte rendu

1. Le Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe s'est tenu à Lusaka (Zambie) du 25 au 28 août 2008. Ce Forum, tenu sous les auspices de l'Autorité des communications de la Zambie et le Gouvernement zambien et organisé conjointement par l'UIT et le Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA), visait à déterminer les principaux enjeux auxquels font face les pays de la région lors de l'élaboration de cadres applicables à la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP), à analyser les bonnes pratiques, à échanger des informations sur les activités de développement entreprises par l'UIT et par d'autres entités et à examiner le rôle des différents partenaires pour promouvoir une culture de la cybersécurité. Les participants au forum ont également analysé les initiatives prises aux niveaux régional et international pour accroître la coopération et la coordination entre les différentes parties prenantes.

2. Ce Forum a été organisé conformément à la Résolution 130 (Antalya, 2006) de la Conférence de plénipotentiaires de l'UIT, intitulée "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 la 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". Près de 60 représentants de 21 pays et 4 organisations régionales ont participé au Forum, parmi lesquels figuraient des professionnels des pouvoirs publics, d'autorités de régulation, du secteur privé et de la société civile. Une documentation complète sur le Forum, comprenant l'ordre du jour définitif et tous les documents présentés, est affichée sur le site web correspondant (www.itu.int/itu-d/cyb/events/2008/lusaka/). Le présent compte rendu[2] de la réunion résume la teneur des quatre jours de débats du Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe et donne un aperçu des sessions et des présentations des orateurs ainsi que de certaines prises de position commune.

3. Le troisième jour du Forum régional UIT sur la cybersécurité (27 août 2008), des séances de travail consacrées au renforcement des capacités nationales et régionales en matière de cybersécurité/CIIP ont été organisées dans le cadre de trois groupes de travail. Ces groupes ont examiné: 1) l'élaboration d'une stratégie nationale sur la cybersécurité; 2) la législation et les mesures d'application; et 3) les dispositifs de veille, d'alerte et de gestion des incidents. Outre les recommandations générales élaborées par le

---

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

2 Ce compte rendu est accessible en ligne, à l'adresse: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08-f.pdf.

Forum, les Annexes 1, 2 et 3 reproduites à la fin du présent document donnent davantage de renseignements sur les recommandations et suggestions formulées par les trois groupes de travail ad hoc[3].

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

4. Les sociétés modernes sont de plus en plus tributaires des technologies de l'information et de la communication (TIC), interconnectées sur le plan mondial. Les pays se rendent compte que cette situation crée des relations d'interdépendance et fait peser des risques auxquels il faut faire face aux niveaux national, régional et international. C'est pourquoi le renforcement de la cybersécurité et la protection des infrastructures essentielles de l'information sont fondamentaux pour la sécurité de chaque pays, comme pour sa prospérité sociale et économique. Au niveau national, la responsabilité est partagée entre les pouvoirs publics, le secteur privé et les particuliers, qui doivent prendre des mesures concertées afin de prévenir les incidents, de s'y préparer, d'y réagir puis de rétablir la situation. Aux niveaux régional et international, il faut coopérer et assurer la coopération et la coordination avec les différents partenaires. L'élaboration et la mise en oeuvre d'un cadre national pour la cybersécurité et la protection des infrastructures essentielles de l'information nécessitent donc une approche globale, pluridisciplinaire et multi-parties prenantes. Les participants au Forum ont débattu de certains éléments clés de l'élaboration de ces cadres politiques et réglementaires et ont proposé des mesures concrètes pour les mettre en oeuvre.

Ouverture de la réunion et allocution de bienvenue

5. Le Forum régional sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe a été ouvert par Amos Marawa, Directeur du développement des infrastructures, Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA), qui a prononcé une allocution de bienvenue[4]. Au nom du COMESA, M. Marawa a souhaité la bienvenue aux participants au Forum, dont il a souligné l'importance pour le renforcement des capacités de la région en matière de cybersécurité. Il a indiqué que le pays était en deuil après le décès du Président et a invité les participants, avant d'ouvrir les débats, à observer une minute de silence à la mémoire du Président décédé. M. Marawa a également remercié l'UIT d'avoir organisé le Forum conjointement avec le COMESA et l'Autorité des communications de la Zambie. Il a ensuite rappelé aux participants que l'objectif du COMESA est de créer une société pleinement intégrée et ouverte à la concurrence, grâce à une coopération et à une intégration accrues dans tous les domaines du développement, y compris dans celui des technologies de l'information et de la communication. Il a souligné que le COMESA, dans le cadre de son programme régional d'intégration et conformément à son Traité, a élaboré des politiques générales, des règlements et des programmes destinés à renforcer et à élargir le processus d"intégration régionale.

6. M. Marawa a ensuite mis l'accent sur la nécessité d'harmoniser la législation technique et juridique, pour progresser dans la lutte contre la cybercriminalité et les menaces connexes, étant donné que ni la législation, ni les solutions techniques ne sont suffisantes à elles seules. En Afrique, la révolution des TIC risque de ne pas donner les résultats escomptés, et pourtant nécessaires, si les pays n'adoptent pas une approche régionale judicieuse permettant d'établir des politiques et des législations nationales en matière de cybersécurité. A cet égard, il a fait observer que les progrès réalisés en permanence dans le domaine des TIC se traduisent par un environnement en mutation constante qui est trop complexe à comprendre et à gérer pour un pays à lui seul. En conséquence, les pays de la région ont besoin des connaissances spécialisées de l'extérieur pour résoudre efficacement les problèmes que posent les TIC. Au fil du temps, les pays de la région dans son ensemble devront créer les compétences collectives nécessaires et nouer des partenariats entre le secteur public et le secteur privé, afin de coopérer dans la mise en oeuvre des approches qu'ils adopteront pour renforcer les capacités de cybersécurité. Etant donné qu'il n'existe aujourd'hui aucune base solide en matière de sécurité au niveau régional, M. Marawa a conclu en soulignant la nécessité d'instaurer des partenariats aux niveaux national, régional et international dans des domaines comme le commerce électronique, la législation commerciale sur Internet, etc. Il a invité les participants au Forum à élaborer un cadre législatif régional sur la cybersécurité, ainsi qu'un modèle possible de stratégie régionale en matière de cybersécurité. Il a également préconisé la création d'un groupe d'experts et d'un système de coopération régionale, pour assurer le suivi et l'application des recommandations du Forum.

7. Marcelino Tayob, Chef du Bureau de zone de l'UIT pour l'Afrique de l'Est et l'Afrique australe[5], a ensuite prononcé quelques remarques liminaires[6] au nom de l'UIT, du Secrétaire général de l'UIT, Dr Hamadoun

---

3 Les recommandations du Forum et les conclusions des trois groupes de travail ad hoc sont accessibles à l'adresse: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/recommendations-and-outcomes-lusaka-aug-08.pdf.

4 Non disponible sur papier.

5 http://www.itu.int/ITU-D/afr/.

Touré, et du Directeur du Secteur du développement des télécommunications de l'UIT (UIT-D), Sami Al Basheer Al Morshid. Il a tout d'abord présenté ses condoléances, au nom de l'UIT, au Gouvernement et au peuple zambien, suite à la disparition du Président Mwanawasa, en indiquant que la Zambie, la SADC, le COMESA et l'Afrique venaient de perdre un grand dirigeant. M. Tayob a ensuite remercié le Gouvernement zambien et l'Autorité des communications de la Zambie d'avoir accueilli le Forum régional sur la cybersécurité, en dépit des circonstances particulières que la Zambie connaît aujourd'hui. Il a fait observer qu'il s'agissait de la deuxième manifestation organisée conjointement par l'UIT et le COMESA en 2008. La première, qui s'est tenue à Addis-Abeba (Ethiopie), était un atelier ayant pour thème: "Concurrence et évolution des conditions du marché, incidences sur la réglementation des TIC et kits pratiques pour l'Afrique de l'Est et l'Afrique australe. La collaboration étroite instaurée avec le COMESA et d'autres organisations régionales pour l'organisation d'ateliers et d'autres activités de renforcement des capacités est un partenariat qui va dans le sens de la politique de collaboration avec des organisations régionales suivie par l'UIT, en vue de fournir des services améliorés aux membres, de rationnaliser l'utilisation des ressources et de compléter les programmes et activités de chaque organisation, et d'éviter ainsi toute répétition des tâches et toute concurrence inutile.

8. M. Tayob a expliqué que l'UIT était résolue à travailler avec les membres pour élaborer une conception commune de l'importance de la création d'une culture mondiale de la cybersécurité. En raison de son importance reconnue, l'UIT, conformément au mandat qui lui a été dévolu par la Conférence de plénipotentiaires, mène actuellement des activités en matière de cybersécurité au sein de tous ses Secteurs (UIT-T, UIT-R et UIT-D). Ces activités font intervenir les Commissions d'études et comprennent des initiatives de renforcement des capacités. A cet égard, les représentants de l'UIT présents au Forum espèrent pouvoir procéder à de nouveaux échanges de vues avec les pays de la région, afin de déterminer ce que les Etats Membres attendent de l'Union en matière d'assistance pour la cybersécurité. Il a rappelé que des dirigeants du monde entier, lors du Sommet mondial sur la société de l'information (SMSI) qui s'est tenu en deux phases, en 2003 et en 2005, avaient reconnu l'importance d'une coopération internationale en matière de cybersécurité et avaient chargé l'UIT de jouer un rôle de premier plan dans la coordination des mesures à prendre à l'échelle mondiale pour relever ce défi mondial. C'est pourquoi il y a plus d'un an, le 17 mai 2007, l'UIT a lancé le Programme mondial cybersécurité, qui constitue le cadre de coopération internationale défini par l'Union, dont l'objet est de proposer des stratégies devant déboucher sur des solutions propres à renforcer la confiance et la sécurité dans la société de l'information. Ce programme repose sur les initiatives existantes en matière de cybersécurité aux niveaux national, régional et international, ce qui permettra d'éviter toute répétition des tâches et d'encourager la collaboration entre tous les partenaires concernés.

9. M. Tayob a également présenté aux participants au Forum certaines initiatives prises récemment par le Secrétaire général de l'UIT. Il a notamment cité la collaboration avec le Partenariat multilatéral international contre le cyberterrorisme (IMPACT), lancé par le Premier Ministre de la Malaisie, une série de réunions tenues avec le Premier Ministre japonais et de nombreux ministres à l'occasion de la Réunion ministérielle de l'OCDE tenue à Séoul (République de Corée), en vue de lutter contre la cybercriminalité et de faire face au changement climatique, et la tenue d'un Segment spécial de haut niveau consacré exclusivement à la cybersécurité lors du prochain Conseil de l'UIT, qui se tiendra en 2008. M. Tayob a appelé les organisations et les pays désireux d'étudier des possibilités de collaboration avec l'UIT afin d'atteindre les objectifs du GCA de se mettre en rapport avec le secrétariat. M. Tayob a conclu ses remarques liminaires en souhaitant aux participants plein succès dans leurs travaux.

Session 1: Elaboration d'un cadre pour la cybersécurité et la protection des infrastructures essentielles de l'information

10. Il est généralement admis qu'il est nécessaire de fiabiliser et de sécuriser l'utilisation des TIC, de promouvoir la cybersécurité et de protéger les infrastructures essentielles sur le plan national. Alors que les professionnels des secteurs public et privé ont leur propre conception de ces questions importantes, dans un souci de cohérence, certains pays ont mis en place des cadres institutionnels, tandis que d'autres ont eu recours à une approche plus légère et moins formelle. De nombreux pays n'ont pas encore élaboré de stratégie nationale pour la cybersécurité et la CIIP. Cette première session du forum, présidée par M. Sufian Dafalla, responsable des télécommunications au COMESA, était consacrée au concept de cadre national pour la cybersécurité et la CIIP ainsi qu'aux efforts déployés par l'UIT, afin que les participants puissent se faire une idée générale des perspectives et des enjeux de la question. M. Dafalla a ouvert la session et a invité les deux intervenants de cette session à présenter leur exposé, en échangeant des renseignements sur certaines des activités en cours et en projet de l'UIT, pour renforcer les capacités dans le domaine de la cybersécurité.

11. Marco Obiso, Conseiller de la Division des applications TIC et de la cybersécurité au Bureau de développement des télécommunications (BDT) de l'UIT, a présenté un aperçu des "Activités de l'UIT-D dans

---

6 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/itu-opening-remarks-lusaka-aug-08.pdf.

le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information (CIIP)"[7]. Il a tout d'abord donné une vue d'ensemble des activités générales menées par l'UIT dans le domaine de la cybersécurité, en faisant observer que des activités relatives à la cybersécurité étaient en cours de réalisation dans les trois Secteurs de l'UIT. Il a ajouté que le Secteur du développement se trouvait à l'avant-garde des activités entreprises par l'Union dans les différentes régions et travaillait en étroite collaboration avec des partenaires en vue de la mise en place de projets et d'initiatives. Il est primordial d'adopter une approche multi-parties prenantes dans toutes les activités de l'UIT, notamment dans le domaine de la cybersécurité, étant donné que les problèmes connexes ne peuvent être traités isolément. M. Obiso a souligné que l'approche retenue par l'UIT pour remédier aux problèmes liés à la mise en oeuvre de la grande orientation C5 du SMSI et à l'instauration de la confiance et de la sécurité dans l'utilisation des TIC était le Programme mondial cybersécurité (GCA). L'UIT utilise cet instrument pour regrouper et harmoniser les activités internes de l'Union en matière de cybersécurité qui sont menées dans l'ensemble des trois Secteurs et pour collaborer avec les parties prenantes, les organisations et les experts de l'extérieur, tout en veillant à la mise en oeuvre des recommandations formulées dans le cadre du GCA.

12. M. Obiso a ensuite donné des précisions sur le Programme de travail de l'UIT-D sur la cybersécurité à l'intention des pays en développement (2007-2009)[8], en fournissant des exemples concrets de ce que l'UIT s'efforce de faire pour apporter une assistance aux pays en développement dans le domaine de la cybersécurité et de la CIIP. Il a mentionné dans son exposé certaines initiatives, en cours et en projet, de l'UIT en matière de cybersécurité: identification de bonnes pratiques dans la création de cadres nationaux pour la cybersécurité et la CIIP; kit pour l'auto-évaluation de l'état de préparation nationale dans le domaine de la cybersécurité/CIIP; kit pour atténuer les effets des "botnets" ou réseaux zombies; publication du Guide de la cybersécurité pour les pays en développement; enquête internationale sur les capacités nationales dans le domaine de la cybersécurité des équipes CSIRT; kit pour un modèle de législation en matière de cybercriminalité pour les pays en développement; kit pour promouvoir une culture de la cybersécurité ainsi que l'organisation de plusieurs ateliers régionaux de sensibilisation et de renforcement des capacités au sujet des cadres pour la sécurité et la CIIP. En outre, il a fait observer que ce programme de travail définissait la façon dont l'UIT compte aider les pays en développement à renforcer leurs capacités dans le domaine de la cybersécurité/CIIP, par la fourniture aux Etats Membres de ressources, de documents de référence et de kits sur les sujets connexes. A mesure que ces kits évolueront vers plus de stabilité, l'UIT envisage de les diffuser largement aux 191 Etats Membres de l'UIT.

13. Joseph Richardson, Consultant (Etats-Unis d'Amérique), a ensuite présenté un exposé en faisant part de ses réflexions sur l'"Approche nationale de l'UIT en matière de cybersécurité" et le "Kit pour l'auto-évaluation de l'état de préparation nationale dans le domaine de la cybersécurité/CIIP"[9]. M. Richardson a décrit la méthode retenue pour organiser les mesures prises au niveau national en matière de cybersécurité/CIIP, qui comprend des déclarations d'intention, définit des objectifs et des mesures concrètes à prendre en vue de les atteindre et présente des références et des documents liés à chacune de ces mesures. En outre, M. Richardson a noté que la méthode définie pour organiser les initiatives nationales en matière de cybersécurité/CIIP était un document conçu pour être évolutif. Il a souligné que la protection du cyberespace était fondamentale pour la sécurité nationale et la prospérité économique. Il a ensuite présenté des idées concrètes sur la manière dont les pays peuvent commencer à élaborer une stratégie nationale en matière de cybersécurité. Les activités menées actuellement par l'UIT pour concevoir un outil d'auto-évaluation de la cybersécurité/CIIP sur le plan national[10] constitue un jalon important dans cette direction.

14. Cet outil peut aider les pouvoirs publics à examiner les politiques, procédures, normes et institutions nationales existantes, ainsi que d'autres éléments nécessaires, à la formulation de stratégies de sécurité dans un environnement des TIC en pleine évolution. Il peut en outre aider les pouvoirs publics à mieux comprendre les systèmes existants, à recenser les points faibles, qui doivent faire l'objet d'une attention particulière, et à hiérarchiser par ordre de priorité les initiatives visant à améliorer la situation. M. Richardson a souligné que le kit mettait en évidence des questions et posait un certain nombre de problèmes qui méritaient d'être étudiés; quelles mesures ont été prises jusqu'à présent, quelles sont les mesures prévues et quel est leur état d'avancement? M. Richardson a également fait observer, à propos des initiatives liées à la cybersécurité, qu'aucun pays ne partait de zéro. En outre, il n'existe pas de formule ou de solution unique, puisque chaque pays a des besoins et des aspirations qui lui sont propres.

---

7 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/obiso-itu-cybersecurity-overview-lusaka-aug-08.pdf.

8 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

9 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/richardson-cybersecurity-framework-overview-lusaka-aug-08.pdf.

10 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Quelle que soit la solution adoptée, il faut la réexaminer et la réévaluer en permanence; il est tout aussi important de faire participer toutes les parties prenantes, en fonction de leur rôle, à l'élaboration d'une stratégie nationale. Les pays désireux de procéder à une auto-évaluation nationale dans le domaine de la cybersécurité/CIIP conjointement avec l'UIT, peuvent contacter le Bureau de développement de l'UIT à l'adresse: cybmail@itu.int.

Session 2: Organisation des activités nationales de cybersécurité/CIIP et études de cas par pays: promouvoir une culture de la cybersécurité

15. Afin de mieux comprendre l'approche adoptée pour organiser les activités nationales de cybersécurité/CIIP et d'examiner plus avant les stratégies retenues par différents pays en matière de cybersécurité, la session 2, animée par Garry Mukelabai, Directeur des systèmes d'information, Autorité des communications de la Zambie (Zambie) a été consacrée à l'étude détaillée des éléments nécessaires à la promotion d'une culture de la cybersécurité.

16. Christine Sund, Coordonnateur de la cybersécurité, Division des applications TIC et de la cybersécurité, Secteur du développement des télécommunications de l'UIT (UIT-D), a brièvement décrit, dans sa présentation sur le thème "Promouvoir une culture de la cybersécurité - Eléments de base"[11], ce que l'on entend par culture de la cybersécurité, ainsi que les rôles que les différentes parties prenantes de la société de l'information pourraient jouer dans l'instauration d'une telle culture à l'échelle mondiale. A cet égard, elle a souligné l'existence de neuf éléments, comme indiqué dans les Résolutions 57/239 (2002): "Création d'une culture mondiale de la cybersécurité" et 58/199 (2004): "Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information" de l'Assemblée générale des Nations Unies. Ces neuf éléments sont les suivants: a) sensibilisation; b) responsabilité; c) réaction; d) éthique; e) démocratie; f) évaluation des risques; g) conception et mise en oeuvre de la sécurité; h) gestion de la sécurité; et i) réévaluation. Ces Résolutions appelaient les Etats Membres de l'ONU et toutes les organisations internationales compétentes à tenir compte de ces éléments dans la préparation des deux phases du Sommet mondial sur la société de l'information (SMSI)[12] organisées en 2003 et 2005. Les documents établis à l'issue de ces deux phases soulignaient en outre la nécessité de renforcer la confiance et la sécurité dans l'utilisation des TIC et la détermination des pays à promouvoir une culture de la sécurité.

17. Dans son exposé, Mme Sund a précisé en quoi les pouvoirs publics pourraient promouvoir une culture de la cybersécurité; à savoir: assurer la protection des ressortissants du pays; jouer un rôle central dans la coordination et la mise en oeuvre d'une stratégie nationale de la cybersécurité, faire en sorte que le pays ait une politique souple et capable d'adaptation; coordonner les responsabilités entre les autorités et les ministères; créer une nouvelle législation, ou adapter la législation existante, afin d'ériger en infraction pénale l'utilisation délictueuse des TIC; mettre un terme aux abus et protéger les droits des consommateurs; mener des activités de coopération dans le domaine de la cybersécurité sur les plans national, régional et international. Mme Sund a souligné que, étant donné que le secteur privé est propriétaire et exploitant de la plus grande partie des infrastructures TIC, il est essentiel de le faire participer à la création d'une culture nationale et mondiale de la cybersécurité. Pour obtenir de bons résultats, à cet égard, il importe de bien comprendre tous les aspects des réseaux TIC; l'expérience et la participation du secteur privé sont donc ainsi indispensables à l'élaboration et à la mise en oeuvre de stratégies nationales de cybersécurité. En outre, Mme Sund a noté que les secteurs public et privé devaient aider les particuliers à s'informer sur la façon de se protéger lorsqu'ils sont en ligne. Puisque des moyens efficaces sont à la portée de tous, chacun, dans la société de l'information, se doit d'être vigilant et de se protéger, même si fondamentalement, la cybersécurité est une responsabilité partagée.

18. John Carr, Secrétaire de la CHIS (Children's Charities' Coalition on Internet Safety), Royaume-Uni, a ensuite présenté son étude de cas portant sur le thème "Comment rendre plus sûr l'Internet et les technologies en ligne pour les enfants et les jeunes"[13]. Dans son exposé, il a expliqué que le secteur des TIC devait intervenir davantage pour protéger les enfants et les jeunes qui utilisent l'Internet et les applications et technologies connexes. Il a rappelé que les enfants et les jeunes constituaient une proportion importante des internautes actuels et que, parallèlement, ils avaient accès à des documents en ligne dangereux ou préjudiciables. Il a ajouté que dans le monde entier, des enfants étaient victimes de maltraitance de la part de prédateurs en ligne et que l'Internet jouait un rôle crucial en facilitant les premiers contacts qui conduisaient à des abus. Lors de l'examen de problèmes tels que le spam, les virus, l'usurpation d'identité et d'autres cybermenaces, les professionnels du secteur de l'Internet se sont montrés résolus à se réunir pour mettre au point des normes techniques et des protocoles communs et

---

11 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/sund-promoting-a-culture-of-cybersecurity-lusaka-aug08.pdf.

12 http://www.itu.int/wsis/.

13 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/carr-safety-for-young-people-lusaka-aug-08.pdf.

pour adopter des moyens communs et efficaces permettant de promouvoir ces solutions. Cependant, cet objectif ne s'est toujours pas concrétisé en ce qui concerne la protection des enfants. Ainsi, la CHIS (*Children's Charities Coalition on Internet Safety*) rassemble les principales organisations de protection et de sécurité des enfants du Royaume-Uni, en vue de défendre les intérêts des enfants dans l'environnement en ligne. Dans son exposé, il a ajouté qu'il fallait promouvoir une culture de la cybersécurité du fait de l'utilisation des TIC par les enfants et les jeunes, pour la raison évidente que les pouvoirs publics et les particuliers considèrent la protection des jeunes et des enfants comme une priorité globale pour la société dans son ensemble.

19. M. Carr a présenté aux participants certaines mesures pouvant être envisagées pour faire face aux différents risques qui existent, notamment le rôle primordial que jouent l'éducation et la sensibilisation dans le domaine de la cybersécurité, et a exposé diverses solutions techniques et mesures juridiques, en donnant des exemples sur les initiatives prises par différentes parties prenantes pour mettre en oeuvre ces mesures. M. Carr a fait observer qu'une large gamme de mesures techniques avaient été mises en place par le secteur privé dans le domaine de la cybersécurité et que ces mesures étaient souvent associées aux programmes de responsabilité sociale des entreprises ainsi qu'aux activités des entreprises visant à faire respecter la réglementation. Le Royaume-Uni a pris diverses initiatives concluantes d'autorégulation dans le domaine de la protection des enfants. Ainsi, des organismes s'occupant de la protection des enfants, les services de police et certains partenaires de l'industrie de l'Internet s'emploient à élaborer une stratégie nationale en faveur de la protection des enfants et des codes de pratique axés sur la sécurité et la protection des enfants ont d'ores et déjà été adoptés. Ces dernières années, les techniques de filtrage se sont sensiblement développées et peuvent également être considérées comme un instrument utile en vue de la réalisation d'objectifs communs. M. Carr a conclu en faisant remarquer qu'il se peut que les initiatives d'autorégulation ne fonctionnent pas dans tous les pays, même si elles ont donné de bons résultats au Royaume-Uni.

20. Helmi Rais, Directeur du CERT-TCC de la Tunisie, Agence nationale de la sécurité informatique de la Tunisie, a fait un exposé intitulé "Etude de cas visant à promouvoir une culture de la cybersécurité: l'expérience de la Tunisie"[14]. M. Rais, qui représentait le CERT-TCC de la Tunisie, le seul CERT (Equipe d'intervention en cas d'urgence informatique) reconnu par la FIRST[15] sur le continent africain, a encouragé les pays d'Afrique de l'Est et d'Afrique australe à créer leurs propres CERT publics ou centres nationaux afin de coordonner les activités de veille, d'alerte et d'intervention en cas d'incident informatique. Il a fait observer que, dans l'ensemble, la sensibilisation aux questions de sécurité et la compréhension de ce que l'on entendait par sécurité des TIC étaient encore insuffisantes dans la région. La Tunisie a été confrontée à divers problèmes, comme le manque de sensibilisation et la pénurie d'experts locaux dans le domaine de la sécurité et le manque de fonds. A cet égard, le CERT-TCC a apporté une assistance à d'autres pays de la région, notamment en prenant diverses initiatives de renforcement des capacités, de sensibilisation et de formation. M. Rais a également présenté des renseignements sur certaines des manifestations actuellement organisées par le CERT-TCC à l'intention des entreprises, pour promouvoir une culture de la cybersécurité. L'un des éléments clés de la solution proposée par le CERT-TCC est le recours à des solutions sécuritaires à source ouverte et l'utilisation de ces ressources pour améliorer les solutions nationales de la Tunisie en matière de cybersécurité, qui peuvent être partagées avec d'autres parties intéressées sur le continent africain. L'orateur a encouragé les pays à utiliser des solutions à source ouverte et à rechercher activement des prêts, par exemple auprès de la Banque mondiale, afin de financer dans un premier temps la mise en oeuvre d'activités nationales liées à la cybersécurité.

21. Même si des initiatives de sensibilisation à la cybersécurité sont prises pour promouvoir une culture de la cybersécurité, il faut à l'évidence réunir une documentation ciblée et spécifique en matière de sensibilisation. A cet égard, M. Rais a donné des exemples d'activités de sensibilisation menées par le CERT-TCC en collaboration avec d'autres partenaires, à l'intention des internautes. Il s'agit notamment de la création et de la diffusion d'affiches sur la sensibilisation à la sécurité informatique, de l'affectation de personnel chargé de préparer des documents à l'intention des journalistes, de la radio et de la télévision de dessins animés pour les enfants, de la création d'un CD-ROM sur le contrôle de l'accès à l'Internet par les parents, etc. M. Rais a également indiqué qu'une formation de niveau master en sécurité informatique avait été mise en place pour accroître le nombre de professionnels qualifiés dans le domaine de la sécurité informatique en Tunisie. Par ailleurs, le CERT-TCC encourage le secteur privé à prendre une part active dans la campagne de sensibilisation, de formation et d'éducation. M. Rais a conclu son exposé en insistant sur l'importance de la collaboration entre les différentes parties prenantes, notamment entre le CERT-TCC et diverses associations, afin d'obtenir leurs réactions et leur contribution pour améliorer encore les programmes en cours d'élaboration.

---

[14] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rais-awareness-raising-tunisia-case-study-lusaka-aug-08.pdf.

[15] Consortium d'équipes chargées de la sécurité informatique et des interventions en cas d'incident (FIRST), http://www.first.org/.

22. A la fin des sessions, Joseph Richardson a aidé les participants, par le biais d'un exercice pratique à mieux comprendre l'utilisation du Kit pour l'auto-évaluation de la cybersécurité/CIIP sur la plan national[16] afin d'évaluer l'état de préparation à l'échelle nationale en matière de cybersécurité pour chacun des sujets concernés. Le processus d'auto-évaluation dans son ensemble vise à aider les pouvoirs publics à mieux comprendre les initiatives en place et leurs répercussions concrètes, à recenser les points faibles qui doivent faire l'objet d'une attention particulière et à hiérarchiser par ordre de priorité les initiatives prises au niveau national. M. Richardson a fait observer qu'il n'existait pas de solution unique pour la mise en oeuvre de processus d'auto-évaluation, puisque chaque pays a des besoins et des aspirations qui lui sont propres. Quelle que soit la solution adoptée, il faut la réexaminer et la réévaluer en permanence, et il est tout aussi important de faire participer toutes les parties prenantes, en fonction de leur rôle, à l'élaboration de tous les éléments nécessaires à une stratégie nationale pour la cybersécurité. M. Richardson a signalé que le kit et les ressources connexes étaient constamment mis à jour sur le site web de l'UIT-D consacré à la cybersécurité (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html) et que des pays lançaient des projets pilotes, afin de tester et d'évaluer ce kit, parallèlement à l'organisation par l'UIT, en 2007, 2008 et 2009, de réunions, de forums et d'ateliers régionaux sur le renforcement des capacités.

Session 3: Cadre pour l'organisation des activités nationales de cybersécurité/CIIP et études de cas par pays: collaboration entre les secteurs public et privé

23. La session suivante était consacrée à la collaboration entre les secteurs public et privé pour l'organisation des activités nationales de cybersécurité/CIIP et aux études de cas par pays connexes. Elle a été animée par M. Marcelino Tayob, Chef du Bureau de zone de l'UIT pour l'Afrique australe à Harare (Zimbabwe), Union internationale des télécommunications (UIT).

24. Nicholas Ngoma, ingénieur en réseaux de télécommunication, POTRAZ (Zimbabwe), a présenté dans son exposé une étude de cas portant sur "L'expérience du Zimbabwe"[17]. Il a expliqué que comme beaucoup d'autres pays, le Zimbabwe ne faisait pas exception à la règle et avait enregistré de nombreuses avancées grâce aux TIC. Afin de tenir compte de cette évolution, il est nécessaire que le pays donne des moyens d'action à tous les secteurs, par le biais d'initiatives des pouvoirs publics, pour qu'ils disposent de suffisamment de connaissances sur la manière d'utiliser efficacement les TIC. En conséquence, les pouvoirs publics ont été amenés à rechercher de nouveaux moyens de protéger le pays contre les délits engendrés par la progression de l'utilisation des TIC et ont mis en place une stratégie nationale destinée à promouvoir la cybersécurité. M. Ngoma a souligné qu'il fallait faire en sorte que toutes les parties prenantes des secteurs concernés se conforment aux lois et aux législations visant à lutter contre la cybercriminalité. Les pouvoirs publics ont engagé un processus destiné à mettre les communications à la portée des habitants du Zimbabwe en informatisant les écoles et les communautés, ce qui a encouragé ces dernières à faire partie du village planétaire en ligne. Malheureusement, des pirates informatiques opportunistes ont saisi cette occasion pour commettre des délits, en soustrayant des données d'une importance capitale auprès de ces communautés. Les informations personnelles et les communautés qui détiennent des dossiers personnels, par exemple les organismes publics et les institutions financières gouvernementales, sont particulièrement vulnérables dans la mesure où elles ne sont pas encore suffisamment préparées pour faire face aux conséquences de ces attaques et de ces vols. A ce jour, bon nombre de ces communautés se trouvent devant le dilemme suivant: comment continuer à développer leurs activités en ligne, sans risquer d'être victime d'activités criminelles destructrices.

25. A l'heure actuelle, le gouvernement élabore et met en place une stratégie nationale de cybersécurité destinée à promouvoir encore la cybersécurité à tous les niveaux de la société. Dans cette optique, une loi visant à freiner l'utilisation des TIC à des fins délictueuses et à protéger les flux d'information à l'intérieur des frontières du Zimbabwe a été adoptée. Cette loi, connue sous le nom de Loi sur l'interception des communications [Chapitre 11:20], est entrée en vigueur en 2007. Elle a pour but de surveiller les communications lors de leur transmission par l'intermédiaire des réseaux TIC du Zimbabwe et prévoit la mise en place d'un Centre de surveillance. Ce Centre doit encore être créé, tout comme la passerelle internationale unique. M. Ngoma a expliqué que les principaux obstacles à la mise en oeuvre de ces programmes étaient la pénurie de crédits pour l'acquisition des systèmes nécessaires, les menaces globales qui pèsent sur les systèmes et réseaux en place et la pénurie de professionnels qualifiés et de programmes éducatifs dans le domaine de la sécurité de l'information et des réseaux.

26. Violet Magagane, Regulatory and Public Policy, Telkom South Africa, a ensuite présenté une "Etude de cas sur la collaboration entre les secteurs public et privé: Telkom South Africa"[18], et a donné un aperçu de

---

16 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

17 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/ngoma-zimbabwe-security-culture-lusaka-aug-08.pdf.

18 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/magagane-telkom-SA-case-study-lusaka-aug-08.pdf.

la stratégie adoptée par Telkom dans un environnement en mutation constante, faisant observer que Telkom était responsable de l'une des infrastructures essentielles de la République sudafricaine. Elle a relevé que la cybersécurité et les cybermenaces connexes figuraient sur la liste des 10 risques majeurs pour le pays. Elle a également souligné que d'après les estimations, les coûts liés à la mise en place de la cybersécurité étaient très élevés. Mme Magagane a présenté le Centre national d'exploitation du réseau (NNOC), qui est responsable de la cybersécurité au niveau national. Elle a échangé des informations sur la structure qui a été mise en place et a fait observer qu'une permanence était assurée 24 heures sur 24 pour faire en sorte que les attaques ou menaces éventuelles pour les systèmes soient contrôlées et traitées instantanément. Des tests de sécurité destinés à évaluer les menaces et les failles du système sont effectuées quotidiennement pour réduire le plus possible les dommages et les délais de rétablissement à la suite de cyberattaques. Bon nombre des activités que Telkom projette de mener à bien dans le domaine de la sécurité devront être achevées en 2010, date à laquelle se tiendra la Coupe mondiale de football en République sudafricaine.

27. Mme Magagane a ensuite déclaré que les choix technologiques de Telkom dans l'environnement actuel en pleine évolution visent à assurer la sécurité des infrastructures de télécommunication, à mesure que les réseaux traditionnels évolueront vers les réseaux de prochaine génération, et à garantir le respect de la stratégie et de l'intégration technologiques (TSI). Cette stratégie prévoit la protection des ressources de bout en bout, l'évolution transparente des technologies dans leur ensemble ainsi que l'adoption de mesures de sécurité rigoureuses dans les réseaux d'arrivée et de départ. L'intervenante a également parlé de la situation actuelle concernant la Loi sur les communications et transactions électroniques 200, qui fournit un cadre permettant de lutter contre la cybercriminalité, et a souligné la nécessité de réexaminer cette loi pour tenir compte de l'évolution que connaît l'environnement actuel. Pour conclure, Mme Magagane a préconisé l'établissement d'un forum régional, qui aurait pour mission d'encourager la compétitivité et la mise en place d'une infrastructure des télécommunications plus efficace et plus sûre. L'intervenante a estimé qu'il fallait avant tout, pour aller de l'avant, promouvoir la coopération régionale afin de renforcer la cybersécurité, en améliorant l'échange d'informations, la formation et l'enseignement.

28. Isabel Nshimbe, analyste informatique, Marché commun de l'Afrique de l'Est et de l'Afrique australe (COMESA), a présenté la stratégie du COMESA, qui vise à amener les pays à travailler en collaboration étroite pour renforcer les capacités de cybersécurité, dans l'exposé intitulé "Stratégie du COMESA pour lutter contre la cybercriminalité"[19]. Mme Nshimbe a présenté aux participants certaines des activités menées par le COMESA dans le domaine de la cybersécurité et a fait observer que la sécurité n'était pas un produit, mais un processus auquel tout un chacun devait participer. Elle a signalé certains faits intéressants qui se sont produits en Zambie dans les domaines de la cybersécurité et de la cybercriminalité, par exemple l'attaque dont le site web du Gouvernement zambien a été victime en 1999 et au cours de laquelle des pirates informatiques ont eu accès à des comptes personnels de courriers électroniques et à d'autres informations personnelles. Mme Nshimbe a expliqué que la stratégie du COMESA en matière de cybersécurité visait à faire une large place aux personnes concernées, aux utilisateurs des différentes technologies et aux personnes qui participent d'une manière ou d'une autre aux processus associés. L'effet dissuasif à l'intérieur du réseau du COMESA intervient à trois niveaux différents: sécurité dans les réseaux, les services et la couche application et auprès des utilisateurs finals et de leurs ordinateurs. L'intervenante a présenté des statistiques indiquant que 98% des messages électroniques qui entrent quotidiennement dans le système du COMESA sont des messages spam.

29. Mme Nshimbe a poursuivi en donnant des précisions sur certaines activités actuelles et prévues en matière de cybersécurité au niveau régional. En vertu du programme de cyberlégislation, une étude sur ce sujet a été effectuée et des ateliers sur la question ont eu lieu en 2007 et 2008. Cette étude et les ateliers correspondants portaient sur quatre domaines différents, mais interdépendants, à savoir: la certitude juridique, la sécurité juridique, la protection juridique et les mesures de dissuasion juridiques. Dans ce dernier domaine, l'intervenante a cité les études sur les initiatives de réforme du droit, y compris du droit pénal matériel et du droit procédural, et la nécessité de renforcer la coopération internationale. Mme Nshimbe a évoqué la possibilité de créer une entité régionale ou internationale chargée de la cybercriminalistique, pour aider les pays de la région à mettre en place des moyens et des compétences techniques en matière de police scientifique, et à échanger des ressources à cet égard.

Session 4: Organisation des activités nationales de cybersécurité/CIIP et études de cas par pays: fondements juridiques et mesures d'application

30. Pour prévenir, détecter et réprimer la délinquance informatique et l'utilisation délictueuse des TIC, il faut une législation adaptée, ainsi qu'une coordination juridique et des mesures exécutoires au niveau international. A cette fin, il est nécessaire d'actualiser les dispositions, les procédures et les grands principes du droit pénal, pour remédier aux incidents en matière de cybersécurité et lutter contre la cybercriminalité. En conséquence, de nombreux pays ont modifié leur code pénal ou ont entrepris de le

---

19 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/nshimbi-comesa-cybercrime-activities-lusaka-aug-08.pdf.

faire, conformément aux conventions et recommandations internationales. Les participants à la session 4 ont analysé la nécessité de mettre en place des fondements juridiques solides et d'adopter des mesures exécutoires efficaces. Le modérateur de la session 4, Lucky Waindi-Kulecho, responsable juridique de la Commission des communications du Kenya (Kenya), a présenté les orateurs, puis a mis en lumière la nécessité d'intensifier la collaboration entre les pays dans ce domaine.

31. Marco Gercke, Conférencier de l'Université de Cologne (Allemagne), a ouvert la session en donnant un aperçu de certains "Fondements juridiques et principes de base de l'application des lois"[20], en exposant la position actuelle de la communauté internationale s'agissant de la révision des législations existantes et l'élaboration de nouvelles législations pour ériger en infraction pénale l'utilisation délictueuse des TIC. M. Gercke a fait observer que de nouveaux délits et de nouveaux problèmes apparaissaient constamment avec l'Internet et que de ce fait, il fallait réexaminer et mettre à jour en permanence les législations nationales. Il faut que les pays et les parties prenantes examinent en premier lieu les techniques concernées et déterminent de quelle manière elles sont utilisées à des fins délictueuses, puis protéger les utilisateurs par le biais d'une nouvelle législation, sans perdre de vue qu'il y a toujours un délai entre le moment où un délit est reconnu et celui où la loi est adaptée. Même si les nombreux problèmes que pose l'Internet appellent des solutions juridiques, tous les problèmes ne nécessitent pas des solutions de cette nature. En conséquence, les pays ne doivent pas envisager d'ériger en fractions pénales des activités sur l'Internet qui ne le seraient pas en dehors de l'Internet. M. Gercke a relevé qu'un fondement juridique offre un cadre permettant d'étudier, de poursuivre et de décourager la cybercriminalité, de promouvoir la cybersécurité et d'encourager le commerce.

32. M. Gercke a souligné que même si l'on s'appuie sur une législation nationale, régionale et internationale en matière de cybrcriminalité, il est important et nécessaire de poursuivre l'harmonisation des législations. Il a relevé qu'il existait plusieurs initiatives internationales pour la cybersécurité et la lutte contre la cybercriminalité et que toutes avaient un rôle à jouer. En ce qui concerne la Convention de Budapest sur la cybercriminalité, M. Gercke a expliqué que cet accord couvrait tous les domaines en rapport avec la cybercriminalité (y compris le droit pénal matériel, le droit procédural et la coopération internationale) et pouvait s'appliquer aux pays de "common law" comme aux pays de droit romain. M. Gercke également a fait valoir que pour les pays en développement, la recherche de solutions adéquates aux problèmes de la cybercriminalité était un défit majeur. L'élaboration et la mise en oeuvre d'une stratégie nationale de cybersécurité, y compris de lutte contre la cybercriminalité, est un processus de longue haleine, quelquefois plutôt onéreux, ce qui risque d'empêcher certains pays de prendre les mesures qui s'imposent. Chaque pays doit donc impérativement se forger les capacités et les compétences nécessaires pour revoir sa législation, enquêter sur les cas d'utilisation abusive ou délictueuse de ses réseaux et veiller à ce que les infractions commises par les délinquants qui les attaquent ou les exploitent soient réprimées.

33. Ehab Elsonbaty, Premier juge d'instruction, Tribunal de Damanhour, Egypte, a donné un aperçu, dans son exposé "Etude de cas par pays et vue d'ensemble - Fondements juridiques et mesures exécutoires"[21], de certains des instruments juridiques qui sont actuellement utilisés pour lutter contre la cybercriminalité en Egypte. Il a fait remarquer qu'étant donné que la cybercriminalité progressait beaucoup plus rapidement que la criminalité traditionnelle, et que les infrastructures essentielles étaient de plus en plus gérées par des ordinateurs et des réseaux, les règles du système juridique égyptien régissant la cybercriminalité étaient en cours de révision. Tous les pays de la région, et au-delà, doivent veiller à ce que les dispositions de leur droit pénal soient remaniées pour tenir compte de la nature particulière de la cybercriminalité, a-t-il ajouté. Pour procéder à cette mise à jour, on pourra modifier certains articles concernant les délits classiques commis par l'intermédiaire de nouveaux supports, en en supprimant d'autres qui ne sont pas appropriés, voire édicter de nouvelles règles pour traiter des questions entièrement nouvelles. M. Elsonbaty a fait observer que les niveaux des sanctions, qu'il s'agisse de peines d'emprisonnement ou d'amendes, devraient également être réexaminés. Il a également rappelé qu'il était important de concevoir des programmes de formation à l'intention des services chargés de faire respecter la loi, des magistrats ainsi que des juges et des législateurs. La cybercriminalité a un caractère international, d'où la nécessité de trouver une solution internationale comprenant des règles de droit pénal matériel et de droit procédural et prévoyant une coopération internationale. A cet égard, l'intervenant a évoqué les travaux menés en Egypte et a indiqué qu'il espérait qu'une loi moderne sur la cybercriminalité serait adoptée en Egypte. Enfin, M. Elsonbaty a indiqué que le réseau high-tech "24/7" du G8 était un point de contact utile pour examiner les cas dans lesquels il était nécessaire d'obtenir des preuves électroniques transfrontières.

---

20 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/gercke-legal-framework-lusaka-aug-08.pdf.

21 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/elsonbaty-legislation-enforcement-lusaka-aug-08.pdf.

34. Garry Mukelabai, Directeur, Information Systems, Autorité des communications de la Zambie (CAZ), Zambie, a ensuite présenté un exposé intitulé "Etude de cas par pays: la cybersécurité en Zambie"[22]. Il a indiqué que si la Zambie avait fait oeuvre de pionnier en matière d'Internet dans la région, le nombre d'internautes, qui s'établissait à 16 830 (soit 0,144 pour cent habitants) demeurait encore très faible. Cela s'explique par le coût élevé de l'accès, la médiocrité des infrastructures, le manque de sensibilisation parmi les utilisateurs et l'insuffisance des compétences dans le domaine des TIC parmi les utilisateurs finals et les professionnels. La Zambie a compris que la cybersécurité était très importante, étant donné que des secteurs clés de l'économie d'un pays s'appuient déjà aujourd'hui sur des réseaux IP pour les transactions commerciales et la fourniture de services énergétiques, de transport, d'approvisionnement en eau, bancaires et d'autres services publics essentiels et que pour tirer le plus grand avantage économique possible de l'utilisation des réseaux IP, il est nécessaire que ces réseaux soient fiables et sécurisés.

35. En ce qui concerne les mesures juridiques visant à lutter contre la cybercriminalité, diverses initiatives ont été prises en Zambie. Bien que la Loi de 2004 sur l'utilisation délictueuse de l'informatique soit en vigueur, les changements survenus depuis sa mise en application font que cette loi n'est plus adaptée pour répondre aux besoins actuels. Par ailleurs, M. Mukelabai a cité la loi de 2007 sur les TIC et les politiques liées aux TIC, qui est actuellement examinée par le Parlement zambien, ainsi que les initiatives actuelles visant à rédiger une loi sur la sécurité des TIC et une loi sur la signature électronique. L'intervenant a souligné qu'il était urgent de dispenser une formation aux agents de la force publique et aux autorités judiciaires du pays. Il a indiqué qu'à ce jour, les cas de cybercriminalité restent peu nombreux en Zambie, mais a cité un cas dans lequel le portrait du Président de la République de l'époque, M. Frederic Chiluba, avait été remplacé par une caricature. L'accusé a été poursuivi en justice au titre de la Loi sur les télécommunications de 1994, créée pour réglementer l'industrie téléphonique et les fournisseurs de services Internet, de sorte que l'accusation n'a pas été retenue. A l'époque, une Loi spécialement conçue pour traiter les délits informatiques était en cours d'élaboration et depuis, la police de la Zambie a été saisie de plusieurs cas de fraudes en ligne. A l'heure actuelle, le cinquième Plan national de développement et le projet "Zambie 2030" tiennent compte de la nécessité de veiller à ce que des mesures soient prises pour instaurer la confiance et la sécurité dans l'utilisation des TIC. Le 13ème volet de la politique correspondante dans le domaine des TIC, qui a été mis en oeuvre en mars 2007, porte sur "la sécurité dans la société de l'information". Selon cette politique, l'une des préoccupations majeures des sociétés connectées est la sécurité des informations qui transitent par l'intermédiaire de réseaux et de systèmes tels que les ordinateurs, des transactions financières, des dossiers médicaux, etc. A mesure que la Zambie intégrera les TIC, les problèmes de sécurité et les cas d'utilisation abusive augmenteront si aucune mesure corrective n'est prise, a estimé M. Mukelabai, qui a demandé aux différentes parties prenantes de faire le nécessaire pour veiller à ce qu'elles comprennent la nature de leurs responsabilités respectives pour rendre le cyberespace plus sûr. Afin de progresser sur la voie de la cybersécurité en Zambie, le Ministère des communications et des transports assure la coordination de la mise en place d'un organisme national chargé de la cybersécurité, qui aura pour tâche de superviser le fonctionnement des différents aspects de cette initiative nationale, y compris la gestion des incidents, la protection des infrastructures essentielles d'une information, la coordination nationale, la coopération régionale, les contrôles de sécurité et les initiatives de formation et de sensibilisation.

36. Thys Kazad Tshibind, Ingénieur, ARPTC (République démocratique du Congo), dans son "Etude de cas par pays: République démocratique du Congo"[23], a donné un aperçu des activités en cours de réalisation en République démocratique du Congo. La République démocratique du Congo va passer à la prochaine phase de développement et la sécurité représente un enjeu majeur à cet égard. La cybersécurité, ou plutôt l'absence de sécurité et de confiance dans l'Internet, ont des conséquences pour toutes les parties concernées, qu'il s'agisse des pouvoirs publics, des entreprises ou des utilisateurs, et tous les pays s'efforcent de concevoir les moyens les mieux appropriés pour sensibiliser davantage l'opinion à la cybersécurité, afin de créer un cyberespace sécurisé pour tous. M. Kazad a fait observer que bien que la République démocratique du Congo compte 200 000 internautes, que cinq entreprises sur dix soient connectées à l'Internet, que cinq banques sur dix aient recours à des transactions électroniques et à des cartes bancaires, il n'existe toujours pas de législation sur la cybersécurité dans le pays. Toutefois, certains délits ont été classés dans la catégories des délits classiques et sont ainsi couverts par la législation actuellement en vigueur. L'intervenant a cité la Loi 013 du 16 octobre 2002, qui porte sur les télécommunications en République démocratique du Congo, et a souligné que cette loi n'englobait pas les TIC et l'Internet, d'où la nécessité de la modifier radicalement.

37. M. Kazad a également évoqué certains problèmes rencontrés par la République démocratique du Congo pour concevoir des mesures de cybersécurité au niveau national. A cet égard, il a déploré le manque de synergie et de coordination internes, l'absence de juristes TIC, le fait que les TIC, tout comme

---

22 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf.

23 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/kazad-case-study-dem-rep-of-congo-lusaka-aug-08.pdf.

les problèmes qu'elles risquent de poser, sont généralement mal comprises par les décideurs, et que l'on connaît mal leur valeur ajoutée dans l'économie nationale. M. Kazad a conclu en formulant certaines recommandations à l'intention du groupe sur la manière de progresser dans ce domaine. Il a souligné la nécessité de clarifier ce que la région attend de la coopération régionale et internationale dans ce domaine et ce que l'on peut attendre du COMESA à cet égard. Il a expressément demandé au COMESA de conduire les travaux sur l'élaboration de directives en matière de cybersécurité pour les pays de la région et a prié les pays d'intégrer ces directives dans leur législation nationale. M. Kazad a également soumis aux participants une proposition visant à instituer une commission chargée de la sécurité au sein du COMESA et a suggéré que des ressources soient mises à la disposition des pays ayant besoin d'une assistance pour élaborer leurs cadres nationaux en matière de cybersécurité, de façon à mettre en place des moyens de cybersécurité qui font cruellement défaut dans les Etats Membres du COMESA.

38. M. Andrew Kisaka, Utilities Regulatory Agengy, Rwanda, a présenté le cas du Rwanda dans l'exposé intitulé "Cybersécurité et infrastructures essentielles de l'information: étude de cas par pays: Rwanda"[24], et a dressé le bilan de ce qui avait été fait à ce jour dans ce pays en matière de cybersécurité. Il a fait observer que le processus appelait des mesures spéciales pour orienter l'élaboration des lois et des législations connexes. Au Rwanda, le RURA (Rwanda Utilities Regulatory Agengy) est chargé de coordonner toutes les activités relatives à la cybersécurité. Le Rwanda a élaboré un Plan national sur les infrastructures de l'information et de la communication (NICI), qui comporte un plan d'action et des lignes directrices visant à faire passer le Rwanda d'une société rurale à une société basée sur le savoir à l'horizon 2020. La phase de 2006 du Plan, intitulée "Concevoir des solutions", consiste à mettre en oeuvre des "applications TIC" et tient compte de la nécessité d'examiner la cybersécurité et les questions connexes. Toutefois, il n'existe aucune politique concernant les applications TIC, ni aucun cadre réglementaire approprié et les problèmes de cybersécurité sont encore mal connus. Tels sont les problèmes auxquels le Rwanda est confronté dans la réalisation des objectifs du Plan NICI. Etant donné que la sécurité est une préoccupation majeure, M. Kisaka a indiqué que le RURA recherchait actuellement le meilleur moyen de garantir l'adoption d'une législation appropriée pour lutter contre l'utilisation des TIC à des fins délictueuses ou criminelles, et notamment contre les activités destinées à nuire à l'intégrité des infrastructures nationales essentielles de l'information.

39. En conclusion, le modérateur de la session, Lucky Waindi-Kulecho, juriste Communications Commission of Kenya, a présenté l'exposé intitulé "Etude de cas par pays: vers l'élaboration d'une législation sur la cybersécurité au Kenya"[25].

Session 5: Organisation des activités nationales de cybersécurité/CIIP et études de cas par pays: Dispositifs de gestion des incidents

40. Les participants à la session 5 ont examiné de manière détaillée les différents éléments nécessaires à la mise en place de moyens efficaces de gestion des incidents en donnant des exemples de pays de la région et du continent africain dans son ensemble. La solution au problème de la cybersécurité passe par la création, dans chaque pays, de capacités de veille, d'alerte et de réponse aux incidents informatiques permettant de prévoir, de détecter, de gérer les incidents qui se produisent dans le cyberespace et d'y réagir. Une gestion efficace de ces incidents nécessite une réflexion sur le financement, les ressources humaines, la formation, les capacités technologiques, les relations entre pouvoirs publics et secteur privé et les exigences juridiques. Une collaboration à tous les niveaux de l'Etat et avec le secteur privé, les milieux universitaires et les organisations régionales et internationales est indispensable pour sensibiliser l'opinion aux attaques potentielles et aux mesures à prendre pour y remédier. Le modérateur de cette session était Charles Munamie, Chef du Département des services de gestion des technologies et des systèmes de l'information du Ministère de l'information et de l'éducation civique du Malawi.

41. Helmi Rais, Directeur du CERT-TCC de la Tunisie, Agence nationale de la sécurité informatique de la Tunisie, a donné un aperçu, dans son exposé intitulé "Etude de cas par pays sur les capacités de gestion des incidents: CERT-TCC de la Tunisie"[26], du mandat, de la structure et des activités du CERT-TCC et de la manière dont les enseignements et l'expérience tirés de ces Centres peuvent aider les pays de la région qui envisagent ou qui sont en train de mettre en place des capacités nationales de gestion des incidents. En janvier 2003, le Conseil des Ministres, présidé par le Président, a pris la décision de créer une Agence nationale spécialisée dans la sécurité informatique et chargée de faciliter la mise en oeuvre de la stratégie nationale adoptée en 2002. En septembre 2005, l'équipe d'intervention en cas d'urgence informatique - Centre de coordination tunisien (CERT-TCC) a été mis en place. Le CERT-TCC s'occupe notamment de veille, d'alerte, de diffusion de l'information, de sensibilisation (différents types de

---

[24] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/kisaka-karangwa-rwanda-case-study-lusaka-aug-08.pdf.

[25] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/waindi-kenya-case-study-legislation-lusaka-aug-08.pdf.

[26] http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rais-cert-tcc-tunisia-case-study-lusaka-aug-08.pdf.

campagnes de sensibilisation), de développement d'une culture de la cybersécurité, information pour les juges, etc.), de partage, d'analyses, de collecte d'informations, de traitement des incidents, de coordination, etc. Le CERT-TCC fournit aussi des avis techniques spécialisés sur la sécurité informatique. M. Rais a noté en outre que la Tunisie était le seul pays ayant commencé à fournir ce service gratuitement aux banques et aux entreprises nationales, de sorte que ce service était très apprécié.

42. Lorsqu'ils réfléchissent au cadre dans lequel fonctionne un CERT-TCC et lorsqu'il s'agit d'assurer le traitement et la gestion des incidents au niveau national, la première chose que les pays doivent prendre en compte est la nécessité de faire partie d'un réseau de partenaires compétents pour obtenir des conseils et un appui. Le CERT-TCC collabore avec des partenaires de nombreux autres pays, est membre du réseau FIRST et fait partie de plusieurs listes de diffusion visant à échanger des informations aux niveaux national et international. Le CERT-TCC dispose d'une base de données sur les menaces et virus et publie actuellement les informations qu'il collecte afin de les envoyer régulièrement aux abonnés de ses listes de diffusion. La liste de diffusion compte actuellement 8 000 abonnés volontaires qui obtiennent des informations en français. Quotidiennement, l'équipe fait le point de la situation de la sécurité et s'efforce de collaborer avec d'autres CERT pour échanger des informations sur les failles existantes. M. Rais a également indiqué que le CERT-TCC avait conçu un outil de travail à source ouverte et qu'il était disposé à l'échanger gratuitement avec d'autres pays à l'échelle du continent. M. Rais a terminé son exposé en encourageant les pays du continent à mettre sur pied des CERT nationaux, en précisant que le CERT-TCC serait heureux d'aider les pays à créer de tels centres.

43. Akram Hamed, National Telecom Corporation, Soudan, a présenté un exposé intitulé "Etude de cas par pays sur le Soudan - Capacités de gestion des incidents"[27], qui traite des mesures prises actuellement par le Gouvernement soudanais dans le domaine de la cybersécurité. Il a donné un aperçu de la situation s'agissant de la pénétration de l'Internet au Soudan et a fait observer que deux entreprises de télécommunication fournissaient aujourd'hui des services Internet dans ce pays. Il a indiqué que le pays était conscient de l'importance de la sécurité pour continuer d'améliorer et d'étendre l'utilisation des services d'administration publique en ligne dans tout le pays. Afin de renforcer la cybersécurité au Soudan, le Gouvernement a pris diverses mesures destinées à renforcer les aspects techniques de la cybersécurité, de manière à tenir compte de l'évolution de la situation au niveau international. Il a notamment mis en place des mesures de protection dans tous les nouveaux réseaux locaux, au niveau gouvernemental, et à sensibilisé davantage les internautes, les professionnels et les décideurs aux dangers que présente l'Internet. En outre, deux lois ont été adoptées pour faire face aux problèmes de plus en plus préoccupants que pose la cybercriminalité. La Loi sur les transactions électroniques (2007) traite de la passation de marchés électroniques, des transactions, des signatures électroniques et d'autres instruments électroniques, tandis que la Loi sur la criminalité informatique (2007) porte sur les délits de nature financière, associés aux données et au chantage, aux délits liés à l'ordre public ou à la moralité publique, aux délits concernant la propriété intellectuelle, etc. Parmi les mesures structurelles prises pour lutter contre la criminalité électronique figure un programme visant à encourager les fournisseurs de services Internet à tenir des fichiers d'enregistrement pour les internautes soudanais, et des programmes destinés à gérer les travaux des cybercafés dans le pays.

44. Le Président de la session, M. Munamie, a conclu en donnant un aperçu de la situation de la cybersécurité au Malawi et a souligné que ce pays pouvait s'inspirer de l'expérience des pays voisins, afin que le cyberespace du Malawi résiste davantage aux menaces.

Session 6: Organisation des activités nationales de cybersécurité/CIIP et études de cas par pays: une stratégie nationale en matière de cybersécurité

45. De plus en plus, les réseaux électroniques sont utilisés à des fins délictueuses ou qui peuvent porter préjudice à l'intégrité des infrastructures essentielles et entraver la diffusion des avantages des TIC. Pour parer à ces menaces et protéger les infrastructures, chaque pays doit mettre en place un plan d'action global, englobant les questions techniques, juridiques et politiques, associé à une coopération régionale et internationale. Il faut donc se demander sur quel élément doit porter l'élaboration de stratégies nationales pour la cybersécurité et la protection des infrastructures essentielles de l'information, quels partenaires doivent s'impliquer et s'il existe des exemples de cadres dont des pays pourraient s'inspirer? La session 6 avait pour objet d'analyser en détail différentes options et bonnes pratiques dans le domaine de la cybersécurité et de définir les principaux modules qui pourraient aider les pays à élaborer des stratégies nationales pour la cybersécurité et la CIIP. A partir des exposés présentés antérieurement au cours des sessions 2, 3, 4 et 5 du Forum, qui traitaient des différents éléments nécessaires pour concevoir une approche nationale en matière de cybersécurité et de CIIP, Patrick Mwesigwa, Directeur technique de la Commission des communications de l'Ouganda, a animé cette session, consacrée au dernier élément qui relie toutes les autres composantes, à savoir l'élaboration générale d'une stratégie nationale en matière de cybersécurité.

---

27 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/hamed-sudan-case-study-lusaka-aug-08.pdf.

46. Mme Nafissatou Diallo, analyste de programme principal du Département des technologies de l'information et de la communication (TIC) des Seychelles, a présenté le premier exposé de cette session, intitulé "Etude de cas par pays: la situation de la cybersécurité et des TIC aux Seychelles"[28]. Mme Diallo a fait le point de la situation des Seychelles en matière de cybersécurité. Elle a précisé que trois lois avaient été adoptées dans le pays, à savoir: la loi sur les transactions électroniques (2001), la loi sur l'utilisation délictueuse de l'informatique (1998) et la Loi sur la protection des données (2003) et que le Gouvernement envisageait de les modifier. Elle a souligné que de nombreuses parties prenantes avaient pris part au processus d'élaboration d'une législation et de politiques liées à la cybersécurité et a noté que ces mêmes acteurs devraient être associés à la définition des aspects cybersécurité des politiques et législations futures.

47. En outre, Mme Diallo a expliqué que les Seychelles mettaient actuellement en oeuvre un processus visant à transférer tous les services publics dans un même réseau. Les Seychelles n'ont pris conscience que récemment de la nécessité de sensibiliser les partenaires sur les menaces qui pèsent sur la cybersécurité, l'utilisation des téléphones mobiles et la protection des données personnelles. Les Seychelles ont fait oeuvre de pionnier dans la région pour ce qui est du déploiement des TIC et la publication du Plan national sur les TIC jette les bases de l'élaboration d'un Plan stratégique national global pour les TIC. Ce Plan servira de guide pour orienter le développement des TIC aux Seychelles, a déclaré Mme Diallo, faisant observer qu'il fallait accorder une plus large place à la cybersécurité. Parmi les principaux problèmes qui se posent en matière de cybersécurité au niveau national figurent la mise en application limitée des lois existantes (et la nécessité de modifier les lois en vigueur), le manque de sensibilisation du grand public sur les TIC en général et sur la cybersécurité en particulier, les compétences techniques et le savoir-faire limités dans le domaine de la cybersécurité, l'insuffisance de la formation en la matière et le dialogue restreint entre les parties concernées et les différents acteurs. En conclusion, et compte tenu des interventions de représentants et d'experts d'autres pays, Mme Diallo a estimé que les politiques nationales actuelles n'accordaient pas une place suffisante à la cybersécurité.

48. Patrick Mwesigwa, Directeur, Technology and Licensing, Uganda Communications Commission, Ouganda, a donné une vue d'ensemble des initiatives actuelles et prévues en matière de cybersécurité, dans son exposé intitulé "Etude de cas par pays: formulation d'une législation en matière de cybersécurité en Ouganda"[29]. M. Mwesigwa a mis l'accent sur les progrès réalisés en vue de l'élaboration d'une législation sur la cybersécurité. Il a fait mention des trois principaux instruments actuellement en vigueur en Ouganda, à savoir la Loi sur les transactions électroniques (2003), la Loi sur l'utilisation délictueuse de l'informatique (2003) et la Loi sur les signatures électroniques (2003). Il a également donné des informations sur les mesures prises par d'autres pays de la région d'Afrique orientale, en vue d'harmoniser les lois et législations relatives à la cybersécurité. Dans les pays d'Afrique de l'Est, l'harmonisation des lois s'effectuera en deux temps. La première phase sera axée sur la législation pour les transactions, les signatures et les authentifications électroniques, la protection des données et la confidentialité, la protection des consommateurs et les délits informatiques, tandis que la deuxième phase portera sur les droits de propriété intellectuelle, les noms de domaine, la fiscalité et la libre-circulation de l'information. Dans cette optique, un certain nombre de réunions régionales ont été organisées et un cadre juridique devrait être adopté par les organes compétents de la CAE en novembre 2008. Par la suite, les Etats partenaires devraient promulguer la nouvelle législation sur la cybersécurité en 2010. M. Mwesigwa a conclu en insistant sur la nécessité de sensibiliser les décideurs, les opérateurs de réseaux et les particuliers sur les questions liées à la cybersécurité et a encouragé tous les pays à mettre en place des cadres juridiques solides pour parer aux menaces liées à la cybersécurité. En outre, il a fait observer que comme le cyberespace ne connaît pas de frontières, la coopération internationale est primordiale pour garantir un environnement en ligne sécurisé.

Session 7: Examen et discussion: organisation des activités nationales de cybersécurité/CIIP

49. La session 7, dernière session de la journée, avait pour but d'examiner et d'analyser de manière plus approfondie les éléments de l'approche visant à organiser les activités nationales de cybersécurité, et de recenser les principaux enseignements tirés des exposés qui leur étaient consacrés et des études de cas par pays, en vue de la dernière session du Forum. Pour contribuer à l'organisation de la session, les modérateurs, Abu Sufian E Dafalla, responsable des télécommunications du Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA), et Marcelino Tayob, Chef du Bureau de zone de l'UIT pour l'Afrique australe à Harare (Zimbabwe), ont demandé à quatre intervenants de rendre compte des principaux enseignements qu'ils avaient tirés des sessions antérieures et, si possible, de formuler des propositions et des recommandations sur les mesures à prendre concrètement en Afrique de l'Est et en Afrique australe.

---

28 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/diallo-case-study-seychelles-lusaka-aug-08.pdf.

29 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/diallo-case-study-seychelles-lusaka-aug-08.pdf.

50. Joseph Richardson, consultant (Etats-Unis d'Amérique), a fait remarquer que les interventions faites ces derniers jours militaient en faveur d'une collaboration entre les gouvernements et le secteur privé dans le domaine de la cybersécurité et a indiqué qu'il existait de nombreuses manières différentes de collaborer avec l'industrie. Il a ajouté que tous les pays étaient confrontés au même problème, à savoir l'impossibilité d'associer au processus tous les partenaires de l'industrie, tous les différents secteurs et les différentes entreprises. En conséquence, les pays doivent plutôt rechercher un moyen de réunir ces représentants au sein d'associations professionnelles, qui pourraient à leur tour débattre en leur nom. Il faut poursuivre les travaux pour définir les cadres nécessaires à cette collaboration. Par ailleurs, il faut envisager la collaboration avec le secteur privé sous un autre angle. Il est nécessaire en particulier de réfléchir au rôle que jouent les relations non seulement avec le secteur privé, mais aussi avec d'autres instances des gouvernements. A terme, il conviendra de veiller à ce que des ministères autres que ceux des communications soient associés aux forums, ateliers et activités consacrés à la cybersécurité. L'orateur a souligné que d'après les observations formulées jusqu'à présent, l'approche retenue pour organiser les activités nationales en matière de cybersécurité et l'outil d'auto-évaluation de l'UIT sont d'une grande utilité pour les pays de la région et que des mesures concrètes pourraient être prises pour aider tous les pays à utiliser ces outils.

51. Ehab Elsonbaty, Juge principal, Tribunal de Damanhour (Egypte), a fait observer qu'il fallait tirer parti de la dynamique actuelle et opter pour des mesures concrètes en utilisant les instruments en place dans le domaine juridique et en les adaptant, en fonction des systèmes nationaux. A propos de la question de savoir s'il faut édicter une seule loi ou des lois distinctes, l'orateur a fait observer qu'en matière de cybercriminalité, plusieurs lois seront nécessaires. Il a estimé à cet égard que la cybersécurité, la protection des données et la confidentialité ainsi que la liberté de l'information, devaient faire l'objet de trois lois différentes. M. Elsonbaty a également insisté sur la nécessité d'instaurer un dialogue social en matière de cybersécurité et a expliqué que les discussions en la matière ne pouvaient se limiter à la nécessité de sensibiliser les utilisateurs. S'agissant de la création éventuelle d'un groupe d'études du COMESA chargé d'examiner les questions de cybersécurité, l'orateur a estimé qu'il fallait tenir compte des travaux de la CAE et d'autres pays de la région. Dans un premier temps, il serait bon d'avoir une vue d'ensemble de la situation juridique dans les pays de la région.

52. John Carr, Secrétaire de la Children's Charities' Coalition on Internet Safety (CHIS), Royaume-Uni, a fait valoir que la protection des enfants dans le cyberespace était importante à plusieurs titres: 1) en tant que telle, étant donné que la protection des enfants, ressource la plus précieuse mais aussi la plus vulnérable, est un devoir pour tous les pays; 2) les gouvernements et les responsables politiques peuvent aussi veiller à la nécessité de protéger les enfants; et 3) la protection des enfants sur l'Internet constitue un moyen utile de permettre au secteur public de collaborer avec le secteur privé.

53. Helmi Rais, Directeur, Centre CERT-TCC Tunisie, Agence nationale pour la sécurité informatique (Tunisie) a indiqué que toute stratégie nationale de cybersécurité devait comporter des activités liées aux Centres CERT/CSIRT. Il a également relevé que la protection des infrastructures de l'information était importante pour assurer la continuité globale des activités menées par le secteur public. M. Rais a fait valoir que la législation jouait certes un rôle important à cet égard, mais ne constituait pas le seul élément à prendre en compte dans le domaine de la cybersécurité. La collaboration entre les pays et les points de contact revêt plus d'importance que les lois et les législations en cas d'incident. Etant donné que la Tunisie possède une certaine expérience en matière de création de Centres CERT, le CERT-TCC serait heureux de partager ses connaissances à cet égard et de contribuer ainsi à l'approche globale adoptée par l'Afrique, en vue de la mise en place d'un Centre africain pour la sécurité de l'information.

Sessions 8 et 9: Kit pratique UIT pour l'auto-évaluation nationale en matière de cybersécurité/CIIP: exercice

54. Les sessions 8 et 9 du Forum avaient pour but de donner davantage de renseignements sur le kit de l'UIT pour l'auto-évaluation nationale en matière de cybersécurité/CIIP et de procéder à des échanges de vues détaillés sur ce sujet. Les intervenants ont présenté le processus d'auto-évaluation, qui vise à aider les pouvoirs publics à mieux comprendre les activités existantes, à recenser les points faibles qui doivent faire l'objet d'une attention particulière et à hiérarchiser par ordre de priorités les initiatives nationales. Le Kit pratique UIT pour l'auto-évaluation nationale en matière de cybersécurité/CIIP vise à aider les pouvoirs publics à évaluer leurs politiques, procédures, normes, institutions et relations existantes à la lumière des besoins nationaux, pour améliorer la cybersécurité et prendre en compte la protection des infrastructures essentielles de l'information. Cet outil s'adresse aux dirigeants des gouvernements et examine sous l'angle de la gestion et de la politique les grandes orientations, le cadre institutionnel et les relations liées à la cybersécurité. Il a pour but de donner un aperçu de l'état actuel des politiques et des capacités nationales, des institutions et des relations institutionnelles, du personnel et des compétences techniques, des relations entre les entités publiques et des relations entre les gouvernements, l'industrie et d'autres entités du secteur privé. Joseph Richardson, consultant, Etats-Unis d'Amérique, a animé les deux sessions.

Session 10: Coopération régionale et internationale

55. La coopération régionale et internationale est extrêmement importante pour promouvoir les initiatives prises au niveau national et faciliter le dialogue et les échanges. Les problèmes que posent les cyberattaques et la cybercriminalité sont de dimension mondiale et sont lourds de conséquence. Ils ne peuvent être réglés qu'en définissant une stratégie cohérente, dans le cadre de la coopération internationale, en tenant compte des rôles joués par les différentes parties prenantes et des initiatives existantes. En tant que coordonnateur de la grande orientation C5 du SMSI, qui a pour but de renforcer la confiance et la sécurité dans l'utilisation des TIC, l'UIT procède à des échanges de vues avec les principales parties prenantes sur la meilleure manière de répondre de manière concertée aux problèmes de plus en plus préoccupants qui se posent en matière de cybersécurité. Ainsi, le Programme mondial cybersécurité (GCA) de l'UIT permet d'établir un dialogue visant à tirer parti des initiatives existantes et à collaborer avec des sources de compétences reconnues, afin d'élaborer des stratégies mondiales destinées à accroître la confiance et la sécurité dans la société de l'information. Les participants à cette session, animée par Abu Sufian E Dafalla, responsable des télécommunications, Marché commun de l'Afrique de l'Est et de l'Afrique australe (COMESA), ont passé en revue certaines initiatives actuelles, afin d'informer les participants et de poursuivre les discussions pour définir les nouvelles mesures à prendre et l'action concrète à envisager pour encourager et promouvoir la coopération internationale afin de renforcer la cybersécurité.

56. Sizo Mhlanga, Conseiller régional, TIC, Division des sciences et des technologies, Commission économique des Nations Unies pour l'Afrique (UNECA) a présenté un exposé intitulé "Perspectives régionales de la CAE sur la cybersécurité"[30], qui traite des mesures prises par la CAE pour contrer les menaces toujours plus nombreuses qui pèsent sur la cybersécurité. Le fait que la connectivité soit limitée et que les internautes soient relativement peu nombreux sont des facteurs qui protègent actuellement les cibles africaines potentielles contre la plupart des cyberattaques, a déclaré M. Mhlanga. Toutefois, il a fait remarquer que, parallèlement, les pays africains restent très vulnérables à la plupart des attaques de grande envergure, en raison de technologies de base insuffisantes et de logiciels vulnérables. Il a indiqué que le problème était encore aggravé par le manque de sensibilisation des internautes sur la cybersécurité, par le fait que certains utilisateurs étaient mal informés ou mal conseillés, et par l'existence d'utilisateurs malveillants. En conséquence, la capacité accrue des TIC, conjuguée à des environnements juridiques, réglementaires et politiques insuffisamment développés ou inexistants et à l'insuffisance des techniques de sécurité, ont pour conséquence que le continent africain est un point d'entrée lucratif pour les cyberdélinquants, qui l'utilisent comme plate-forme pour coordonner et lancer des attaques. A cet égard, M. Mhlanga a donné un aperçu de l'état de préparation des pays africains en matière d'administration publique en ligne et a présenté des données sur ce sujet concernant différents groupes régionaux africains (COMESA, SADC et CAE), en comparant ces données à celles de certains pays européens. Il ressort de ces données que le principal problème tient à l'absence d'infrastructures TIC.

57. M. Mhlanga a également donné des précisions sur l'"AISI", qui est un projet de développement des TIC en Afrique. Lancé en 1996, ce projet constitue également un cadre de coopération pour les partenaires désireux de favoriser le développement des TIC sur le continent africain. Les activités liées à l'initiative AISI englobent l'élaboration de grandes orientations, la formation et le renforcement des capacités, les applications sectorielles et le développement des infrastructures. Dans le cadre de l'AISI, la nécessité de renforcer la cybersécurité se traduit par la formulation de politiques et de stratégies nationales et

---

30 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mhlanga-uneca-lusaka-aug-08.ppsm.

régionales dans le domaine des TIC et par la mise au point de cadres juridiques. L'UNECA apporte un appui aux pays de la région pour l'élaboration de stratégies régionales et nationales, y compris de politiques et d'applications sectorielles telles que celles nécessaires aux cyberapplications. A cet égard, l'UNECA considère que la cybersécurité est une application sectorielle qui doit être intégrée dans les politiques générales et dans les cyberstratégies en matière de TIC qui sont actuellement définies et mises en oeuvre.

58. M. Mhlanga a également parlé de l'action entreprise par l'UNECA pour aider les pays à concevoir un cadre africain de la cybersécurité par le biais du réseau ePol-NET (réseau mondial des ressources en cyberpolitiques (ePol-NET)). Le Burkina Faso, le Ghana, le Kenya et le Mozambique participent à ce programme, qui est axé sur les besoins politiques, législatifs et de sécurité des infrastructures. A cet égard, plusieurs projets sont en cours de réalisation dans ces pays. M. Mhlanga a conclu en encourageant les pays de la région à continuer de participer à des initiatives visant à intensifier la coopération régionale et internationale, sachant que l'UNECA continuera d'apporter un appui aux gouvernements pour mettre en place des mesures de cybersécurité et pour établir le Forum africain sur les infrastructures publiques essentielles.

59. Jacquot Rasemboarimanana, informaticien, Commission de l'océan Indien (COI), a ensuite donné un aperçu de "La communication, la connectivité et la sécurité dans la région COI"[31]. Dans son exposé, il a fait le point sur le développement des TIC dans les pays de l'océan Indien et sur leur niveau de connectivité et de sécurité. A propos de la situation actuelle de la cybersécurité dans la région, il a fait observer que les politiques nationales en matière de sécurité de l'information prévoyaient que, lors de l'établissement de centres de communication, ceux-ci devaient être mis en place et gérés sans perdre de vue les impératifs de sécurité. En ce qui concerne l'évaluation, la prévention et la formation, M. Rasemboarimanana a précisé que des programmes de formation et de vulgarisation sur l'utilisation sécurisée de l'Internet étaient en cours de mise en place. Il a noté que bien souvent, le problème était de nature culturelle ou tenait au fait qu'il n'existait aucune culture de la sécurité à tous les niveaux de la société. Il fallait donc intégrer la notion de cybersécurité dans l'utilisation courante des TIC, dans la définition des besoins de formation, dans l'enseignement et les programmes scolaires.
M. Rasemboarimanana a souligné qu'avec la multiplication des risques, il deviendrait encore plus urgent de promouvoir la coopération et la coordination internationales entre les différents acteurs. Il a encouragé les pays de la région à faire de la cybersécurité une priorité nationale et à prendre part aux activités communes menées par l'UIT et le COMESA pour renforcer la cybersécurité.

60. Marco Obiso, Conseiller de la Division des applications TIC et de la cybersécurité, Bureau de développement des télécommunications de l'UIT (BDT), était le dernier intervenant à prendre la parole lors de cette session et a présenté un exposé intitulé "Programme mondial cybersécurité (GCA) de l'UIT: cadre de coopération internationale en matière de cybersécurité"[32]. Par le biais du GCA, l'UIT ouvre la voie à un renforcement de la coopération mondiale dans l'optique d'une sécurisation accrue du cyberespace. L'UIT, qui compte 191 Etats Membres et plus de 700 Membres de Secteurs, parmi lesquels figurent de grands noms de l'industrie, est particulièrement bien placée pour favoriser la coopération internationale dans le domaine de la cybersécurité. Forte de la longue expérience qu'elle a acquise en matière de cybersécurité, l'UIT a été chargée par des dirigeants du monde entier, lors du Sommet mondial sur la société de l'information (SMSI), de jouer un rôle de premier plan au titre de la grande orientation C5 "Etablir la confiance et la sécurité dans l'utilisation des TIC". L'UIT, par le biais de ses trois Secteurs, à savoir l'UIT-R, l'UIT-T et l'UIT-D, oeuvre en faveur d'une approche mondiale concertée et harmonisée pour assurer la cybersécurité. M. Obiso a fait remarquer qu'en tant que coordonnateur unique pour la grande orientation C5 du SMSI, l'UIT collaborait avec toutes les principales parties prenantes, afin de trouver le meilleur moyen de répondre de manière concertée aux problèmes de plus en plus préoccupants liés à la cybersécurité. A cet égard, le Programme mondial cybersécurité de l'UIT fournit les orientations stratégiques propres à encourager la coopération internationale. L'orateur a également fait mention du rôle prépondérant que jouent les Secteurs de l'UIT, notamment l'UIT-D, en concrétisant les stratégies convenues en mesures et en projets qui seront appliquées conjointement avec d'autres partenaires.

Session 11: Synthèse, recommandations et activités futures

61. La dernière session de la réunion, animée par Abu Sufian E Dafalla, responsable des télécommunications du Marché commun pour l'Afrique de l'Est et l'Afrique australe (COMESA), et Marcelino Tayob, Chef du bureau de zone de l'UIT pour l'Afrique australe à Harare (Zimbabwe), ont présenté certains des principaux résultats de la réunion et ont défini un ensemble de recommandations pour les activités futures, afin de renforcer la cybersécurité et la protection des infrastructures essentielles de l'information en Afrique de l'Est et en Afrique australe.

---

31 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/rasemboarimanana-ioc-lusaka-aug-08.pdf.

32 http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/obiso-ITU-GCA-lusaka-aug-08.pdf.

62. A la fin du Forum régional sur la cybersécurité, les participants ont approuvé un ensemble de résultats et de recommandations (voir les Annexes du présent rapport). Il a été convenu que chaque pays de la région devrait:

1) concevoir une stratégie nationale en matière de cybersécurité (voir l'Annexe 1);

2) examiner et, le cas échéant, revoir la cyberlégislation actuelle et rédiger une nouvelle législation, afin d'ériger en infraction pénale l'utilisation délictueuse des TIC, compte tenu de l'évolution rapide des menaces liées à la cybersécurité (voir l'Annexe 2);

3) développer des capacités de gestion des incidents sur le plan national, sur la base des exemples actuels des CERT/CSIRT (voir l'Annexe 3).

(voir les Annexes 1, 2, et 3 pour plus de renseignements)

63. Les participants à la réunion ont également prié l'UIT-D, en partenariat avec le COMESA et d'autres organisations régionales ou internationales ainsi que des entités nationales, de prendre les initiatives nécessaires pour assurer le suivi de la mise en oeuvre des recommandations formulées par le Forum régional et de fournir des mises à jour sur les progrès accomplis et sur la coopération régionale ou internationale. Les participants se sont également félicités de la coopération et de la collaboration entre l'UIT et le COMESA, qui ont organisé conjointement ce forum régional et ont encouragé un renforcement de la coopération, afin d'associer d'autres organisations régionales ou internationales.

Clôture de la réunion

64. Dans ses remarques de clôture au nom de l'UIT, Marcelino Tayob, Chef du bureau de zone de l'UIT pour l'Afrique australe à Harare (Zimbabwe), a exprimé l'espoir que le Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe tenu pendant quatre jours, notamment les sessions de travail consacrées au développement des capacités nationales et régionales en matière de cybersécurité/CIIP, avait été utile aux participants. M. Tayob a remercié les intervenants, qui, malgré un calendrier chargé, se sont libérés pour échanger leurs expériences et leurs compétences avec les participants. Il a également remercié chacun des participants qui, directement ou indirectement, ont contribué à la réussite de ce Forum et a transmis des remerciements tout particuliers au pays hôte ainsi qu'au COMESA, pour leur travail remarquable grâce auquel ce Forum régional sur la cybersécurité a pu être un franc succès. L'UIT, qui est active depuis longtemps dans le domaine de la normalisation et du développement des télécommunications, continuera d'être une instance où les divers points de vue des Etats, du secteur privé et d'autres parties prenantes concernant la cybersécurité et la protection des infrastructures essentielles de l'information peuvent être examinés dans le cadre de ses différentes activités et initiatives.

Le présent projet de compte rendu[33] de la réunion est ouvert pour d'éventuelles observations pendant une période de 30 jours après sa réception et sa publication sur le site web du forum. L'adresse électronique pour faire parvenir vos observations sur ce projet de compte rendu, ou sur le programme de travail de l'UIT sur la cybersécurité en faveur des pays en développement (2007-2009)[34], est cybmail(at)itu.int[35].

A des fins de partage des informations, les noms de tous les participants seront ajoutés aux listes de diffusion électronique cybersecurity-africa(at)itu.int[36] pour toutes les questions concernant les activités de l'UIT-D dans le domaine de la cybersécurité. Si vous n'avez pas participé directement à l'atelier, ou si votre nom ne figure pas déjà sur la liste de diffusion électronique, mais si vous souhaitez participer à ces discussions, veuillez nous envoyer un courrier électronique à l'adresse: cybmail(at)itu.int.

_____

[33] Le présent compte rendu du Forum est accessible en ligne à l'adresse: http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08-f.pdf.

[34] http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme.

[35] Veuillez nous faire parvenir vos éventuelles observations sur le compte rendu du Forum à l'adresse:cybmail@itu.int.

[36] Liste de diffusion électronique sur la cybersécurité régionale de l'UIT: cybersecurity-africa@itu.int. Veuillez envoyer un courrier électronique à l'adresse: cybmail@itu.int, qui sera ajouté à la liste de diffusion.

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[37]

Doc. RFL/2008/REC01-F
29 août 2008
Original: anglais

Recommandations du Forum

Le Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe a eu lieu à Lusaka (Zambie) du 25 au 28 août 2008. Tenu sous les auspices de la Communications Authority of Zambia et du Gouvernement de la Zambie, et organisé conjointement par l'UIT et le COMESA, il visait à 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 qu'à analyser les bonnes pratiques, à échanger des informations sur les activités de développement entreprises par l'UIT et par d'autres entités et à examiner le rôle des différents partenaires pour promouvoir une culture de la cybersécurité.

Une soixantaine de personnes de 21 pays et 4 organisations régionales ont pris part à cette manifestation. On comptait parmi les participants des professionnels des pouvoirs publics, des autorités de réglementation, du secteur privé et de la société civile. Tous les documents relatifs au Forum, y compris l'ordre du jour et tous les exposés présentés, sont disponibles sur le site web du Forum à l'adresse www.itu.int/itu-d/cyb/events/2008/lusaka/.

---

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

Recommandations du Forum

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

Au terme du Forum régional sur la cybersécurité, les participants sont convenus des résultats et recommandations ci-après:

- Ils ont reconnu que le renforcement de la cybersécurité est un problème mondial et que chaque pays de la région doit redoubler d'efforts au niveau national et mettre en oeuvre des mesures afin de prendre part aux activités régionales et internationales visant à améliorer la cybersécurité et de les appuyer.
- Ils ont demandé aux pays d'adhérer à une approche régionale harmonisée dans le domaine de la cybersécurité.
- Ils ont convenu que, pour élaborer une cyberstratégie nationale de cybersécurité, il est essentiel de s'associer aux activités régionales et internationales visant à promouvoir une culture de la cybersécurité.
- Ils ont reconnu d'une part les initiatives, mesures et approches existantes qui se sont avérées efficaces dans un certain nombre de pays et dans d'autres régions et, d'autre part, les efforts déployés par l'UIT et d'autres organisations afin d'élaborer des projets et de développer des outils susceptibles d'appuyer les initiatives nationales pour l'Afrique de l'Est et l'Afrique australe.
- Ils ont reconnu que l'approche intégrée adoptée par l'UIT pour les activités de cybersécurité ainsi que la volonté de l'Union de renforcer la coopération internationale, par exemple grâce à son Programme mondial cybersécurité, constituent une base utile pour mener une campagne de sensibilisation, lancer ou étudier des mesures nationales de cybersécurité et veiller à la cohérence et la compatibilité au niveau international.
- Ils ont demandé aux pays de la région d'utiliser le Guide pratique UIT pour l'autoévaluation nationale en matière de cybersécurité/CIIP lorsqu'ils mettent en place leurs institutions et élaborent leurs politiques et stratégies dans le domaine de la cybersécurité et de la protection des infrastructures essentielles.
- Ils ont demandé à chaque pays de la région d'identifier une institution principale qui assurera la coordination des activités relatives à la cybersécurité.
- Ils ont souligné l'importance que revêt la mise en place d'une coopération régionale et internationale qui pourra permettre d'élaborer des lignes directrices relatives à la mise en oeuvre d'initiatives visant à renforcer la cybersécurité dans les pays à l'intérieur comme à l'extérieur de la région.
- Ils ont encouragé l'élaboration de modèles de renforcement des capacités pouvant être adaptés aux besoins de chaque pays de la région.
- Ils ont reconnu que les pays de la région auront peut-être besoin d'un appui et d'une assistance en ce qui concerne l'élaboration et la mise en oeuvre d'une stratégie nationale de cybersécurité ainsi que l'utilisation du Guide pratique UIT pour l'autoévaluation nationale en matière de cybersécurité/CIIP afin d'évaluer les moyens disponibles en matière de cybersécurité, et ont demandé que l'UIT et les organisations d'intégration régionale apportent leur soutien dans ce domaine.
- Ils sont convenus que chaque pays de la région devrait:
    - élaborer une stratégie nationale de cybersécurité (Voir l'Annexe 1);
    - examiner et, au besoin, revoir la législation actuelle applicable au cyberespace et rédiger une nouvelle législation afin que l'utilisation abusive des TIC devienne un délit, compte tenu de l'évolution rapide des menaces liées à la cybersécurité (Voir l'Annexe 2); et
    - développer des capacités de gestion des incidents responsables au niveau national et utiliser les exemples actuels des équipes d'intervention en cas d'incident ou d'urgence informatique (CSIRT/CERT) lors de la mise en place de ces capacités (Voir l'Annexe 3).

  (Voir les Annexes 1, 2 et 3 pour plus de détails)
- Ils sont convenus de la création d'un groupe de travail chargé de poursuivre les activités de cybersécurité dans la région, et plus précisément d'étayer et de développer les projets de

document relatifs aux stratégies nationales, aux cadres juridiques et à la surveillance, l'alerte et la gestion des incidents établis par le Forum. Ce groupe sera composé de représentants des Etats Membres ainsi que du COMESA, de la Commission économique des Nations Unies pour l'Afrique (CEA), de l'UIT, de l'Union africaine, de l'IOC, de la Communauté d'Afrique de l'Est et d'organisations d'intégration régionale.

- Ils ont demandé à l'UIT D, en partenariat avec le COMESA et d'autres organisations régionales et internationales, ainsi qu'avec d'autres entités nationales, de mener les initiatives nécessaires au suivi de la mise en oeuvre des recommandations du Forum régional et de fournir des informations mises à jour sur les progrès réalisés et la coopération régionale et internationale.
- Ils ont rendu hommage à l'UIT et au COMESA pour leur coopération et collaboration dans l'organisation conjointe de la présente manifestation régionale et ont encouragé l'élargissement de cette coopération à d'autres organisations régionales et internationales.

_____

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.

_____

ANNEX 2: GROUPE DE TRAVAIL 2

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[39]

Doc. RFL/2008/WG02-F

29 août 2008

Original: anglais

Groupe de travail 2: Fondements juridiques et mesures exécutoires

Recommandations du Groupe de travail ad hoc du Forum sur les fondements juridiques et les mesures exécutoires

1.0 Fondements juridiques et mesures exécutoires: Introduction

La société moderne est de plus en plus dépendante des technologies de l'information et de la communication (TIC), il en va de même pour la cybercriminalité, d'où la nécessité d'élaborer et de faire appliquer une législation sur la cybercriminalité.

Le Groupe de travail ad hoc du Forum formule des propositions générales à inclure dans la législation modèle sur la cybersécurité du COMESA. Ces propositions concernent les quatre domaines suivants:

- Droit positif faisant de certains comportements des infractions pénales.
- Droit procédural.
- Coopération internationale.
- Traitement de la preuve.

2.0 Droit positif

Le Groupe de travail ad hoc du Forum propose que les actes énumérés ci-après soient considérés comme des infractions pénales. Il est proposé que le Groupe de travail donne une description claire de ces délits:

1) Accès illicite à un ordinateur.

2) Interception illicite d'une communication électronique.

3) Intrusion dans des données informatiques.

4) Intrusion dans un système informatique [il est proposé que le Groupe de travail réfléchisse à l'imposition de peines plus graves pour sanctionner toute intrusion dans des systèmes publics].

5) Emploi abusif de certains dispositifs [à noter qu'il faut avoir une définition claire de ce que l'on entend par emploi abusif afin que l'utilisation licite ne soit pas pénalisée].

6) Contrefaçon informatique.

7) Fraude informatique.

8) Création, possession ou distribution d'images ou de documents de pornographie infantile [il est proposé que le Groupe de travail réfléchisse à l'imposition de sanctions pour la pornographie en général, en particulier pour les Etats Membres qui sanctionnent déjà la création physique, la possession et la distribution de documents pornographiques].

9) Usurpation d'identité.

---

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

10) Phishing (hameçonnage) [la description de ce délit devrait être suffisamment large pour englober un délit analogue commis en utilisant une autre technologie, par exemple le smishing].

11) Espionnage de données.

12) Spam.

13) Harcèlement.

14) Incitation à la haine et autres délits religieux [les Etats Membres devraient être autorisés à exercer leur pouvoir de discrétion pour l'adoption de telles sanctions].

15) Tentative de perpétrer de tels délits ou complicité pour les délits susmentionnés [les sanctions devraient être plus légères que celles appliquées pour les délits proprement dits].

16) Responsabilité pour les délits susmentionnés [le Groupe de travail devrait indiquer s'il s'agit d'une responsabilité civile ou d'une responsabilité pénale].

17) Protection des données [pour les pays qui n'ont pas de législation en vigueur sur la protection des données].

3.0 Dispositions relatives à la procédure

Il devrait y avoir des dispositions habilitantes sur les sujets suivants:

1) Sauvegarde accélérée des données informatiques stockées.

2) Sauvegarde accélérée et divulgation partielle des données de trafic.

3) Autorité de poursuite visant à contraindre les fournisseurs de réseaux informatiques à divulguer des informations relatives au contenu ou d'autres informations stockées sur le réseau.

4) Recherche et saisie de données informatiques stockées par les autorités chargées de faire respecter la loi.

5) Collecte en temps réel de données de trafic se rapportant aux communications électroniques.

6) Interception du contenu de communications électroniques.

7) Rétention de données.

4.0 Coopération internationale

Insérer des dispositions relatives à la coopération internationale conformément aux instruments internationaux pertinents sur la coopération internationale en matière criminelle.

Il conviendrait d'adopter de nouvelles normes pour l'assistance mutuelle parallèlement aux dispositions prises concernant les points de contact du réseau disponibles 24/7.

5.0 Preuves

La loi type comporte des dispositions relatives à la recevabilité de preuves électroniques devant un tribunal.

_____

ANNEX 3: GROUPE DE TRAVAIL 3

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[40]

Doc. RFL/2008/WG02-F

29 août 2008

Original: anglais

Groupe de travail 3: Veille, alerte et intervention en cas d'incident

Recommandations du Groupe de travail ad hoc du Forum sur la veille, l'alerte et l'intervention en cas d'incident

L'objet du présent document est de fournir des lignes directrices et des recommandations relatives à la mise en place des structures organisationnelles nationales et régionales requises pour commencer les activités de veille, d'alerte et de gestion des incidents.

1. Création d'un centre national de cybersécurité qui serait le point de contact national pour la cybersécurité. Ce centre constituerait l'élément de base et évoluerait vers des moyens de gestion des incidents plus complets et plus structurés (par exemple, CERT, CSIRT).

• Activité connexe:

a. Elaboration d'un plan d'action conforme aux lignes directrices figurant à l'Annexe.

• Calendrier: d'ici à un an (troisième trimestre 2009)

• Budget: 100 000 USD par centre de cybersécurité (une ventilation plus détaillée des coûts sera fournie ultérieurement)

2. Elaboration et mise en oeuvre d'une campagne de sensibilisation, afin d'échanger les expériences nationales aux niveaux régional et international, à laquelle participeront les organisations concernées (Union africaine, UIT, COMESA, IOC, CEA, Communauté d'Afrique de l'Est, organisations d'intégration régionale, etc.). Ce processus permettrait d'obtenir l'indispensable adhésion des principaux décideurs et de mobiliser les ressources financières et humaines nécessaires.

• Activités connexes:

a. Identification de réunions régionales dans le cadre desquelles la cybersécurité peut être examinée.

b. Organisation d'au moins une manifestation internationale par an (au niveau régional ou continental) afin de passer en revue les activités nationales en cours et de définir les mesures qu'il est nécessaire de mettre en oeuvre aux niveaux régional et international.

• Calendrier: Courant 2009 (éventuellement début 2010).

• NOTE: Le calendrier dépendrait des ressources financières disponibles pour lancer les activités nationales. Les activités de sensibilisation serviraient à lever des fonds afin de créer le centre national de cybersécurité.

• Budget: A établir.

3. Création d'un CERT régional auquel participerait le COMESA et tout autre pays africain intéressé. L'Union africaine, l'UIT, le COMESA, l'IOC, la CEA, la Communauté d'Afrique de l'Est, des organisations d'intégration régionale et d'autres organisations internationales assureraient la coordination et apporteraient tout l'appui nécessaire à la mise en oeuvre des activités opérationnelles connexes. Le CERT servirait de lien avec les centres nationaux de cybersécurité et faciliteraient leur transformation en CERT

---

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

ou CSIRT nationaux/gouvernementaux. La mise en oeuvre de la présente recommandation découlerait de la création de centres nationaux de cybersécurité.

• Activités connexes:

a. Evaluation des besoins opérationnels coordonnée et réalisée par l'UIT, le COMESA, la CEA et d'autres parties prenantes intéressées.

b. Elaboration du plan de mise en oeuvre.

c. Mise en oeuvre.

• Durée: Un an (quatrième trimestre 2010, premier trimestre 2011).

• Budget: A établir.

Annexe 1 :

Lignes directrices opérationnelles relatives à la création d'un centre national de cybersécurité

Facteurs clés de réussite

L'objet des présentes lignes directrices est de donner des orientations de départ, y compris d'indiquer les domaines dans lesquels des mesures concrètes peuvent être prises, concernant la création d'un centre national de cybersécurité.

Pour obtenir les résultats escomptés, il faut tenir compte de certains facteurs clés de réussite, dont le respect permettrait de mettre en oeuvre efficacement l'activité en question.

Ces facteurs indispensables à la création et à la mise en oeuvre d'un centre national de cybersécurité seront peut-être les suivants:

• Volonté politique: au plus haut niveau possible.

• Connaissance: compréhension approfondie des besoins et des objectifs à atteindre.

• Structure: définition claire des concepts comme la responsabilité individuelle et administrative.

• Gestion: fonctionnement, viabilité et durabilité.

• Budget: capacité financière requise.

• Développement progressif: possibilité d'utiliser les ressources existantes afin de minimiser l'investissement de départ.

Phase 1 – Cadre initial - Création d'un centre de sécurité

Objectif: Création d'une cellule opérationnelle complète capable de fournir un ensemble de services bien définis.

Besoins:

Ressources humaines (3-4 personnes):

• Ingénieur en technologies de l'information - Administration de réseaux/systèmes.

• Responsable de la sécurité - Mise en oeuvre des mesures de sécurité.

• Spécialiste d'applications - Déploiement de solutions logicielles.

• NOTE : Pour la structure de départ, il conviendrait d'envisager d'avoir recours au personnel adéquat dont disposent déjà les pouvoirs et/ou les organismes publics.

Equipements et installation:

• Configuration client/serveur (serveur standard, bureau, etc.).

• Réseau local.

• Imprimantes.

• Connexion Internet large bande solide et efficace - 1 Mb recommandé: faire du lobbying auprès de fournisseurs de services Internet locaux pour obtenir une connexion Internet gratuite.

• Installations: emplacement physique, etc. Envisager la possibilité que des entités publiques autonomes, comme les régulateurs, hébergent le CERT.

Phase 2 – Compétences, bénéficiaires, rôles et responsabilités

Identifier un coordonnateur chargé de la cybersécurité.

• Interlocuteur spécifique.

• Eventualités devant être prises en compte par le coordonnateur:

  - Accusés de réception automatiques par courrier électronique, par exemple, pour rassurer l'utilisateur.

• Services à fournir:

  – Gestion d'incidents simples:

- Signaler les incidents aux parties prenantes.
- Recueillir et stocker des données.

– Appui aux services et assistance:

- Premier niveau d'appui.

– Renforcement des capacités et sensibilisation:

- Assurer la coordination avec les parties prenantes concernées (responsables en matière de technologies de l'information, décideurs, régulateurs, fournisseurs de services Internet, etc.).
- Créer un site web permettant d'échanger des informations.
- Organiser des formations et des ateliers.
- Mener des campagnes de sensibilisation à l'échelle de la région.
- Mener des campagnes de sensibilisation à l'échelle du continent.

• Bénéficiaires:

– Ministères et organismes publics.

– Clients institutionnels (ONG, société civile, etc.).

– A long terme, tous les citoyens.

Phase 3 – Réseau de collaboration

• Coordination nationale:

– Fournisseurs de services Internet, centres de données.

– Sollicitation des fournisseurs de services locaux afin d'obtenir un sponsoring.

– Listes de diffusion et coordonnées des clients institutionnels.

• Coordination internationale:

– Coordination avec d'autres centres de sécurité dans le domaine des technologies de l'information - CERT.

– Organisations régionales (COMESA, UIT, CEA, Union africaine, AFRISPA, Communauté d'Afrique de l'Est, organisations d'intégration régionale, etc.).

_____