GOVERNO DE CABO VERDE

Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP)

Document RWPR/2007/01-F
1er décembre 2007
Original: anglais

Projet de compte rendu de réunion: Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la CIIP, Praia, Cap-Vert, 27-29 novembre 2007

Veuillez adresser toutes vos observations éventuelles sur ce projet de compte rendu à: cybmail@itu.int

Objet du présent Rapport

1. L'atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP) s'est tenu à Praia (Cap-Vert), du 27 au 29 novembre 2007[1]. Il a rassemblé des représentants des pouvoirs publics, des professionnels du secteur et d'autres parties prenantes de la région de l'Afrique de l'Ouest qui ont débattu, échangé des informations et collaboré à l'élaboration et à la mise en oeuvre de cadres nationaux politiques et réglementaires pour faire appliquer des mesures liées à la cybersécurité et à la CIIP. Cet atelier devait intéresser les parties prenantes suivantes: décideurs en matière de technologies de l'information et de la communication dans les ministères et administrations de la région; institutions et départements responsables des politiques et législations dans le domaine de la cybersécurité et de leur mise en application; représentants des opérateurs, équipementiers, prestataires de services, associations de professionnels et de consommateurs qui cherchent à encourager une culture de la cybersécurité. Les participants à l'atelier ont également examiné des initiatives prises aux niveaux régional et international pour renforcer la coopération et la coordination entre ces différentes parties prenantes.

2. Cet atelier a été suivi par quelque 120 personnes, venant de la région de l'Afrique de l'Ouest, y compris du pays hôte, le Cap-Vert, du continent africain dans son ensemble, ainsi que d'autres régions du monde. Une documentation complète sur l'atelier, 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/2007/praia/). Le présent document résume la teneur des trois jours de débats, donne un aperçu des sessions et des présentations des orateurs ainsi que de certaines prises de position communes.

Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la CIIP, organisé à Praia (Cap-Vert), 27-29 novembre 2007

3. Les sociétés modernes sont de plus en plus tributaires des technologies de l'information et de la communication (TIC), globalement interconnectées. 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, multidisciplinaire et multi-parties prenantes. Les participants à l'atelier ont débattu de certains éléments clés de l'élaboration de ces cadres politiques et réglementaires.

---

1 http://www.itu.int/ITU-D/cyb/events/2007/praia/.

Ouverture de la réunion et allocution de bienvenue

4. L'Atelier régional sur les cadres pour la cybersécurité et la protection des infrastructures essentielles de l'information a été ouvert par Margarida Evora-Sagna, représentante du bureau de zone de l'UIT pour l'Afrique de l'Ouest au Sénégal, qui a prononcé une allocution de bienvenue[2]. Au nom de l'UIT, Mme Evora-Sagna a souhaité la bienvenue aux participants à l'atelier, dont elle a souligné l'importance pour le renforcement des capacités de la région en matière de cybersécurité. Elle a rappelé que la plupart des pays africains souffraient de lacunes au niveau des cadres réglementaires en matière de cybersécurité et que les questions de cybersécurité n'étaient pas traitées avec toute l'attention requise. Alors que seule une minorité d'Africains ont accès aux TIC, on insiste sur la nécessité de faciliter cet accès, sans toutefois donner aux particuliers les moyens de se protéger et de faire face aux menaces. Cependant, a poursuivi Mme Evora-Sagna, la présence à cet atelier de représentants d'un si grand nombre de pays africains tend à prouver que les pays de la région sont désormais déterminés à prendre des mesures pour améliorer la cybersécurité et renforcer la protection des infrastructures essentielles de l'information. Pour conclure, Mme Evora-Sagna a remercié les organisateurs locaux d'avoir permis la tenue de cette rencontre et a exprimé l'espoir que les recommandations et conclusions qui s'en dégageraient pourraient aider les pays à créer, sur le plan des TIC, un environnement propice qui tienne pleinement compte des grandes questions liées à la cybersécurité - et, ainsi, faciliteraient l'instauration d'une économie du savoir, dans l'intérêt du développement et de la prospérité des pays d'Afrique de l'Ouest.

5. Patricia de Mowbray, coordonnateur résident des agences des Nations Unies au Cap-Vert, a ensuite prononcé quelques remarques liminaires. Au nom de l'Organisation des Nations Unies, elle a évoqué la révolution de l'Internet dans les secteurs de la santé et de l'enseignement - moyen essentiel pour permettre à la société actuelle d'encourager le développement socio-économique. Elle a insisté sur le rôle des technologies de l'information et de la communication dans la lutte contre la pauvreté et sur celui de l'Internet, dont elle a relevé les nombreux avantages potentiels pour la société, puis a décrit les liens entre l'Internet et la sécurité et la demande, toujours plus forte, de mesures visant au renforcement de la cybersécurité. Mme de Mowbray a également mentionné certaines des résolutions des Nations Unies ayant trait à la cybersécurité, en particulier la Résolution 57/239[3] de l'Assemblée générale, relative à la création d'une culture mondiale de la cybersécurité et qui donne aux pays des lignes directrices pour la mise en oeuvre d'activités à l'échelle nationale. Mme de Mowbray a conclu en souhaitant plein succès aux organisateurs et en exprimant l'espoir que cet atelier permettrait de continuer à forger les moyens nécessaires à la lutte contre la cybercriminalité.

6. Son Excellence M. Manuel Sousa, Ministre des infrastructures, des transports et de la mer du Cap-Vert, a ensuite prononcé une allocution de bienvenue au nom de son ministère, en expliquant que la cybersécurité et la protection des infrastructures essentielles de l'information étaient, pour la société de l'information, des enjeux fondamentaux qui appelaient des mesures concrètes. Il a fait remarquer que c'était un grand honneur pour le Cap-Vert d'accueillir cet atelier et de collaborer avec les experts et participants au renforcement des liens avec tous les pays africains dans ce domaine. M. Sousa a également relevé la qualité des experts et des orateurs invités et a convié tous les participants à tirer profit de leur présence ainsi que de celle de leurs homologues d'autres pays de la région et d'autres parties du monde, pour prendre une part active à toutes les sessions de l'atelier en échangeant des idées et des données d'expérience et en posant des questions sur les thèmes. Chacun, qu'il soit expert de la sécurité ou utilisateur, a besoin de mieux comprendre quels sont les enjeux et les perspectives dans les différents pays. Pour conclure, M. Sousa a souhaité la bienvenue à toutes les personnes présentes à cette très importante réunion et a invité les participants à entamer un débat, qu'il a espéré fructueux et ciblé.

Session 1: Elaborer une stratégie et créer un cadre national pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP)

7. 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, dans un souci de cohérence, certains pays ont mis en place des cadres institutionnels tandis que d'autres recourent à une approche plus légère et moins formelle. De nombreux pays n'ont pas encore de stratégie nationale pour la cybersécurité et la CIIP. Cette session était consacrée au concept de cadre national pour la cybersécurité et la CIIP et aux efforts déployés par l'UIT pour élaborer un cadre de bonnes pratiques, afin que les participants puissent se faire une idée générale des perspectives et des enjeux en question.

8. M. Robert Shaw, de la Division applications TIC et cybersécurité du Secteur du développement des télécommunications de l'UIT (UIT-D), a été le modérateur de cette session dans le cadre de laquelle on a cherché à analyser, au sens large, différentes conceptions de la cybersécurité et des cadres CIIP et de leurs composantes, souvent analogues, afin de donner aux participants une idée de la situation. M. Shaw a présenté un aperçu des "Activités de l'UIT-D dans le domaine de la cybersécurité et de la CIIP"[4] et a décrit en détail le

---

2 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/evora-sagna-opening-remarks-praia-27-nov-07.pdf.

3 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

4 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/evora-sagna-opening-remarks-praia-27-nov-07.pdf.

programme de travail de l'UIT-D sur la cybersécurité à l'intention des pays en développement (2007-2009)[5]. Il a mentionné dans son exposé certaines initiatives, en cours et en projet, de l'UIT: *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 cybersécurité et la CIIP*.

9. M. Shaw a fait remarquer que la plupart des pays n'avaient pas encore élaboré ou mis en oeuvre de stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information et que les pays en développement, qui disposent de ressources humaines, institutionnelles et financières limitées, éprouvaient des difficultés particulières à cet égard. Il a fait observer que la Commission d'études 1 du Secteur du développement des télécommunications de l'UIT élaborait actuellement, dans le cadre de la Question 22, des bonnes pratiques contenant un projet de cadre pour les initiatives nationales en matière de cybersécurité, en étroite relation avec le programme de travail sur la cybersécurité à l'intention des pays en développement mis au point par l'UIT-D. Ce programme de travail définit la façon dont l'UIT compte aider les pays en développement à renforcer leurs capacités dans le domaine de la cybersécurité/CIIP, entre autres, 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-D envisage de les diffuser largement aux 191 Etats Membres de l'UIT. M. Shaw a indiqué que l'un des problèmes sur lequel achoppaient les discussions relatives à la cybersécurité était la recherche de mécanismes permettant aux différents acteurs de mieux communiquer les uns avec les autres, sachant que chaque catégorie a souvent des besoins différents et spécifiques concernant le degré de confiance nécessaire au partage d'informations précises. Il a également signalé que l'UIT prévoyait d'organiser au cours de l'année sur le continent africain au moins deux autres réunions sur la cybersécurité et espérait lancer en 2008 un programme de bourses liées à la cybersécurité[6].

10. Jorge Lopes, Nucleo Operacional da Sociedade de Informacao (NOSI) (Cap-Vert), a, dans sa présentation "Cybergouvernance et cybersécurité"[7], évoqué la mise en oeuvre de services d'administration publique en ligne au Cap-Vert et la façon dont le pays s'efforce d'améliorer par ce moyen la gouvernance et la fourniture de services. Pour commencer, il a décrit le contexte dans lequel s'inscrivent ces services dans son pays, en mettant l'accent sur la façon dont le Cap-Vert traite des questions relatives à la sécurité et sur les aspects précis de la sécurité actuellement à l'étude. Il a désigné les trois grands piliers de la stratégie de son pays en matière d'administration publique en ligne, à savoir les relations entre les administrés et les pouvoirs publics, entre les pouvoirs publics et le secteur privé, et entre les pouvoirs publics et les fournisseurs de services publics. Il a souligné que la sécurité sur Internet était un élément essentiel de la sécurité des utilisateurs des TIC et que la réalisation du plein potentiel de l'Internet dans les relations économiques et commerciales passait par la mise en place d'un environnement stable et fiable. Alors que le nombre de points d'accès public aux services hertziens déployés dans le pays est en constante augmentation et qu'un grand nombre de services publics à valeur ajoutée sont mis en oeuvre, les pouvoirs publics sont instamment appelés à renforcer la sécurité pour empêcher que des personnes non autorisées aient accès à ces services et en fassent une utilisation délictueuse. M. Lopes a assuré que des mesures ont été prises pour qu'il soit possible de relever ces nouveaux défis. Le Cap-Vert s'est ainsi aperçu qu'il était très important de créer une culture qui favorise le renforcement de la collaboration et l'efficacité de la coopération horizontale entre les différents services publics.

11. Pour conclure, M. Lopes a signalé qu'au Cap-Vert le lien entre la cybergouvernance et la sécurité était fondé sur les lignes directrices établies par l'UIT et sur la Convention du Conseil de l'Europe sur la cybercriminalité. Il a toutefois fait valoir que la gestion du réseau public n'avait jusqu'à maintenant pas clairement pris en compte la sécurité, ce qui devait changer. Les habitants doivent être informés de qui est qui sur le réseau, de qui est chargé de telle ou telle tâche, etc. L'orateur a également mis en avant les observations formulées précédemment par le Ministre sur la nécessité d'accorder à la cybersécurité et à la protection des infrastructures essentielles de l'information un rang de priorité plus élevé que ce n'est le cas actuellement au Cap-Vert.

12. James Ennis, du Département d'Etat des Etats-Unis d'Amérique, s'est exprimé en tant que Rapporteur pour la Question 22 de la Commission d'études 1 de l'UIT-D (Sécurisation des réseaux d'information et de communication: Meilleures pratiques pour créer une culture de la cybersécurité). Il a présenté un aperçu des travaux sur l'élaboration d'un cadre pour les initiatives nationales en matière de sécurité, en cours de mise au point par la Commission d'études 1 de l'UIT-D dans le cadre de sa Question 22, dans une présentation intitulée "Bonnes pratiques pour organiser les initiatives nationales en matière de cybersécurité"[8]. Ce cadre est l'un des

---

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

6 http://www.itu.int/ITU-D/cyb/cybersecurity/.

7 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/lopes-e-government-cybersecurity-praia-nov-07.pdf.

8 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/ennis-best-practices-cybersecurity-praia-nov-07.pdf.

éléments des travaux menés par la Commission d'études, comme proposé dans un rapport sur ces bonnes pratiques[9], dont les pouvoirs publics peuvent se servir pour élaborer et mettre en oeuvre des stratégies nationales relatives à la cybersécurité et à la CIIP. M. Ennis a invité les participants à l'atelier et les pays à prendre part aux activités relatives à la Question 22/1, lancées dans le cadre de la Conférence mondiale de développement des télécommunications (Doha, 2006). A ce jour, trois réunions ont eu lieu et la prochaine doit se tenir en avril 2008.

13. Le rapport en cours d'élaboration par la Commission d'études traite des grands problèmes auxquels les décideurs font face en matière de cybersécurité. Ce projet de rapport débute par une définition fonctionnelle de la cybersécurité ("On appelle cybersécurité la prévention des dégâts causés aux systèmes électroniques d'information et de communication et à l'information qu'ils contiennent, l'utilisation et l'exploitation non autorisées de ces systèmes, et - s'il y a lieu - leur remise en état, afin d'en renforcer la confidentialité, l'intégrité et la disponibilité"). Il est également indiqué dans ce projet de rapport que différents systèmes appellent différents niveaux de sécurité, d'où la nécessité d'une gestion des risques adaptée. Le cadre établi pour les initiatives nationales en matière de cybersécurité décrit cinq grandes composantes des meilleures pratiques dans ce domaine: 1) élaboration d'une stratégie nationale de la cybersécurité; 2) collaboration entre secteur public et secteur privé; 3) prévention de la cybercriminalité; 4) capacités de gestion des incidents sur le plan national; 5) culture nationale de la cybersécurité. Le projet de rapport comprend en outre une déclaration d'intention pour chaque composante du cadre, définit des objectifs et des mesures concrètes en vue de les atteindre et présente des références et des documents liés à chacune de ces mesures. M. Ennis a ajouté que ce rapport, cadre compris, était un document conçu pour être évolutif.

14. M. Ennis a également souligné que la cybersécurité était l'un des sujets brûlants dans le monde des télécommunications. Il a ajouté qu'aujourd'hui tous les principaux secteurs de la société étaient tributaires des réseaux de l'information et de la communication pour pouvoir fonctionner harmonieusement et que, pour atteindre un niveau de sécurité maximal, les systèmes devaient être fiables et sûrs. Et, a-t-il ajouté, ce problème concerne tous les pays, qu'ils soient développés ou en développement.

Session 2: Elaboration d'une stratégie nationale pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP)

15. 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 a besoin de mettre en place un *plan d'action global* englobant des questions techniques, juridiques et politiques, associé à une coopération régionale et internationale. Il faut donc se demander sur quels éléments doit porter l'élaboration de stratégies nationales pour la cybersécurité et la CIIP, quels partenaires doivent s'impliquer, et s'il existe des exemples de cadres dont des pays pourraient s'inspirer. Cette session, dont le modérateur était Basil Udotai, Direction de la cybersécurité, Office du Conseiller national pour la sécurité (Nigéria), 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 de l'Afrique de l'Ouest à élaborer des stratégies nationales pour la cybersécurité et la CIIP.

16. Dans son exposé sur l'élaboration d'une stratégie nationale, "Cadre de la cybersécurité au Nigéria"[10], M. Udotai a présenté ses vues sur les enjeux de l'élaboration d'une telle stratégie, en prenant des exemples concrets au Nigéria et dans d'autres pays d'Afrique de l'Ouest. Il a souligné que les problèmes de cybersécurité auxquels les pays font face aujourd'hui sont pratiquement les mêmes dans les pays développés et dans les pays en développement, dans la mesure où les sociétés sont de plus en plus tributaires des réseaux informatiques pour la fourniture de toutes sortes de services. En Afrique subsaharienne, a-t-il dit, les pouvoirs publics ne sont guère incités à modifier les législations ni à prendre les mesures nécessaires pour lutter efficacement contre la cybercriminalité et pour instaurer la cybersécurité. Dans ces pays, le secteur privé ne déploie pas assez d'efforts pour traiter du problème de la cybersécurité puisque le marché est florissant et que les professionnels ne voient pas dans l'immédiat la nécessité de consentir des dépenses supplémentaires. Le développement des TIC dans la région évolue sur un plan horizontal, avec l'adjonction de nouveaux services à valeur ajoutée.

17. M. Udotai a attiré l'attention des participants sur ce qu'il a appelé "le paradoxe de la cybersécurité dans les pays en développement". En effet, ces pays sont encouragés à utiliser davantage les TIC et l'Internet, à promouvoir l'adaptation des TIC et une meilleure pénétration de l'Internet, tout en étant avertis des dangers et des risques que courent les pouvoirs publics, le secteur privé et les particuliers dans le cyberespace. M. Udotai a fait remarquer que même si l'Internet, plus que tout autre moyen, permet de redéfinir la coopération mondiale, toutes les parties intéressées devraient néanmoins être conscientes de la réalité du "forum shopping", c'est-à-dire de la tendance qu'ont les pirates informatiques et les spammeurs à utiliser les juridictions les moins réglementées et les plus libérales pour lancer des attaques dans le cyberespace. Et, a-t-il ajouté, comme dans les pays en développement on n'encourage guère, voire pas du tout, la sécurité, et comme c'est la connectivité

---

9 http://www.itu.int/md/D06-SG01-C-0130/en *(nom d'utilisateur et mot de passe TIES nécessaires).*

10 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/udotai-nigeria-cybersecurity-framework-praia-nov-07.pdf.

Internet et non la proximité qui détermine qui on côtoie sur l'Internet, ces pays représentent le maillon faible de la chaîne de la société de l'information. M. Udotai a poursuivi en présentant un aperçu de la façon dont le Nigéria conçoit la cybersécurité, des commissions et sous-commissions mises en place dans ce pays et des perspectives et des enjeux futur. Il a décrit les mesures prises par le Nigéria pour faire face aux problèmes de cybersécurité et a relevé l'existence de nombreuses initiatives, qu'il s'agisse de réforme de la législation ou d'activités de sensibilisation. M. Udotai a signalé qu'un projet de législation avait été mis en place avec l'assistance de nombreux partenaires, dans le pays comme à l'étranger.

18. Pour terminer, M. Udotai a expliqué que, même si la situation et les domaines de compétence variaient d'un pays à l'autre, les questions de cybersécurité étaient souvent communes à de nombreux pays et à de nombreuses juridictions. Il conviendrait par conséquent d'élaborer sur le plan national des cadres de base axés sur les changements à apporter dans plusieurs domaines (politiques, législation, renforcement des capacités, partenariats avec le secteur privé, coopération internationale et sensibilisation du public), en s'inspirant de modèles déjà adoptés avec succès dans d'autres pays. Pour l'orateur, si, après cet atelier, un pays ici représenté était encouragé à revoir son cadre juridique ou les activités opérationnelles de ses organismes chargés de l'exécution des lois, dans l'optique de la réforme visant à relever les nouveaux défis des TIC, alors cette conférence pourra être considérée comme une grande réussite.

19. Christine Sund, Division des applications TIC et de la cybersécurité, Secteur du développement des télécommunications de l'UIT (UIT-D) a, dans sa présentation sur le thème "Promouvoir une culture de la cybersécurité"[11], brièvement décrit ce que l'on entend par culture de la cybersécurité, ainsi que les rôles que les différentes parties prenantes à 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 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.

20. 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 le plan 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 indispensables à l'élaboration et à la mise en oeuvre de stratégies nationales de cybersécurité. En outre, les secteurs public et privé doivent 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 la cybersécurité est, fondamentalement, une responsabilité partagée.

21. A partir des exposés présentés au cours des Sessions 1 et 2, décrivant des cadres pour la cybersécurité et la CIIP et différentes stratégies et approches nationales, Joseph Richardson, Etats-Unis d'Amérique, dans sa présentation sur le thème "Cadre de gestion pour les initiatives nationales en matière de cybersécurité: kit d'autoévaluation"[13], a décrit les éléments des travaux entrepris par l'UIT en vue de l'élaboration d'un kit pour l'autoévaluation de la cybersécurité/CIIP sur le plan national[14]. Fruit de l'une des principales synergies entre les travaux de la Commission d'études 1 de l'UIT-D sur la Question 22 ("Sécurisation des réseaux d'information et de communication: Meilleures pratiques pour créer une culture de la cybersécurité")[15] et les activités au titre du Programme de travail de l'UIT-D sur la cybersécurité à l'intention des pays en développement (2007-2009)[16], ce kit applique le cadre en cours d'élaboration par la Commission d'études auquel est associé un moyen pratique,

---

11 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/sund-promoting-a-culture-of-cybersecurity-praia-nov-07.pdf.

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

13 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/richardson-cybersecurity-framework-and-readiness-assessment-praia-nov-07.pdf.

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

15 http://www.itu.int/ITU-D/cyb/cybersecurity/index.html.

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

pour analyse à l'échelle nationale. Ce kit peut aider les pouvoirs publics à évaluer les politiques, procédures, normes et institutions nationales existantes, ainsi que d'autres éléments nécessaires à la formulation de stratégies de sécurité dans un environnement 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. Ce kit examine sous l'angle de la gestion et de la politique chacun des cinq éléments du cadre de bonnes pratiques présenté par M. Ennis au cours de la Session 1, à savoir: a) stratégie nationale; b) collaboration entre secteur public et secteur privé; c) prévention de la cybercriminalité; d) capacités de gestion des incidents sur le plan national; e) culture nationale de la cybersécurité, institutions participantes et relations entre pouvoirs publics, industrie et entités du secteur privé.

22. M. Richardson a fait observer, à propos des initiatives liées à la cybersécurité et à la protection des infrastructures essentielles de l'information, 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. 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 pour la cybersécurité et la CIIP. M. Richardson a signalé que le kit et les ressources connexes étaient constamment mis à jour sur le site web de l'UIT-D sur 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 d'ateliers régionaux de renforcement des capacités en 2007, 2008 et 2009.

23. Au cours de la dernière session de la première journée, les participants se sont répartis en petits groupes pour discuter des sujets au programme du jour, dans le cadre d'une table ronde placée sous la direction d'un modérateur. Ce dernier a veillé à ce que tous les participants aient la possibilité d'échanger des expériences propres à tel ou tel pays et de poser des questions aux experts présents à chaque table. Les thèmes abordés pendant la première journée concernaient la création d'une stratégie et d'un cadre national pour la cybersécurité et la protection des infrastructures essentielles de l'information.

24. Au cours de la soirée du premier jour, les participants ont été invités par les organisateurs à une réception à l'Hôtel Praia Mar.

Session 3: Fondements juridiques, démarche réglementaire et application des lois

25. Pour prévenir, détecter et réprimer la délinquance informatique, 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, procédures et grands principes du droit pénal. De nombreux pays ont donc modifié leur code pénal ou ont entrepris de le faire, conformément aux conventions et recommandations internationales. Les participants aux Sessions 3, 4 et 5 ont analysé les solutions choisies par différents pays et se sont demandé quels domaines pouvaient se prêter à la coordination juridique et à l'adoption de mesures exécutoires sur le plan international. Le modérateur de la Session 3, Matoso Carvalho, de l'Institut angolais des communications (INACOM) (Angola), a présenté les orateurs, puis a mis en lumière les problèmes posés par les différents régimes juridiques dans les différents pays et la nécessité de renforcer d'urgence la collaboration dans ce domaine.

26. Marco Gercke, Allemagne, a ouvert la session en présentant un aperçu de la position actuelle de la communauté internationale quant à la révision des législations existantes et à l'élaboration de législations nouvelles, dans un exposé intitulé "Les enjeux de la lutte contre la cybercriminalité dans les pays en développement et le rôle des législations nationales, régionales et internationales dans ce domaine"[17]. Il a mis l'accent sur certains problèmes auxquels les pays en développement font face dans leur lutte contre la cybercriminalité et a renvoyé, pour plus de détails, à la publication que l'UIT s'apprête à faire paraître sur le sujet[18]. Il a également donné des précisions sur les législations nationales, régionales et internationales visant à promouvoir une culture mondiale de la cybersécurité. Dans ce contexte, il a insisté sur l'importance de l'harmonisation et a fait référence à la Convention de Budapest sur la cybercriminalité[19] (2001) - seul cadre international existant. M. Gercke a fait valoir que pour les pays en développement, la recherche de solutions adéquates au problème de la cybercriminalité était un défi 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. M. Gercke a en outre souligné que les risques entraînés par une protection insuffisante pouvaient avoir de lourdes conséquences pour la vie socio-économique. Les pays en développement risquent donc de servir de refuge aux délinquants informatiques, ce qui aurait des conséquences désastreuses pour le marché national. Toutefois, le fait que ces pays partent de zéro pourrait leur donner une occasion exceptionnelle de mettre dès le départ leurs stratégies de lutte contre la cybercriminalité en conformité avec les normes en vigueur.

---

17 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gercke-challenge-of-fighting-cybercrime-praia-nov-07.pdf.

18 http://www.itu.int/ITU-D/cyb/cybersecurity/index.html.

19 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

27. M. Gercke a également relevé que l'Internet était idéal pour dissimuler des informations secrètes. Le réseau offre, certes, d'immenses potentialités, mais l'inconvénient est qu'un grand nombre de délinquants sont passés maîtres dans l'utilisation de ces techniques. Les participants à l'atelier ont beaucoup apprécié les démonstrations en direct présentées par M. Gercke, qui leur ont permis de mieux comprendre les techniques permettant, par exemple, d'introduire des conversations et des messages masqués dans des images et des courriels.

28. Gabriela Sarmiento, consultante, Venezuela, a ensuite présenté un exposé sur "Les délits informatiques, les lois qui les punissent et la pratique judiciaire"[20], dans lequel elle a examiné certaines des méthodes juridiques adoptées par des pays pour lutter contre la délinquance informatique. Elle a énoncé certaines normes nationales applicables à la cybercriminalité, ainsi que les conventions internationales, des cas concrets et des informations détaillées sur les actes délictueux commis et leur répression. Elle a également présenté les résultats d'une étude faisant apparaître que 22 pays d'Amérique latine et des Caraïbes travaillaient sur des projets de loi sur la cybercriminalité ou modifiaient leur code pénal afin d'établir une législation qui réprime ce type de délit. Mme Sarmiento a décrit les différentes législations adoptées dans le monde pour décourager la cybercriminalité, en soulignant l'augmentation du nombre de pays qui ont déjà pris des mesures. Elle a également cité en exemple un pays, non nommément désigné, qui est en train d'élaborer une législation sur la cybercriminalité et qui a expressément déclaré ne pas vouloir inclure le secteur privé dans cette législation par crainte des critiques. Elle a rappelé que tout projet de législation en la matière devait être capable de résister aux critiques pour remplir sa fonction et contribuer à la réussite de la mise en oeuvre de ladite législation.

29. Mme Sarmiento a conseillé aux pays de commencer par cerner les problèmes au niveau national et de faire le point de la situation législative avant de se lancer. Elle a ensuite encouragé les participants à utiliser les ressources, modèles et bonnes pratiques existants. Elle a cité à titre d'exemple les ressources de l'UIT dans le domaine de la cybersécurité, le kit antispam de l'OCDE, le Manuel d'Interpol pour les enquêtes en matière de cybercriminalité, les ressources d'Europol pour la formation de formateurs, etc. Pour permettre aux pays d'aller de l'avant, elle a signalé qu'il fallait: a) normaliser le concept de cybercriminalité; b) harmoniser les législations en la matière; c) faciliter les actions en justice en vue de réunir des preuves; d) améliorer la coopération internationale entre les forces de police, les juges compétents et les Etats nations. Elle a rappelé que l'un des facteurs importants de l'amélioration de la cybersécurité était le renforcement de la coopération régionale et de l'assistance mutuelle dans le domaine de la législation contre la cybercriminalité.

Session 4: Fondements juridiques, démarche réglementaire et application des lois (suite)

30. Les participants à la Session 4 ont poursuivi les débats de la Session 3. Le modérateur, Marco Gercke (Allemagne), a ouvert la session en donnant un aperçu de certaines "Solutions nationales, régionales et internationales existantes dans la lutte contre la cybercriminalité"[21], en mettant l'accent sur la Convention de Budapest sur la cybercriminalité[22] (2001). Il a fait remarquer 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, mieux connue sous le nom de Convention du Conseil de l'Europe sur la cybercriminalité, il a expliqué qu'il s'agissait du seul accord international en vigueur qui couvrait tous les domaines en rapport avec la cybercriminalité (y compris le droit pénal matériel, le droit procédural et la coopération internationale) et qui pouvait s'appliquer aux pays de "common law" comme aux pays de droit romain.

31. Il a présenté aux participants le concept d'"ADN" appliqué à la législation. Lorsqu'on utilise ce concept comme marqueur d'initiatives et de lois visant à ériger en infraction pénale l'utilisation délictueuse des TIC, on peut alors établir des comparaisons légales tendant à prouver que de nombreux pays érigent en infraction pénale les mêmes délits en lien avec le cyberespace. L'orateur a poursuivi en expliquant que la Convention du Conseil de l'Europe sur la cybercriminalité n'était pas destinée aux seuls pays européens et que d'autres pays avaient participé à son élaboration. Le principal objectif de cette Convention est d'établir un cadre utilisable par les pays lorsqu'ils cherchent à rédiger, actualiser ou réviser leur législation. M. Gercke a expliqué comment, en pratique, la Convention pouvait aider les pays à adopter un programme national de cybersécurité. Il a ajouté que les pays qui souhaitaient en savoir plus à ce sujet pouvaient se mettre en rapport avec les personnes de contact au Conseil de l'Europe pour obtenir de plus amples renseignements.

32. Il a ensuite poursuivi en évoquant la nature de l'Internet, qui transcende les frontières, et la persistance de certaines frontières dans le cyberespace. Par "frontières", M. Gercke faisait référence à la possibilité de bloquer des adresses IP ou d'utiliser les moyens actuels de géolocalisation. Son idée était d'analyser les arguments de ceux qui s'opposent à la recherche de solutions régionales et nationales. En effet, beaucoup prétendent que puisque l'Internet n'a pas de frontières, les seules solutions qui s'imposent sont de nature internationale. M. Gercke a fait remarquer que, dans ce cas, il fallait harmoniser si l'on voulait lutter efficacement contre la cybercriminalité, mais que cela n'excluait pas le recours à des solutions régionales et nationales. L'objet de la Convention sur la cybercriminalité est d'harmoniser les législations nationales et de faciliter la coopération

---

20 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/sarmiento-cybercrime-laws-practice-praia-nov-07.pdf.

21 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gercke-convention-on-cybercrime-praia-nov-07.pdf.

22 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

internationale. Si les pays érigent les mêmes délits en infractions pénales, ils peuvent alors coopérer efficacement lorsqu'il s'agit d'enquêter, de réunir des preuves, d'envisager des poursuites, etc. M. Gercke a, pour conclure, indiqué que le Secrétariat de la Convention sur la cybercriminalité (2001) incitait davantage de pays à manifester leur intérêt pour la Convention.

33. Baye Issakha Gueye, Membre du Conseil de régulation de l'Agence de régulation des télécommunications (ART) (Sénégal) a ensuite présenté un exposé sur le thème "Fondements juridiques et démarche réglementaire pour la cybersécurité - survol des enjeux et perspectives au Sénégal"[23]. Il a fait remarquer que les délinquants informatiques n'avaient pas besoin de visa pour pénétrer dans un pays et que la protection des citoyens relevait de la responsabilité de chaque Etat. M. Gueye a rappelé que plusieurs solutions avaient déjà été proposées pour renforcer la cybersécurité, dont l'élaboration de stratégies nationales et de campagnes de sensibilisation, l'harmonisation des normes et la création de lois et législations solides. Il a ensuite rappelé les mesures prises par le Sénégal pour mettre en place, dans le pays, des cadres juridiques et réglementaires adaptés à la lutte contre la cybercriminalité. A titre d'exemple, il a précisé qu'il était envisagé d'inclure dans les dispositions juridiques en vigueur des mesures visant à faciliter la détection rapide, l'investigation, les poursuites, la réunion de preuves électroniques, l'extradition et l'assistance juridique mutuelle.

34. En conclusion, M. Gueye a évoqué ce qu'il a appelé sa vision d'avenir de la "cyberjustice", lorsque les tribunaux nationaux auront intégré les règles applicables à la cybercriminalité et auront formé des professionnels capables de traiter ces affaires. L'adoption de nouvelles infractions spécifiques aux TIC nécessite diverses sanctions adéquates et l'aménagement de la procédure pénale classique par rapport aux TIC. M. Gueye a appelé au renforcement de la sensibilisation à la cybersécurité sur le plan national et à la prise de mesures en conséquence.

35. L'orateur suivant, Mody Ndiaye, du Bureau des Nations Unies sur les drogues et la criminalité (UNODC), dans son exposé sur le thème "Application de la loi contre le cybercrime - quelle stratégie en Afrique de l'Ouest?"[24], a évoqué les infractions et délits les plus courants en Afrique, cybercriminalité comprise. Il a reconnu que la criminalité transnationale organisée, qui inclut le trafic de drogue, le trafic d'êtres humains et d'armes à feu et la contrebande de migrants, le terrorisme, la corruption, la criminalité économique et financière, dont le blanchiment d'argent, et la cybercriminalité, freinait considérablement le développement socio-économique durable, affaiblissait la productivité, l'efficacité et la rentabilité et portait atteinte à l'intégrité de la vie sociale, économique, culturelle et politique. M. Ndiaye a mentionné certaines des récentes résolutions de l'Assemblée générale des Nations Unies et de l'UNODC traitant de la cybercriminalité. Il a dit qu'en Afrique de l'Ouest, les mesures prises pour lutter contre la cybercriminalité, en pleine expansion, étaient insuffisantes. Comme les principaux intéressés, à savoir la force publique et les écoles de police, ne savent pas ce qu'est la cybercriminalité et en quoi elle consiste, les responsables n'ont pas accès aux outils et méthodes dont ils auraient besoin. L'orateur a également fait remarquer que l'utilisation croissante des technologies à des fins délictueuses nécessitait un renforcement de la coopération et de la coordination entre les Etats et avec le secteur privé.

36. M. Ndiaye a ensuite réfléchi à la méthode qui serait la plus efficace dans la lutte contre la cybercriminalité. Il a évoqué la nécessité de faire en sorte que tous les pays connaissent la Convention de Budapest sur la cybercriminalité[25] (2001), en veillant à encourager plus avant l'harmonisation et la coordination sur le plan régional. Pour conclure, il a déclaré: "Même si un crime passe la frontière, ce crime doit être puni".

Session 5: Fondements juridiques, démarche réglementaire et application des lois (suite)

37. Les débats se sont poursuivis sous la direction de M. David Gomes, Agencia Nacional das Comunicações (ANAC) (Cap-Vert), modérateur de la session.

38. Le premier exposé de cette session a été présenté par M. Joel Schwarz, Computer Crime & Intellectual Property Section (CCIPS), Criminal Division, Département de la justice des Etats-Unis d'Amérique. Dans son exposé "Fondements et processus juridiques: les risques de la cybercriminalité et ses incidences sur l'Afrique"[26], il a présenté aux participants différents cas montrant que presque chaque affaire traitée aujourd'hui (criminalité organisée, jeu, kidnapping, etc.) a à voir avec l'informatique. La cybercriminalité va désormais au-delà des attaques informatiques puisque des personnes qui ne sont pas spécialistes de ce domaine utilisent aujourd'hui l'ordinateur, en nombre croissant. Les gens continueront à se servir d'ordinateurs et d'autres moyens en ligne, même si ce n'est pas le cas des magistrats instructeurs et des policiers. L'orateur a fait observer que si des pays sont considérés comme peu sûrs du point de vue de l'univers en ligne, ils n'ont guère de chances d'attirer les industriels et les investisseurs. Il a ajouté que l'Internet offrait d'immenses possibilités de croissance économique, mais que celles-ci dépendaient de la fiabilité et de la sûreté des réseaux d'information et qu'elles seraient remises en question si un pays ne pouvait fournir à ses citoyens et entrepreneurs des réseaux

---

23 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/gueye-senegal-perspective-praia-nov-07.pdf.

24 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/ndiaye-cybercrime-strategy-for-west-africa-praia-nov-07.pdf.

25 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

26 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/schwarz-legal-development-praia-nov-07.pdf.

d'information sûrs. Chaque pays doit donc impérativement se forger les capacités et les compétences nécessaires pour enquêter sur les cas d'utilisation abusive ou délictueuse de ces réseaux et veiller à ce que les infractions commises par les délinquants qui les attaquent ou les exploitent soient réprimées.

39. M. Schwarz a ensuite évoqué la façon dont les pays devraient réagir à la menace de la cybercriminalité du point de vue de l'application des lois. Afin de pouvoir enquêter efficacement, poursuivre et faire condamner ceux qui utilisent l'informatique et l'Internet à des fins délictueuses, il a recommandé, dans un premier temps, de privilégier la mise en oeuvre de plusieurs mesures: création et mise en application d'une législation adéquate en matière de cybercriminalité, établissements d'équipes spécialisées pour l'application des lois et de relations avec d'autres pays. A cet égard, il a donné quelques conseils simples sur la façon dont un pays peut s'assurer que sa législation est à jour. Par exemple, si ce pays ne veut pas procéder à une nouvelle rédaction de ses lois, il peut au moins amender la législation existante et vérifier qu'elle n'utilise pas de termes qui ne pourraient s'appliquer qu'à l'univers non virtuel. Il a conseillé aux pays de se fonder sur la Convention du Conseil de l'Europe sur la cybercriminalité pour revoir leur législation existante. Cette Convention commence par énoncer quelques définitions qui, a-t-il fait remarquer, étaient le principal point sur lequel achoppait la rédaction de ce texte. Même aujourd'hui, lorsqu'on passe en revue différentes législations, on peut constater des différences dans les définitions.

40. Pour conclure, M. Schwarz a mentionné plusieurs projets auxquels le Département de la justice des Etats-Unis participe étroitement sur le continent africain. Il a ainsi cité deux ateliers organisés au Botswana en 2006 et auxquels une vingtaine de pays avaient participé. Suite à ces rencontres et à d'autres activités de sensibilisation, une liste de diffusion a été créée et deux nouveaux pays d'Afrique se sont récemment associés au High Tech Crime Network of Contacts, opérationnel 24 heures sur 24 et 7 jours sur 7.

41. Alex da Costa, Public Utilities Regulatory Authority (PURA), Gambie, a ensuite pris la parole. Dans sa présentation sur les "Perspectives juridiques et réglementaires"[27], il a examiné le rôle du régulateur dans la lutte contre la cybercriminalité et pour la promotion de la cybersécurité, du point de vue de son pays et de l'organisme de réglementation multisectoriel qu'il représente. Il a fait valoir que les enjeux de l'édification des fondements juridiques étaient importants et que les pays ne pouvaient pas faire grand chose contre la cybercriminalité s'ils ne disposaient pas d'une législation appropriée. L'orateur a insisté sur la nécessité, pour tous les pays, de modifier les lois existantes et d'en créer de nouvelles pour faire face aux menaces croissantes liées à l'utilisation délictueuse des TIC. Il a en outre mis l'accent sur la nécessité de créer une culture de la cybersécurité en axant ses propos sur l'importance de cette dernière dans la démarche réglementaire et en faisant valoir que la réglementation implique un contrôle réglementaire direct de secteurs précis de l'économie nationale; il a en outre assimilé l'absence d'implication directe des pouvoirs publics dans la réglementation de certains secteurs de l'économie à un "retour à la loi de la jungle". M. da Costa a également énuméré les facteurs essentiels au succès de la démarche réglementaire et certaines des fonctions caractéristiques du régulateur: indépendance, autonomie, autorité, transparence financière et consultations avec les parties prenantes

42. M. da Costa a expliqué que la Gambie n'avait pas actuellement de législation sur la cybersécurité, la protection des données et des flux d'informations, domaines dont un organisme doit assurer la responsabilité dans chaque pays. Il a demandé si cette responsabilité relevait, dans chaque pays, du régulateur, du ministère de la justice ou d'une autre partie prenante. Cette question peut, certes, sembler simple, mais il n'est pas toujours facile d'y répondre. Les ressources publiques étant toujours très sollicitées, il n'y a en règle générale pas d'accord sur ce que l'on entend par besoins essentiels. Pour conclure, il a dit qu'il fallait passer des paroles aux actes. Il a souligné que l'absence de législation était un problème majeur. L'Afrique de l'Ouest doit impérativement se rendre compte qu'elle a besoin d'infrastructures et de cadres juridiques appropriés. En conclusion, il a déclaré que, pour être efficace, la cybersécurité nécessitait la pleine coopération et participation de toutes les parties prenantes, des consommateurs, des services publics et surtout de toutes les branches de l'Etat.

43. Juste avant la clôture de l'atelier, les participants ont pris part à une séance de questions et réponses consacrée aux fondements juridiques, à la démarche réglementaire et à l'application des lois. Il a été établi un bref résumé des thèmes débattus par les experts pendant la journée ainsi que des principaux enjeux mis à jour. Les conclusions qui se sont dégagées de ces discussions ont ensuite été récapitulées dans le cadre de la Session 9.

Session 6: Capacités de veille, d'alerte et de réponse aux incidents informatiques

44. 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, les organisations régionales et internationales est indispensable pour sensibiliser l'opinion aux attaques potentielles et aux mesures à prendre pour y remédier. Cette première session

[27] http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/da-costa-gambia-praia-nov-07.pdf.

du deuxième jour de l'atelier, animée par M. Seymour Goodman, Georgia Institute of Technology (Etats-Unis d'Amérique), a permis d'avoir un échange de vues sur les bonnes pratiques et les normes connexes concernant la création de capacités nationales ou régionales de veille, d'alerte et de réponse aux incidents sur les plans technique, financier et de gestion.

45. M. Seymour Goodman, Georgia Institute of Technology (Etats-Unis d'Amérique), a ouvert la session avec un exposé intitulé "Capacités de veille, d'alerte et de réponse aux incidents (et autres)"[28]. Il a d'abord parlé des différents aspects de la cybersécurité et pas uniquement de la cyberdéliquance qui n'est qu'un aspect du problème. Selon lui, d'autres aspects doivent occuper davantage de place dans les débats: en effet, l'identification et la localisation des délinquants n'est qu'un aspect très limité de la cybersécurité, laquelle, plus largement, englobe les vulnérabilités, les menaces et les mesures à prendre pour se protéger contre elles. Les exploiteurs sont qualifiés de "menace", mais il y en a aussi d'autres, en particulier celles qui pèsent sur les infrastructures essentielles de l'information, et certaines ne sont pas d'origine humaine. Soulignant que la confiance fait partie intégrante de la cybersécurité, M. Goodman a ajouté que la sécurité doit être au coeur de la conception des systèmes que nous utilisons tous les jours. Il est en effet difficile de garantir la sécurité des systèmes informatiques car, à l'origine, cet élément n'était pas intégré dans leur conception.

46. Présentant les capacités de veille, d'alerte et de réponse aux incidents ainsi que d'autres activités opérationnelles durables, M. Goodman a posé la question de savoir qui assurait la veille, qui était chargé de l'alerte et quel était le destinataire des informations ainsi recueillies? Il s'agit d'un élément très important si l'on veut que le cyberespace soit plus sûr et mieux sécurisé. Les aspects de la sécurité qui relèvent du droit pénal ont été examinés en détail au cours des trois jours de l'atelier. M. Goodman a tenu à souligner une fois de plus que ce n'était là qu'un aspect de la cybersécurité. Aujourd'hui, a-t-il poursuivi, il y a des lois sur le port de la ceinture de sécurité dans les voitures afin d'assurer la sécurité des conducteurs et de leurs passagers. De même, les personnes qui se connectent devraient prendre des mesures pour assurer leur sécurité dans le cyberespace. M. Goodman a noté qu'il y avait encore beaucoup à faire pour sécuriser le cyberespace. Les pays, dans l'hypothèse où ils ont déjà élaboré une législation et mis en place une politique relative à la cybersécurité, doivent aussi disposer de capacités fonctionnelles opérationnelles, notamment dans les domaines suivants: prévention et dissuasion; veille et alerte; gestion des incidents (ce qui inclut l'investigation numérique); mesures à prendre en cas d'attaque; définition d'une stratégie pour savoir comment réagir à une attaque; gestion des conséquences de l'attaque, ce qui inclut la remise en état (que faire une fois que l'attaque est terminée) et le châtiment (retrouver le ou les auteurs de l'attaque). M. Goodman a souligné qu'il est très important d'évaluer les dommages subis et de savoir comment redevenir opérationnel lorsqu'il y a des problèmes concrets dans le cyberespace.

47. Toutefois, l'accent doit également être mis sur la prévention, les normes, la certification et la conformité. Il faut notamment adopter de bonnes pratiques et encourager le respect des normes, en soi mais aussi pour assurer la sécurité d'autrui, en particulier dans le monde interconnecté qui est le nôtre. De l'avis de M. Goodman, les utilisateurs doivent développer une culture de la sécurité afin qu'ils sachent mieux comment utiliser certains produits de sécurité et comment agir en ligne dans de meilleures conditions de sécurité. Actuellement, les attaques dans le cyberespace sont de plus en plus sophistiquées et malgré tous les efforts qui sont actuellement faits dans le domaine de la cybersécurité, l'heure n'est pas à l'optimisme et les délinquants sont toujours plus nombreux et plus habiles. M. Goodman a souligné le fait qu'il est beaucoup plus facile de perpétrer une attaque dans le cyberespace que de s'en protéger et que les mesures de rétorsion ne sont pas élaborées suffisamment rapidement pour pouvoir contrer les menaces. En d'autres termes, nous sommes, à bien des égards, en train de perdre la bataille contre la cybercriminalité.

48. M. Goodman a ensuite parlé de la création de centres nationaux de cybersécurité sur le continent africain, des nouvelles technologies et de l'innovation. Il a également rappelé aux participants qu'une enquête avait été faite pour évaluer la sécurité de l'information en Afrique. Il a fait observer que le continent africain comptait 54 pays et que tous étaient des pays en développement, et a ajouté que pour les pays de cette catégorie, la meilleure solution pour disposer de capacités fonctionnelles est de développer des capacités opérationnelles. Il a demandé aux participants où devraient se trouver ces capacités fonctionnelles et proposé plusieurs options: des équipes d'intervention en cas d'urgence informatique (CERT) ou des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT). Il a toutefois souligné que ces deux termes pouvaient prêter quelque peu à confusion étant donné que ce dont ont besoin la plupart des pays africains c'est surtout d'un Centre national de cybersécurité (NCSC). Plutôt que des "brigades du feu" de type CERT/CSIRT, il faut une vision plus large et la première question à se poser est de savoir quelle est la finalité de ces entités.

49. M. Goodman a ensuite décrit comment on pouvait imaginer un centre NCSC. Il s'agit d'organisations nationales qui fournissent aux pays les capacités opérationnelles dont ils ont besoin pour protéger leurs systèmes et leurs réseaux ainsi que les utilisateurs qui en sont tributaires. M. Goodman a été d'avis que les centres NCSC devraient être des centres publics utilisant au mieux les ressources humaines limitées. Les pays africains n'ont pas généralement toutes les compétences techniques suffisantes pour lutter contre la cybercriminalité. Réunir des experts techniques au sein d'un centre NCSC pourrait donc être une solution plus efficace en encourageant

[28] http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/goodman-watch-warning-praia-nov-07.pdf.

un dialogue et une coopération entre ces experts. Par ailleurs, on ne sait pas vraiment comment trouver, former et fidéliser des personnes dans ce domaine. La création d'un centre NCSC pourrait donc être une solution à ce problème, en particulier pour soutenir les activités des organismes chargés de faire respecter la loi et des instituts de criminalistique. M. Goodman a fait remarquer que, dans de nombreux pays africains, le secteur privé est souvent trop faible et qu'il y a peu, voire aucune mesure sur le plan commercial susceptible d'inciter des personnes à accepter ce rôle et ces responsabilités. En outre, dans ces pays, les ressources TIC de l'Etat constituent une partie importante de ce qui doit être protégé dans le pays (administration publique en ligne, contrôle sur les noms de domaine de premier niveau, étant donné qu'il s'agit de la signature du pays sur Internet et que c'est donc une ressource que le pays souhaite protéger). En conclusion, M. Goodman a donné quelques options possibles concernant le lieu d'implantation des centres NCSC notamment: 1) une organisation indépendante relevant d'un ministère; 2) un département d'un centre déjà existant (par exemple d'un centre informatique national); 3) une unité relevant de l'autorité nationale de régulation des télécommunications (une autre législation qui n'est pas le droit pénal); 4) une unité externalisée au secteur privé (secteur privé national ou étranger) tout en soulignant que de nombreux pays seraient quelque peu réticents à le faire étant donné qu'en cas d'externalisation il faudrait un audit très strict. M. Goodman a mis l'accent sur le fait que les fonctions du centre NCSC et les contraintes devraient être définies par la loi.

50. Dans l'intervention suivante, M. Belhassen Zouari, Agence nationale de la sécurité informatique (ANSI), Cert-Tcc, Tunisie a fait un exposé intitulé "Mise en oeuvre d'une stratégie nationale: le cas du CERT tunisien[29]. M. Zouari, P.-D. G. du CERT-Tcc, seul CERT reconnu par la FIRST[30] sur le continent africain, a rappelé brièvement aux participants comment l'agence avait été créée. Fin 1999, une unité (un micro-CERT), spécialisée dans la sécurité informatique, a été créée. Au départ, l'unité avait pour objectif de sensibiliser les décideurs et le personnel technique aux questions de sécurité et de créer le premier groupe d'experts tunisiens en sécurité informatique, chargé de veiller à la sécurité des infrastructures et des applications nationales hautement stratégiques. En 2002, l'unité a commencé à mettre en place une stratégie et un plan national dans le domaine de la sécurité informatique. 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 mettre en oeuvre la stratégie et le plan national en la matière. En septembre 2005, l'équipe d'intervention en cas d'urgence informatique - le Centre de coordination tunisien (Cert-Tcc) a été mis en place. Il s'occupe notamment de veille, d'alerte, de diffusion de l'information, de sensibilisation (différents types de campagnes de sensibilisation, développement d'une culture de la cybersécurité, information pour les juges, etc.), de partage, d'analyse et de collecte des informations, de traitement des incidents, de coordination, etc. Les partenaires avec lesquels travaille le Cert-Tcc sont différents, selon l'activité concernée. Le Cert-Tcc fournit aussi des avis techniques spécialisés sur la sécurité informatique. M. Zouari a souligné que les fournisseurs de services Internet sont un partenaire important dans cette activité étant donné qu'ils gèrent les points de connexion d'entrée et de sortie du pays. Il a également souligné que le Cert-Tcc partage volontiers son expérience avec d'autres pays de la région qui envisagent de lancer ou qui lancent déjà des programmes et des initiatives similaires.

51. Il a également été pris note du fait que l'UIT a un projet en cours visant à développer un kit sur la réduction des effets des réseaux zombies (botnet)[31] afin de trouver une solution aux problèmes croissants que posent ces réseaux, problèmes qui ont été évoqués au cours de la Session 6 sur les capacités de veille, d'alerte et de réponse aux incidents informatiques. Ce kit est un projet multi-parties prenantes et pluridisciplinaire visant à faire la chasse à ces réseaux zombies et atténuer leurs effets en mettant tout particulièrement l'accent sur les problèmes propres aux économies Internet émergentes. Ce kit, qui utilise les ressources existantes, recense les principaux partenaires aux niveaux local et international et tient compte des contraintes particulières des pays en développement. Il a pour objet de sensibiliser les Etats Membres aux menaces toujours plus grandes que font peser les réseaux zombies et à leurs liens avec les activités délictueuses. Il intègre les dimensions politique, technique et sociale de la réduction des effets de ces réseaux. L'avant-projet a été diffusé en décembre 2007 et des essais pilotes sont prévus dans un certain nombre d'Etats Membres de l'UIT en 2008.

Session 7: Collaboration entre les pouvoirs publics et le secteur privé

52. Avec la privatisation, les réseaux TIC dans chaque pays sont, en très grande majorité, détenus et exploités par le secteur privé. La mise en place d'un cadre national pour la cybersécurité et la protection des infrastructures essentielles de l'information suppose le regroupement de représentants du secteur privé et des pouvoirs publics dans des forums de confiance où pourront être examinés les problèmes de sécurité qui se posent à chaque pays. La réussite des partenariats privé-public, c'est la confiance qui est nécessaire pour établir, développer et entretenir des relations de partage entre secteur privé et pouvoirs publics. Plusieurs sujets ont été examinés au cours de cette session: partenariats entre le secteur privé et les pouvoirs publics, fraudes dans le domaine des télécommunications et collaboration mise en place pour atténuer les effets de cette fraude. L'animateur de la session, El Hadji Mansor Sy Tandine, représentant de la Présidence de la République du Sénégal, a proposé que les pays africains oeuvrent ensemble à l'élaboration de solutions dans le

29 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/zouari-cert-tunisia-praia-nov-07.pdf.

30 http://www.first.org.

31 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

domaine de la cybersécurité, en étroite collaboration avec le secteur privé et les gouvernements. Il a insisté sur le fait que le monde a besoin d'un cyberespace sûr et sécurisé et a relevé que le Forum sur la gouvernance de l'Internet qui s'est tenu récemment au Brésil avait lui aussi mis l'accent sur ce point.

53. Luis Sousa Cardoso, Qualité de service et sécurité des réseaux, PT Comunicações, Portugal, a ouvert la session avec un exposé sur "La cybercriminalité et ses incidences sur les infrastructures essentielles de l'information"[32] au cours duquel il a présenté le FIINA (Forum for International Irregular Network Access). Le FIINA compte actuellement 250 membres et seuls les opérateurs, les fournisseurs de services ou les opérateurs télécom peuvent être membres de ce forum. L'objectif de ce forum est de partager les informations entre opérateurs uniquement, à l'exclusion de toute autre partie. Six compagnies et organisations sont membres fondateurs du FIINA et la Commission d'études 2 du Secteur de la normalisation des télécommunications (UIT-T) de l'UIT participe aussi à leurs activités.

54. Se fondant sur l'expérience qu'il a acquise en travaillant dans la région, M. Cardoso a parlé de la situation actuelle de l'Afrique en ce qui concerne la cybercriminalité. Il a fait observer que même si, d'après les travaux de recherche actuellement en cours, l'Afrique n'est ni à l'origine ni la cible de cyberattaques de grande envergure, elle reste très vulnérable à la plupart d'entre elles. Compte tenu de l'évolution de la cybercriminalité, il ne faut plus compter sur la protection que la connectivité limitée a pu fournir dans le passé. Les conséquences de l'élargissement de la connectivité et de la capacité sont lourdes pour l'Afrique qui manque de technologies, de connaissances spécialisées et de politiques dans le domaine de la sécurité. Si aucune mesure n'est prise, le continent va devenir un point d'entrée pour les délinquants et les terroristes du cyberespace et servira de plaque tournante pour coordonner et lancer des attaques. M. Cardoso a parlé de quelques-uns des gros problèmes signalés en 2007, notamment la fraude sur la vente en gros, la fraude avec les cartes d'appel, la fraude aux sms, les réseaux zombies (les fournisseurs de services déconnectent aujourd'hui les utilisateurs qui font partie de ces réseaux car ils ne se protègent pas eux-mêmes contre ces réseaux), les menaces qui pèsent sur le commerce électronique (y compris la fraude aux cartes de crédit), la fraude à la téléphonie VoIP ainsi que le pharming. Il a fait observer qu'aujourd'hui les personnes sont de plus en plus nombreuses à utiliser une infrastructure des communications autrefois restreinte mais aujourd'hui plus ouverte, et qu'il faut donc s'attendre à davantage d'innovation avec l'arrivée sur le marché de nouvelles compagnies riches de nouvelles idées, à un travail plus lourd dans le domaine de la sécurité étant donné que les choses ne sont plus cachées et à un besoin accru en matière d'assurance qualité et de services de sécurité. Un autre problème qu'il faut garder à l'esprit est celui de la sécurité des téléphones mobiles, étant donné que les opérateurs de téléphonie mobile ont signalé en 2006 et 2007 cinq fois plus d'incidents de sécurité que les années précédentes.

55. M. Cardoso a également fait part de ses réflexions sur les jeux d'argent et les jeux en ligne, un secteur qui prend de l'ampleur. Les jeux en ligne nécessitent l'utilisation d'un réseau local d'entreprise, de l'Internet ou d'un autre service de télécommunication. Normalement, pour pouvoir jouer en ligne, il suffit d'avoir un logiciel de navigation sur le web et/ou un logiciel client approprié. Avec l'essor des technologies de l'information, les jeux d'argent et les jeux en ligne sont devenus une industrie très fructueuse et très lucrative. M. Cardoso a indiqué que, selon DataMonitor.com, le marché mondial des jeux en ligne représentait 3,2 milliards USD et comptait 113 millions d'utilisateurs en 2005. Le succès des jeux en ligne fait évoluer les modèles d'activité économique des fabricants de logiciels et a fait prospérer d'autres activités: déploiement des réseaux large bande, systèmes de paiement en ligne, utilisation des cafés Internet, publicité, etc. M. Cardoso a parlé des incidences économiques de la cybercriminalité et de l'érosion de la confiance des consommateurs qui s'en est suivie, ainsi que de la baisse de la productivité et des secrets commerciaux.

56. Almiro Rocha, Cabo Verde Telecom, Cap-Vert, a poursuivi avec son exposé sur "CVTelecom et la sécurité des systèmes informatiques"[33]. M. Rocha a présenté aux participants de l'atelier une étude de cas concrète montrant comment une compagnie des télécommunications a dû s'adapter et se repenser dans un environnement où les menaces ne cessent d'évoluer. Il a expliqué comment Cabo Verde Telecom, fournisseur de services de communication, en situation de monopole sur le marché jusqu'en 2005, réagit aux différents problèmes. Il a fait observer que 2006 avait été une année de profonds changements dans le domaine de la réglementation sur le marché des télécommunications du Cap-Vert et que, depuis le début de 2007, ce marché avait été libéralisé. De ce fait, la compagnie a dû être subdivisée en trois branches différentes, conformément au droit de la concurrence (CVTELECOM, CVMOVEL et CVMULTIMEDIA) qui constituent aujourd'hui le groupe CVTelecom.

57. M. Rocha a décrit comment l'ancien modèle utilisé par l'organisation pour détecter les cas de fraudes dans le secteur des télécommunications était basé sur la collecte de données relatives au trafic international qui représentait la branche d'activité la plus importante de la compagnie. Aujourd'hui toutefois, la protection des systèmes d'information et des infrastructures va au-delà de l'atténuation des effets d'événements qui mettaient à mal la relation entre le fournisseur et ses clients qui devaient faire face à des coûts irréalistes. Dans l'ancien modèle, les efforts portaient essentiellement sur les services de télécommunication alors qu'aujourd'hui l'accent est mis sur la protection des plates-formes de services pour le client, grâce à un produit standard disponible sur le marché. Le système de facturation de la compagnie ne permettait pas de détecter suffisamment rapidement

---

32 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/cardoso-cybercrime-impact-praia-nov-07.pdf.

33 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/rocha-security-in-information-systems-praia-nov-07.pdf.

les cas de fraude. Par conséquent, les dommages subis ont considérablement augmenté, touchant en particulier le trafic international, principale source de recettes pour la compagnie. M. Rocha a expliqué certains des problèmes auxquels la compagnie a dû faire face pour mettre en oeuvre son propre plan de sécurité: nécessité d'être prête en interne, s'agissant de la sécurité, de la formation et de l'actualisation permanente du savoir-faire des techniciens en ce qui concerne les technologies et les techniques concernées, nécessité d'avoir les bons outils et les bons équipements pour pouvoir agir et régler les incidents en situation de crise.

Session 8: Coopération régionale et internationale

58. La coopération régionale et internationale est extrêmement importante pour promouvoir une culture de la sécurité tout comme le rôle des forums régionaux qui sont susceptibles de faciliter le dialogue et les échanges. Les participants ont examiné certaines des initiatives de coopération en cours au niveau régional ou international visant à encourager les participants à prendre part aux nouvelles actions concrètes qui pourraient être mises en oeuvre dans la région de l'Afrique de l'Ouest et aussi au niveau international. L'animateur de la session, M. Sekou Kromah, Ministre des postes et des télécommunications du Libéria, a ouvert la session et présenté les deux orateurs, M. Alain Aina et M. Joel Schwarz.

59. Alain Patrick Aina, membre du SSAC (Stability and Security Advisory Committee) de l'ICANN, Togo, a parlé dans son exposé "Cybersécurité en Afrique: Appel pour une collaboration régionale et internationale/Cybersecurity in Africa: For increased Regional and International Collaboration"[34] de la situation sur le continent africain dans le domaine de la cybersécurité, et indiqué certains des problèmes spécifiques que doivent résoudre ces pays: capacité médiocre des systèmes, ce qui accroît leur vulnérabilité, faiblesse des capacités humaines et techniques, faible déploiement et mauvaise gestion des systèmes, peu de connaissances techniques des utilisateurs. M. Aina a fait observer que même si le continent africain n'offre peut-être pas beaucoup de cibles intéressantes pour les pirates informatiques, il ne faut pas négliger ces pays car ils pourraient être des clients potentiels pour les réseaux zombies afin de lancer des attaques vers d'autres destinations.

60. M. Aina a ensuite parlé d'autres phénomènes spécifiques aux pays africains, notamment l'augmentation du nombre de cybercentres/cybercafés sans qu'il y ait pour autant de législation protégeant les jeunes contre les pédophiles, etc. Il a donné aux participants un aperçu de quelques-unes des initiatives régionales ou internationales, mentionnant les Forums existants AfriPKI, CERT-Tcc in Tunisia, AfNOG, AfriNIC, AfriSPA, AfLTD, etc. Il a souligné qu'en Afrique il faut mieux coordonner les initiatives et renforcer la collaboration régionale et internationale. Etant donné que chaque pays n'a pas nécessairement à lui seul les ressources suffisantes (financières et/ou humaines) pour se protéger contre les pirates informatiques, la coopération est encore plus importante pour les pays africains. L'orateur a proposé d'adopter trois principes pour stimuler la coopération régionale dans le domaine de la sécurité: a) assurer une sécurité basée sur les compétences africaines; b) éviter de réinventer la roue; et c) adopter une approche multi-parties prenantes impliquant la société civile, les pouvoirs publics et le secteur privé. Il a ajouté que le fait de donner davantage d'argent aux universités pour les inciter à s'engager dans le domaine de la sécurité au niveau de la région pourrait être un pas en avant positif et nécessaire.

61. En conclusion, M. Aina a formulé des recommandations visant à faire de la sécurité de l'Internet un grand axe de la coopération régionale et internationale, étant entendu qu'il faut mettre en place un cadre juridique, instaurer la confiance dans le numérique en vue du développement, du renforcement des capacités, et de l'établissement d'une capacité de veille, d'alerte et de réponse aux incidents dans chaque pays d'Afrique et associer activement le continent africain aux efforts déployés à l'échelle mondiale dans le domaine de la cybersécurité.

62. Joel Schwarz, Computer Crime & Intellectual Property Section (CCIPS), Ministère de la justice, Etats-Unis d'Amérique, a parlé dans son exposé de la "Coopération internationale dans les enquêtes sur la cybercriminalité"[35]. Il a d'abord passé brièvement en revue les problèmes que pose la mondialisation des enquêtes judiciaires et a ajouté qu'il fallait promulguer des lois adéquates permettant d'ériger en infraction pénale l'utilisation des ordinateurs à des fins délictueuses, de mobiliser un personnel et des ressources suffisantes, d'améliorer les capacités de localisation et d'identification des délinquants ainsi que de collecte et de partage des éléments de preuve au niveau international afin de traduire ces délinquants devant la justice. M. Schwarz a souligné qu'il fallait d'urgence ériger en infraction pénale les attaques de pirates informatiques dans tous les pays, faisant observer que lorsqu'un pays sanctionne un certain comportement, et qu'un autre pays ne le fait pas, il n'y a pas nécessairement de passerelle de coopération (on parle de "double incrimination"). On a donc besoin de traités d'extradition et de traités d'assistance juridique mutuelle. La Convention de Budapest sur la cybercriminalité[36] (2001) peut faire office de traité d'assistance juridique mutuelle lorsqu'il n'y a pas de traité en vigueur ou de modèle garantissant l'incrimination de certains actes dans chaque pays. L'orateur a fait observer que les législations ne doivent pas nécessairement porter le même nom ou avoir le même jargon. Il a

---

34 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/aina-cybersecurity-africa-praia-nov-07.pdf.

35 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/schwarz-international-cooperation-praia-nov-07.pdf.

36 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

souligné que, pour faire appliquer la loi, il faut qu'il y ait dans chaque pays des compétences et des spécialistes de la délinquance technologique. En d'autres termes, des experts disponibles 24 heures sur 24 doivent recevoir une formation continue et être dotés d'équipements en permanence mis à niveau.

63. Pour aider les participants à l'atelier à mieux comprendre toute l'importance d'une coopération internationale dans le domaine de l'application des lois, M. Schwarz a estimé qu'il serait utile d'examiner un cas particulier. La première chose à faire dans une enquête est de localiser l'auteur de l'attaque ou de la communication. Il est souvent relativement facile de découvrir ce qui s'est passé mais il est très difficile d'identifier la personne responsable. Les informations doivent être partagées entre les parties prenantes et entre les pays. Les pays doivent améliorer leur capacité à partager rapidement les informations car si ce partage ne se fait pas rapidement, on risque de perdre très vite la "trace" électronique. Malheureusement, la mise en place de la plupart des mécanismes de coopération prend des mois, voire des années et non quelques minutes.

64. M. Schwarz a fait observer qu'en signant la Convention sur la cybercriminalité, les parties acceptent de fournir une assistance à d'autres pays pour obtenir et divulguer des éléments de preuve électroniques. A cet égard, l'article 30 de la Convention porte sur la divulgation rapide des données relatives au trafic, sur la nécessité pour chaque pays de conserver les données relatives au trafic, d'informer un pays demandeur si une "trace" conduit à un pays tiers et de fournir suffisamment de données pour donner suite à la demande d'assistance d'un pays tiers. Pour travailler ensemble à l'identification des cibles, M. Schwarz a également parlé d'une initiative du G8, le réseau 24/7 sur la criminalité informatique, qui est un réseau de points de contact d'urgence pour lutter contre les comportements délictueux dans le cyberespace. Ce réseau est constitué de personnes responsables de l'application des lois qui partagent des informations et des avis sur la conservation des données, sur les points de contact ISP et sur les modalités à suivre pour engager des procédures d'assistance juridique mutuelle. Actuellement, le réseau 24/7 a des points de contact dans près de 50 pays. Ce réseau est ouvert à tous et M. Schwarz a indiqué qu'il est facile d'en devenir membre. La seule condition est la disponibilité mais cela ne signifie pas nécessairement que l'on s'engage à apporter une aide. Les pays qui souhaitent se connecter au réseau doivent définir un point de contact principal qui a suffisamment de connaissances techniques dans le domaine de la cybercriminalité, l'un des problèmes essentiels en la matière étant le traitement des preuves numériques résultant de la criminalistique. La personne doit aussi connaître la législation et les procédures nationales existant dans ce domaine bien particulier. M. Schwarz a précisé que les pays qui souhaitent en apprendre davantage sur le réseau peuvent prendre contact avec le CCIPS (Computer Crime and Intellectual Property Section)[37] auprès du Ministère de la justice.

Session 9: Synthèse, Recommandations et activités futures

65. La dernière session de la réunion, animée conjointement par Robert Shaw, Division de la cybersécurité et des applications TIC du Secteur du développement des télécommunications de l'Union (UIT-D) et David Gomes, ANAC (Agencia Nacional das Comunicações), Cap-Vert, a permis de faire la synthèse des différentes sessions de l'atelier et de poser des questions sur les stratégies, les solutions et les partenariats futurs. Il faut maintenant définir des cadres pour faire progresser les discussions relatives à la cybersécurité et la protection des infrastructures essentielles de l'information. M. Shaw a fait observer que, pendant les trois jours de l'atelier, les participants ont écouté toute une série d'exposés très intéressants portant sur les principaux problèmes que rencontrent les pays africains dans le domaine de la cybersécurité et obtenu des informations sur les travaux en cours à l'UIT, dans d'autres organisations internationales et régionales et dans différents pays pour améliorer la cybersécurité. Il est apparu que l'amélioration de la cybersécurité est un problème d'envergure mondiale et que chaque pays doit s'associer aux efforts déployés au niveau international dans ce domaine. Au cours de l'atelier, des échanges ont eu lieu sur les activités et les méthodes qui ont donné de bons résultats dans d'autres pays et régions. Les représentants des cinq grands domaines sont repartis avec un dossier reflétant non seulement les débats qui ont eu lieu au cours de la session qui les concernait mais aussi leurs points de vue sur certaines mesures possibles et constructives pour aller de l'avant.

66. **Sessions 1 et 2: Cadres pour la cybersécurité et la protection des infrastructures essentielles de l'information**: Joseph Richardson, Etats-Unis d'Amérique, a attiré l'attention des participants à l'atelier sur le kit UIT d'autoévaluation sur la cybersécurité et la protection des infrastructures essentielles de l'information, qui peut servir de point de départ pour l'élaboration d'une stratégie sur la cybersécurité et aider chaque pays à déterminer où il en est et à hiérarchiser ses activités en fonction de ses besoins spécifiques. M. Richardson a utilisé une métaphore empruntée au football pour faire comprendre aux participants pourquoi les initiatives relatives à la cybersécurité devaient être engagées sans plus tarder. Il a expliqué que la cybersécurité était comme un terrain de football à plusieurs dimensions où chaque pays avait son propre terrain et que ce que chacun faisait sur son terrain affectait le terrain des autres pays. Dans un environnement aussi complexe, ce dont on a besoin c'est d'un cadre qu'un pays peut utiliser pour structurer son équipe nationale, faire en sorte que tous les joueurs présents simultanément sur le terrain coopèrent pour défendre au mieux les couleurs nationales tout en aidant à protéger le terrain des autres pays. M. Richardson a expliqué que l'UIT est prête à aider les pays à sensibiliser les personnes concernées à leurs responsabilités, à parler avec les pays intéressés des différentes questions et des cadres qui ont été examinés au cours de ces trois jours. Concrètement, cela pourrait se faire

[37] http://www.cybercrime.gov.

dans chaque pays, peut-être même au sein de petits groupes de pays dans les différentes régions, afin d'utiliser au mieux les ressources limitées. L'orateur a utilisé une analogie empruntée au football à propos du partage des informations avec les parties concernées dans les différents pays en vue de l'élaboration d'un cadre pour la cybersécurité et la protection des infrastructures essentielles de l'information.

67. **Sessions 3, 4 et 5: Fondements juridiques, démarche réglementaire et application des lois**: Marco Gercke (Allemagne), a souligné dans ses remarques qu'il y a deux types de conférences: celles où l'on se contente de parler et celles qui produisent des résultats concrets. A propos des récents ateliers régionaux de l'UIT sur les cadres pour la cybersécurité et la protection des infrastructures essentielles de l'information qui se sont tenus à Hanoï (Viet Nam), en août 2007[38] et à Buenos Aires (Argentine), en octobre 2007[39], il a fait observer que ces conférences avaient marqué le point de départ de nombreux autres types d'activités dans les différentes régions et au niveau international. Il a indiqué que l'atelier au Cap-Vert avait déjà produit des résultats. Les bons contacts qui ont été établis avec les différentes parties prenantes et le réseau peuvent conduire à des résultats positifs. L'orateur a exprimé l'espoir que les travaux concrets qui ont été réalisés ici et dans d'autres conférences connexes puissent se poursuivre et que les pays puissent obtenir l'assistance dont ils ont besoin pour mettre en place des cadres nationaux pour une cybersécurité améliorée.

68. **Session 6: Capacités de veille, d'alerte et de réponse aux incidents informatiques**: Belhassen Zouari, ANSI (National Agency for Computer Security), CERT-Tcc, Tunisie, a noté que l'atelier avait permis aux participants et aux orateurs de partager un grand nombre d'idées différentes sur la façon de répondre aux problèmes que rencontrent les pays pour combattre les menaces sur la cybersécurité. Il a estimé que les différents exposés avaient donné un bon aperçu des questions qu'il convenait de traiter en priorité ainsi que des outils utiles permettant aux pays de régler ces problèmes.

69. **Session 7: Collaboration entre les pouvoirs publics et le secteur privé**: El Hadji Mansor Sy Tandine, représentant de la Présidence de la République du Sénégal, a indiqué que des messages importants concernant la cybersécurité et la protection des infrastructures essentielles de l'information ont été adressés, lors de l'atelier, dans les différentes présentations et que la cybersécurité doit être une question hautement prioritaire pour les pays. M. Tandine a souhaité que les délégués présents à l'atelier puissent relayer ces messages dans leurs propres pays. Il a également exprimé l'espoir qu'une réunion similaire puisse avoir lieu de nouveau dans la région dans un avenir proche. Il a souligné qu'il n'y a plus aucune excuse pour ne pas agir pour une meilleure sécurité dans le cyberespace et a indiqué qu'il fallait une plus grande harmonisation entre les pays de la région et au-delà.

70. **Session 8: Coopération régionale et internationale:** M. Basil Udotai, Directorate for Cybersecurity, Office of the National Security Adviser, Nigéria, et M. Alain Aina, membre du SSAC (Stability and Security Advisory Committee) de l'ICANN, Togo, ont brièvement rendu compte des principaux enseignements qu'ils avaient tirés de la manifestation. M. Aina a souligné qu'il était nécessaire de renforcer la coopération afin d'utiliser les synergies et d'oeuvrer à une meilleure cybersécurité dans le monde. M. Udotai a déclaré que cet atelier de trois jours avait fait apparaître une convergence en ce qui concerne non seulement la nécessité et la réalité de la cybersécurité mais aussi une convergence des différents modèles et des différentes approches pour améliorer la cybersécurité. Il a indiqué qu'il fallait peut-être aujourd'hui privilégier les mesures concrètes susceptibles d'être adoptées aux niveaux national, régional et international pour créer une culture de la cybersécurité. Il a fait observer que des organisations comme l'UIT, le Conseil de l'Europe, etc., sont prêtes à apporter des solutions réelles pour les pays africains et que de bons exemples de ce qui peut être fait dans ce domaine ont été donnés au cours de l'atelier. M. Udotai a demandé aux participants de s'assurer que les dirigeants des pays représentés à l'atelier comprennent bien les questions en jeu et les mesures de suivi qui doivent être prises pour aller de l'avant.

Clôture de la réunion

71. David Gomes, Agencia Nacional das Comunicações (ANAC), Cap-Vert, a fait observer que la sécurité n'est plus un problème spécifique aux technologies de l'information, à telle ou telle organisation, au secteur privé ou aux pouvoirs publics et que les pays doivent faire en sorte que les menaces et les vulnérabilités liées à la cybersécurité soient traitées de manière coordonnée dans tous ces domaines.

72. Dans ses remarques de clôture[40], au nom de l'Union internationale des télécommunications, Mme Margarida Evora-Sagna, représentante du Bureau de zone de l'UIT pour l'Afrique de l'Ouest, a remercié chacun des participants, qui directement ou indirectement, a contribué à la réussite de cet atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection des infrastructures essentielles de l'information. Elle a transmis des remerciements tout particuliers au pays hôte, le Cap-Vert, au Gouvernement de ce pays, au Ministre de l'infrastructure, des transports et de la mer, au Ministre de la Justice et à l'Agência Nacional das Comunicações (ANAC) pour leur travail remarquable grâce auquel cet atelier régional sur la cybersécurité a pu être un franc succès. Elle a également mentionné les sponsors de l'atelier, CVTelecom,

---

38 http://www.itu.int/ITU-D/cyb/events/2007/hanoi/.

39 http://www.itu.int/ITU-D/cyb/events/2007/buenos-aires/.

40 http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/evora-sagna-closing-remarks-praia-29-nov-07.pdf.

CVMovel, CVMultimedia, etc., qui ont répondu immédiatement à l'invitation qui leur avait été adressée de rejoindre les organisateurs de la manifestation ainsi que tous les orateurs qui, malgré leur calendrier chargé, ont pris le temps de venir partager leurs expériences et leurs compétences techniques avec les participants. Enfin, Mme Evora-Sagna a remercié les interprètes qui ont assuré une excellente interprétation en anglais, français et portugais pendant les trois jours de l'atelier ainsi que les délégués pour leur attention, leur participation active et leurs contributions. 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.

73. C'est M. Jose Manuel Andrade, Ministre de la Justice du Cap-Vert qui a prononcé les dernières remarques de clôture. Il a souhaité que ces trois jours au Cap-Vert, riches en discussions très fructueuses aient été utiles aux participants à l'atelier. Il a fait remarquer qu'aujourd'hui on ne saurait parler de cyberespace sans parler de cybersécurité, et que tous sont conscients du fait que la société de l'information est un véritable défi pour le Cap-Vert, étant donné que l'avènement de cette société apporte avec elle des bouleversements non seulement techniques mais aussi politiques et sociaux. Il a souligné que dans chaque pays la société de l'information devrait être étroitement liée à la société au sens large et qu'il appartient aux gouvernements de mettre en place les mesures et les outils nécessaires pour combattre les nombreuses menaces dont il a été question pendant l'atelier afin de construire une culture de la cybersécurité. Il a reconnu que le Cap-Vert s'était pleinement engagé dans un certain nombre d'initiatives relatives à la création d'un comité/d'une commission chargé(e) des informations sensibles, étant donné que de plus en plus les données traversent les frontières, et avait aussi approuvé une loi sur la cybersécurité. Il a noté que l'adhésion à la Convention de Budapest sur la cybercriminalité (2001) est un objectif pour le Cap-Vert. Il a poursuivi en ajoutant que les organismes du pays devaient s'engager à appuyer ces initiatives et à garantir la cybersécurité pour tous les citoyens.

Le présent projet de rapport 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 de l'atelier. L'adresse électronique pour faire parvenir vos observations sur ce projet de rapport ou sur le programme de travail de l'UIT sur la cybersécurité en faveur des pays en développement (2007-2009)[41], est **cybmail(at)itu.int**[42]. A des fins de partage des informations, les noms de tous les participants seront ajoutés aux listes de diffusion électroniques (**cybersecurity-africa@itu.int**) et forums 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**.

_____

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

42 Veuillez nous faire parvenir vos éventuelles observations sur le rapport de l'atelier à l'adresse cybmail@itu.int.