Forum régional UIT 2009 sur la cybersécurité, Tunis (Tunisie)

Document RFT/2009/01-F

8 juin 2009

Original : anglais

Projet de rapport sur les travaux de la réunion :

Forum régional UIT sur la cybersécurité pour l'Afrique et les États arabes, tenu à Tunis (Tunisie) (4-5 juin 2009)[1]

Prière de faire parvenir toute observation relative au présent rapport à cybmail(at)itu.int

Objet du présent compte rendu

1. Le Forum régional UIT 2009 sur la cybersécurité pour l'Afrique et les États arabes s'est tenu à Tunis (Tunisie) les 4 et 5 juin 2009. Le forum, accueilli par l'Agence nationale pour la sécurité informatique (ANSI) (laquelle est rattachée au Ministère tunisien des technologies de la communication) était consacré au thème « Connecter le monde de manière responsable » et avait pour objet d'identifier certains des principaux problèmes auxquels les pays de la région doivent faire face pour renforcer la cybersécurité et sécuriser les infrastructures essentielles de l'information. Les participants au forum ont examiné les meilleures pratiques, les mécanismes de partage d'information et les mesures concrètes à prendre pour renforcer la cybersécurité, compte tenu de principes fondamentaux tels que la prise en compte de la nature décloisonnée et transnationale des cybermenaces, tout en répondant à des besoins précis aux niveaux national et régional. Ils ont également analysé les mesures prises ou envisagées par les pays de la région pour accroître la coopération et la collaboration avec d'autres parties prenantes, sur les plans national, régional et international.

2. Ce forum, qui s'inscrit dans une série de manifestations régionales sur la cybersécurité organisée par le Secteur du développement des télécommunications de l'UIT (UIT-D), s'est tenu conformément à la Résolution 130 (Antalya, 2006) de la Conférence de plénipotentiaires de l'UIT, intitulée « Renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication », et au Plan d'action établi en 2006 par la Conférence mondiale de développement des télécommunications de Doha définissant la Question 22/1 devant être étudiée par les Commissions d'études de l'UIT-D : Sécurisation des réseaux d'information et de communication : meilleures pratiques pour créer une culture de la cybersécurité » et pour réaliser les objectifs du Programme mondial cybersécurité (GCA) de l'UIT. Des spécialistes de divers secteurs spécifiques de la cybersécurité, venus d'institutions des Nations Unies, d'organisations internationales et régionales, d'institutions financières, d'entreprises privées, d'organisations non-gouvernementales et de représentants d'organismes publics de 25 pays d'Afrique et des États arabes, ont examiné et peaufiné des mesures concrètes à prendre pour renforcer la capacité et les compétences en matière de cybersécurité grâce au partage d'information et de données d'expérience et à l'idée de créer des partenariats et d'approfondir ensemble ces questions. Une documentation complète sur le Forum, comprenant l'ordre du jour définitif et tous les documents présentés, est affichée sur le site web correspondant : www.itu.int/itu-d/cyb/events/2009/tunis/. Le présent compte rendu de la réunion[2] résume la teneur des deux jours de débats du Forum régional UIT sur la cybersécurité pour l'Afrique et les États arabes et donne un aperçu de haut niveau des sessions et des interventions des orateurs ainsi que de certaines prises de position commune constatées à l'occasion de cette manifestation. L'interprétation simultanée en anglais, arabe et français a été assurée durant tout le forum.

---

[1] Site web du Forum régional UIT sur la cybersécurité: http://www.itu.int/ITU-D/cyb/events/2009/tunis/

[2] Le présent rapport sur le Forum peut être consulté en ligne: http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/tunis-cybersecurity-forum-report-june-09-fr.pdf

Forum régional sur la cybersécurité pour l'Afrique et les États arabes, tenu à Tunis (Tunisie), les 4 et 5 juin 2009

3. Situons le débat dans son contexte général : on s'accorde le plus souvent à penser que les technologies de l'information et des communications (TIC) sont à même de jouer un rôle décisif dans le processus de développement d'un pays. Cela étant, la croissance rapide des TIC a également ouvert aux criminels de nouvelles voies pour exploiter les vulnérabilités susceptibles de se manifester sur la Toile mais aussi pour s'en prendre aux infrastructures essentielles des pays. Pour cette raison, l'instauration de la confiance et de la sécurité dans l'utilisation des TIC constitue l'un des enjeux les plus importants et les plus complexes auxquels les pays sont actuellement confrontés. Étant donné que le cyberespace est dans une grande mesure sans frontières nationales nettes et que les cybermenaces peuvent frapper partout et à tout moment, provoquant en un laps de temps très court d'énormes dégâts avant même qu'on puisse tenter d'y remédier, les tentatives actuelles visant à résoudre ces problèmes sur les seuls plans national et régional sont insuffisantes. Une approche mondiale s'impose donc et c'est pourquoi l'UIT, dans le cadre de son Programme mondial cybersécurité, a mis en place un cadre pour la coopération internationale dans le domaine de la cybersécurité. La cybersécurité et la protection des infrastructures essentielles de l'information relèvent de la responsabilité conjointe de l'État, des entreprises et des autres organisations, ainsi que des particuliers, c'est-à-dire de tous ceux qui interviennent dans les technologies, systèmes et réseaux de l'information et des communications, que ce soit au niveau de la conception, des droits de propriété, de la prestation de services, de la gestion, de l'entretien ou encore de l'utilisation. La promotion de la cybersécurité et la mise en place de mesures correspondantes se doivent d'être hautement prioritaires si l'on veut que les pays puissent bénéficier pleinement de la révolution numérique et des nouvelles technologies de communication, en pleine évolution. Les participants au Forum ont analysé un certain nombre des éléments essentiels permettant de mettre au point ces politiques générales et réglementaires et ont proposé des initiatives concrètes que l'on peut prendre pour mettre en œuvre ces politiques dans les deux régions visées.

Ouverture de la réunion et allocution de bienvenue

4. C'est Belhassen Zouari, Directeur général de l'Agence nationale pour la sécurité informatique et du CERT-TCC, qui a souhaité la bienvenue aux participants au forum, soulignant à quel point cette manifestation était une étape importante vers la mise en place d'une capacité de cybersécurité en Afrique et dans les États arabes. Le Forum régional UIT sur la cybersécurité pour l'Afrique et les États arabes a été ouvert par S.E. Lamia Sghair Chaffai, Secrétaire d'État de la Tunisie chargée de l'informatique, de l'Internet et des logiciels libres, qui a prononcé l'allocution de bienvenue[3]. Au nom du Gouvernement tunisien, sous les auspices duquel se tenait la manifestation, Mme Chaffai a appelé l'attention des participants sur le Sommet mondial sur la société de l'information, l'Engagement de Tunis et le Programme de Tunis pour la société de l'information[4], faisant valoir la nécessité d'accorder à la question de la confiance et de la sécurité dans l'utilisation des TIC une grande priorité dans les programmes nationaux de développement des TIC. Elle a de plus souligné la nécessité de promouvoir la multiplication de partenariats de divers types entre les pays de la région, d'autres pays représentés à la manifestation mais aussi au-delà. Mme Chaffai a dit que la Tunisie était un pionnier dans le domaine des TIC, et plus particulièrement de la cybersécurité. Outre la stratégie nationale de la Tunisie en matière de sécurité et les services assurés par l'Agence nationale pour la sécurité informatique (ANSI), elle a relevé la nécessité d'un environnement juridique propice pour protéger les investisseurs.

5. Mme Chaffai a dit que, par exemple, en vertu de la législation, l'audit informatique est désormais obligatoire en Tunisie, et que le pays s'est également doté d'une législation spécifique prévoyant l'identification électronique. S'agissant du renforcement des capacités, de la formation et de l'enseignement, la Tunisie a réussi à créer le premier institut national de la sécurité sur le continent africain ; l'Équipe de réponses aux urgences informatiques – Centre de coordination tunisien (CERT-TCC), membre du Consortium d'équipes chargées de la sécurité informatique et des interventions en cas d'incident (FIRST). La Tunisie compte par ailleurs sept programmes universitaires au niveau du mastère qui visent à renforcer les capacités dans le domaine de la sécurité des réseaux et de l'information ; et a mis en place un réseau national d'auditeurs. Mme Chaffai a conclu ses propos liminaires en soulignant que, doté d'un programme ambitieux rendant compte de nombreux volets de la cybersécurité, le Forum régional sur la cybersécurité représente l'occasion pour les organisations et les pays de la région de se rencontrer pour partager leurs données d'expérience. Elle a appelé de ses vœux une collaboration plus étroite entre les parties prenantes africaines et arabes pour qu'elles œuvrent à la réalisation d'objectifs communs dans le domaine de la cybersécurité dans le but d'édifier une société de l'information à la fois inclusive et sécurisée.

6. Khedija Gheriani, Secrétaire général de l'Organisation arabe pour les TIC (AICTO) a elle aussi fait l'honneur d'assister à la session d'ouverture. L'AICTO est une organisation gouvernementale arabe travaillant sous l'égide de la Ligue des États arabes, laquelle est basée en Tunisie. Dans le cadre de la Stratégie arabe générale en

[3] Texte non disponible.

[4] http://www.itu.int/wsis/

matière de TIC visant à instaurer la société de l'information, 2007-2012, l'AICTO et ses groupes de travail mènent des activités dans tout un ensemble de domaines : administration électronique, commerce en ligne et cyber-éducation, mais aussi sécurité de l'information et sécurité informatique, etc.

7. Miloud Ameziane, Chef du Bureau régional de l'UIT pour les États arabes, a prononcé un discours liminaire[5] au nom de Sami Al Basheer Al Morshid, Directeur du Bureau de développement des télécommunications de l'UIT. Il a souhaité la bienvenue aux participants au forum et souligné à quel point les questions ayant trait à la cybersécurité constituaient un ensemble complexe de défis à la fois technologiques, politiques et culturels. Avec le nombre d'abonnés à un cellulaire mobile atteignant 4 milliards et un taux de pénétration estimé à 61 pour cent, M. Ameziane a rappelé aux participants le rôle capital des TIC dans la vie des gens. Parallèlement à l'apparition de nouvelles technologies et à l'accroissement de l'utilisation des TIC, les menaces contre la sécurité de ces technologies se multiplient elles aussi, a-t-il relevé. Ces menaces se manifestent au niveau mondial : l'attaque lancée depuis un pays peut avoir un impact dans un autre pays, alors que l'auteur peut fort bien se trouver dans un autre pays encore. Pour garantir la cybersécurité, il nous faut donc adopter une vision mondiale du problème et nous accorder sur la manière de tenir compte des besoins de tous les pays : pays les moins développés, pays en développement et pays développés. Ce n'est qu'en travaillant ensemble pour mettre au point des stratégies et recenser les meilleures pratiques que nous pourrons résoudre ces problèmes, qui se posent au niveau mondial, a poursuivi M. Ameziane.

8. M. Ameziane a de plus rappelé aux participants que la manifestation intervient dans le droit fil des activités lancées à l'occasion du Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe tenu à Lusaka (Zambie) du 25 au 28 août 2008 et de l'atelier régional correspondant sur les cadres pour la cybersécurité et les infrastructures essentielles de l'information (CIIP) pour les États arabes, organisé à Doha (Qatar) du 18 au 21 février 2008. Il a continué en expliquant de quelle manière les conclusions de cette manifestation-là entretenaient des liens avec les activités relevant du Programme mondial cybersécurité de l'UIT. Les dirigeants mondiaux présents au Sommet mondial sur la société de l'information ont chargé l'UIT de coordonner la grande orientation C5 - Établir la confiance et la sécurité dans l'utilisation des TIC – et, en réponse, l'UIT a lancé le Programme mondial cybersécurité. M. Ameziane a en outre noté que l'UIT avait lancé le Programme mondial cybersécurité en 2007 à titre de mécanisme et de cadre de coopération et d'intervention internationales. À ce titre, le Programme vise à favoriser les synergies, à créer des partenariats et à instaurer une collaboration entre toutes les parties prenantes dans la lutte contre les cybermenaces, et ce dans le cadre de cinq grands secteurs : 1. Mesures juridiques ; 2. Mesures techniques et procédurales ; 3. Structures administratives et mesures transversales 4. Renforcement des capacités, et 5. Coopération internationale. Enfin, M. Ameziane a invité les participants au forum à approfondir le dialogue et la réflexion au cours des deux jours durant lesquels se déroulerait le forum et à élaborer un plan de travail concret visant le renforcement des capacités en matière de cybersécurité en Afrique et dans les États arabes.

Session 1: Vers une approche intégrée de la cybersécurité et de la protection des infrastructures essentielles de l'information

9. La confiance et la sécurité dans l'utilisation des technologies de l'information et des communications sont essentielles à l'édification d'une société de l'information inclusive, sure et universelle. L'évolution permanente de l'utilisation des TIC, des systèmes et des réseaux présente des avantages incontestables, mais, parallèlement, les États, le secteur privé, les organisations et les particuliers qui utilisent ces technologies – autrement dit, tous ceux qui mettent au point, possèdent, fournissent, gèrent, entretiennent et utilisent ces réseaux doivent faire davantage porter leurs efforts sur la cybersécurité et la protection des infrastructures essentielles de l'information. En raison des interconnexions entre les TIC, on ne peut en effet véritablement promouvoir la cybersécurité que si toutes les parties prenantes sont conscientes des dangers et des menaces existants et savent comment se protéger à l'occasion de leurs activités en ligne. L'État doit assumer un rôle de premier plan pour instaurer une culture favorable à la cybersécurité et pour soutenir les efforts déployés par d'autres parties prenantes à cet égard. En outre, la coopération régionale et internationale est essentielle pour encourager une culture mondiale de la cybersécurité.

10. La première session du forum, présidée par Mongi Hamdi, Chef du Service de la science, de la technologie et des TIC, (UNCTAD)/(CNUCED), et Chef du Secrétariat de la Commission des Nations Unies sur la science et la technologie au service du développement, a tracé un portrait général des cybermenaces actuelles et fait le point des défis que les pays, les entreprises et les particuliers doivent relever pour gérer leur quotidien dans un environnement en évolution constante. M. Hamdi a note que la raison d'être du forum était d'aider les pays à mieux comprendre les différentes responsabilités incombant à toutes les parties prenantes sur le plan de la sécurisation de l'information, et d'aider les pays à mettre au point une approche nationale de la cybersécurité. Les questions de cybersécurité sont en effet cruciales pour toutes les parties en jeu. Le nombre d'utilisateurs de l'Internet étant de quelque 1,4 milliard, et en progression constante, la cybersécurité doit elle aussi progresser au même rythme. M. Hamdi a souligné le rôle de premier plan que les pouvoirs publics doivent assumer pour promouvoir une culture de la cybersécurité, comme précisé dans les résolutions 57/239 (2002)[6] et 58/199

[5] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/itu-opening-remarks-june-09.pdf

[6] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

(2004)[7] des Nations Unies sur la création d'une culture mondiale de la cybersécurité et sur la protection des infrastructures essentielles de l'information. Il a noté l'urgence qu'il y avait à prendre des initiatives dans le domaine de la cybersécurité, car les utilisateurs ne pourront tirer pleinement profit de l'Internet tant que la sécurité ne peut en être assurée.

11. Dans son intervention, Mohd Shamir Hashim, Chef du Département de politique stratégique et de recherche sur les cybermédia, CyberSecurity Malaysia (Malaisie), et représentant de l'Équipe d'intervention en cas d'urgence informatique de l'Organisation de la Conférence islamique (OCI-CERT), a présenté la politique nationale de la Malaisie en matière de cybersécurité [8]. M. Hashim a noté que, comme bien d'autres pays, la Malaisie est empoisonnée par toutes sortes de cybermenaces ; c'est pour riposter à la multiplication de ces menaces que le Ministère malaisien de la science, de la technologie et de l'innovation a mené, en 2005, une étude sur l'élaboration d'une politique nationale en matière de cybersécurité (NCSP). Cette politique vise à « veiller à ce que les infrastructures nationales essentielles de l'information soient sécurisées, résilientes et autonomes. Prenant appui sur une culture de la sécurité, la politique sera à même de promouvoir la stabilité, le bien-être social et la création de richesses ». Le gouvernement a accepté les conclusions de cette étude en 2006, en vue de sa mise en œuvre. Il s'agit principalement de rendre plus résilientes les infrastructures nationales essentielles de l'information, celles-ci étant recensées comme étant les biens (réels et virtuels), les systèmes et les fonctions essentielles à la nation et dont l'incapacité ou la destruction porterait un coup dévastateur à la défense et à la sécurité nationales, à la croissance économique et à l'image du pays, à la capacité de l'État de fonctionner et à la santé et à la sécurité publiques. M. Hashim a donné un aperçu de la politique en matière de cybersécurité avec ses huit grandes orientations, à chacune de celles-ci correspondant un certain nombre de résultats escomptés. Il a en outre noté que la politique adoptée recensait 10 secteurs constituent l'infrastructure nationale essentielle de l'information (CNII) de la Malaisie : défense & sécurité nationales, banque & finance, information & communication, énergie, transports, eau, services de santé, administration, services d'urgence et alimentation & agriculture.

12. Le caractère essential et interdépendant de la CNII est reconnu ; la politique vise à mettre au point et à établir un programme complet et une série de structures à même de garantir l'efficacité des contrôles de cybersécurité sur les avoirs essentiels. La mise en œuvre de cette politique, a poursuivi M. Hashim, permettra à la Malaisie d'adopter une démarche proactive face aux questions relatives à la cybersécurité, aux plans local et mondial. Une fois la CNII en place, la Malaisie sera en meilleure position pour répondre aux défis et saisir les occasions créées par l'innovation technologique, ce qui aidera à atteindre les objectifs de la Vision à l'horizon 2020 et au-delà. CyberSecurity Malaysia apporte son dynamisme aux domaines ayant trait à la coopération internationale. La création de l'Équipe d'intervention en cas d'urgence informatique de l'Organisation de la Conférence islamique (OIC-CERT) en est un exemple, comme le sont également l'Agence nationale tunisienne pour la sécurité informatique et le CERT-TCC tunisien. Le premier séminaire organisé par l'OCI-CERT s'est tenu début 2009, la Tunisie en assurant le Secrétariat et CyberSecurity Malaysia la présidence. M. Hashim a invité tous les pays membres de l'OCI d'adhérer à l'OCI-CERT, qui est une organisation qui encourage et appuie la collaboration et la coopération entre le CERT des pays membres de l'OCI.

13. Ian Cook (défenseur de la sécurité, Team Cymru Research), dans le cadre de son intervention intitulée « Prévoir l'imprévu – Les incidences, sur le plan de la sécurité, de l'élargissement de la largeur de bande » [9] a fait part des constatations de Team Cymru - entreprise spécialisée en recherche sur la sécurité de l'Internet – à l'occasion de recherches sur le « qui » et le « pourquoi » des activités malveillantes menées sur l'Internet à l'échelle mondiale. Team Cymru, a fait savoir M. Cook, s'intéresse principalement aux auteurs et aux raisons de cette utilisation malveillante, et c'est précisément pour cette raison que son entreprise surveille l'Internet de près. M. Cook a expliqué comment les câbles sous-marins reliant le continent africain et les États arabes au reste du monde, et l'élargissement de la largeur de bande qui en sera la conséquence, aura un impact sur les populations de la région au niveau de la multiplication probable des utilisations malveillantes. Invoquant des statistiques portant sur d'autres régions du monde, il a tenté de montrer ce qui se passe au niveau des cybermenaces et d'autres activités lorsque de nouveaux utilisateurs et de nouveaux pays accèdent à l'Internet. M. Cook a également donné des précisions sur la manière dont les ordinateurs et les appareils sont récupérés par des réseaux zombies. Il a conclu en donnant quelques astuces pour contrer la montée éventuelle des cybermenaces lorsque la largeur de bande augmentera dans la région. Il s'agit de bloquer d'urgence les réseaux zombies (on peut notamment s'abonner à des fichiers qui facilitent la tâche), bloquer l'accès aux serveurs Web infectés, surveiller dans chaque pays l'activité malveillante sur l'Internet, mettre en place une Équipe nationale d'intervention en cas d'urgence informatique (CSIRT)/Équipe d'intervention en cas d'incident(CIRT) ; dispenser une formation sur les interventions en cas d'incident ainsi qu'une formation à l'intention des forces de l'ordre et des fournisseurs d'accès Internet et, enfin, sensibiliser le grand public.

---

[7] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[8] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashim-cybersecurity-malaysia-june-09.pdf

[9] Diapositives non disponibles.

14. Salma Abbasi, Présidente du e-Worldwide Group, est ensuite intervenue sur le thème « Comment répondre aux défis que constitue la vie dans une société de l'information pour les jeunes et les personnes vulnérables »[10], soulignant par la même occasion les activités en cours dans le cadre de l'initiative de l'UIT sur la protection de l'enfance en ligne, à laquelle elle est associée de près. À mesure que la technologie en vient à être utilisée à tous les niveaux de nos sociétés, par tous les groups d'âge, il devient de plus en plus difficile de protéger les utilisateurs les plus vulnérables contre les dangers et les effets délétères de la technologie du cyberespace, plus précisément les enfants et les jeunes. Mme Abbasi a en outré souligné que le Moyen Orient et l'Afrique représentent les deux régions où l'utilisation de l'Internet progresse le plus rapidement. Cette progression s'accompagne des dangers que les pays occidentaux connaissent déjà. Alors que l'arabe ne représente que 3,7 pour cent du contenu sur l'Internet, ce pourcentage risque fort d'augmenter dans les années à venir étant donné que les pays encouragent des contenus plus localisés pour leurs propres citoyens. Mme Abbasi a évoqué quelques-uns des problèmes, risques et dangers spécifiques qui se posent du fait de l'expansion et de la pénétration de la technologie dans tous les milieux sociaux.

15. Pédophiles, photos humiliantes, harcèlement et intimidation en ligne, mutilation par des enfants se tailladant avec une lame pour s'afficher ensuite sur l'Internet, voila quelques-uns des acteurs et des activités que l'on trouve sur l'Internet. L'innocence et la curiosité des enfants en font la proie privilégiée des agressions et de l'exploitation des cybercriminels, causant un préjudice grave non seulement aux enfants, mais aussi à la collectivité et au pays tout entier. Dans ce contexte, Mme Abbasi a présenté une stratégie d'atténuation et de prévention des problèmes, dangers et risques émanant du cyberespace. Pour relever efficacement ce défi, Mme Abbasi a souligné à quel point il importait d'adopter une démarche mobilisant toutes les parties prenantes, tenant compte de partenariats multisectoriels aux échelons local, national, régional et international. « Si nous utilisons à bon escient le système existant et renforçons le réseau de contacts dont nous disposons pour faire front et pour éduquer les jeunes, nous serons déjà en bien meilleure posture », a-t-elle dit. Mme Abbasi a fait mention des directives que l'UIT est en train d'élaborer dans le cadre d'un effort déployé au plan mondial pour protéger les enfants et les jeunes dans le cyberespace[11]. Ces directives ont été publiées sous forme de projet à l'occasion de la Journée mondiale des télécommunications et de la société de l'information sur le thème « La protection en ligne des enfants » Le projet de directives reprend certaines des principales questions et prévoit des conseils sur la manière dont les décideurs pourraient s'attaquer aux causes du problème et la manière dont l'industrie pourrait en empêcher la prolifération. Les menaces qui pèsent sur le bien-être des enfants et des adolescents constituent un défi qui doit être relevé par toutes les parties prenantes, y compris les enfants eux-mêmes. L'objectif est d'élaborer des directives définitives avant la fin de l'année 2009, dans le cadre de l'initiative Protection de l'enfance en ligne.

16. Mme Abbasi a incité les pays à ne pas se contenter du volet répression, mais aussi à mobiliser l'ensemble des parties prenantes présentes dans le pays, à faire le bilan de la situation, à déterminer où en est le pays, à envisager la création de partenariats, à rassembler l'ensemble des contenus et du matériel et à apprendre à les exploiter, et à mettre au point un plan d'action. L'UIT et IMPACT sont en train de créer un réseau visant à faciliter le travail d'équipe, mais c'est tout de suite qu'il faut commencer, avant qu'il ne soit trop tard. Il existe déjà des contenus dans plusieurs langues ; les pays peuvent d'ores et déjà lancer des campagnes de sensibilisation, organiser des formations spécialisées, procéder au partage des données d'expérience, diffuser des conseils et astuces, etc.

Session 2 : Concilier les enjeux mondiaux et les besoins nationaux et régionaux

17. L'UIT, avec son Programme mondial cybersécurité (GCA), a mis en place un cadre international de coopération en matière de cybersécurité – tribune mondiale dans le cadre de laquelle toutes les parties prenantes intéressées peuvent débattre et collaborer afin de résoudre au mieux et de manière coordonnée les problèmes de cybersécurité, de plus en plus préoccupants. Toutefois, chaque pays et chaque région ont leurs propres impératifs et besoins, dont il faut tenir compte dans le contexte national et régional. L'UIT, avec la coopération de ses États Membres, s'efforce de tenir compte de ces besoins pour que l'aide apportée soit efficace. Les participants à la session 2, présidée par Marco Obiso, Conseiller, Division des applications TIC et de la cybersécurité, Secteur du développement des télécommunications (UIT-D) ont analysé comment une approche ascendante ou descendante peut contribuer à harmoniser les efforts globaux en vue de fournir aux États Membres une réponse et une assistance intégrées et cohérentes.

18. M. Obiso, dans son intervention, a fait le point des activités de l'UIT-D dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information[12]. Il a commencé par les activités générales que mène l'UIT dans le domaine de la cybersécurité, notant que l'on en trouve dans les trois secteurs de l'UIT. Le secteur du développement des télécommunications est au premier plan des activités de l'UIT dans les différentes régions, et travaille de près avec ses partenaires pour concrétiser projets et initiatives. L'adoption d'une approche multilatérale est de la plus haute importance pour toutes les activités de l'UIT, a-t-il rappelé,

---

[10] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/abbasi-child-online-protection-june-09.pdf

[11] http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

[12] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/obiso-overview-itu-activities-june-09.pdf

mais plus encore dans le domaine de la cybersécurité, étant donné que les problèmes qui se posent ne peuvent être traités isolément les uns des autres. Il a souligné que la riposte de l'UIT à ces problèmes faisant l'objet de la grande orientation C5 du Sommet mondial sur la société de l'information - établir la confiance et la sécurité dans l'utilisation des TIC - se trouvait dans le Programme mondial cybersécurité auquel l'UIT a recours pour regrouper et harmoniser les activités internes sur la cybersécurité menées par les trois secteurs de l'UIT et pour travailler avec les parties prenantes, organisations et experts de l'extérieur, dans le but de veiller à l'application des recommandations du Programme.

19. M. Obiso a ensuite donné des précisions sur le Programme de travail de l'UIT-D sur la cybersécurité à l'intention des pays en développement (2007-2009)[13], en fournissant des exemples concrets de ce que l'UIT s'efforce de faire pour apporter une assistance aux pays en développement dans le domaine de la cybersécurité. Grâce aux activités ainsi menées, l'UIT-D aide les pays à renforcer leurs capacités institutionnelles et humaines dans le domaine de la cybersécurité sur divers plans. D'une manière générale, le Programme mondial cybersécurité constitue le cadre de la coopération internationale pour la cybersécurité, portant notamment sur l'identification de stratégies essentielles pour coordonner la riposte internationale aux problèmes croissants qui se posent sur le plan de la cybersécurité ; l'UIT-D aide également les pays à renforcer la confiance et la sécurité dans la société de l'information. De concert avec ses partenaires des secteurs public et privé, l'UIT-D a mis au point des outils relatifs à la cybersécurité pour aider les pays en développement à sensibiliser leurs populations à ce problème et à faire des auto-évaluations sur la cybersécurité au niveau du pays, à assurer des formations et à renforcer les capacités d'une manière générale, mais aussi les capacités spécifiques en matière de dispositifs de veille, d'alerte et de gestion des incidents.

20. Parmi les outils mis au point on trouve notamment les Ressources de l'UIT sur la législation en matière de cybercriminalité[14], destinées à aider les pays à comprendre les aspects juridiques de la cybersécurité et à harmoniser les structures juridiques. Il s'agit en particulier d'un kit de l'UIT pour la législation en matière de cybersécurité[15] qui met à la disposition des pays des modèles de législation et des textes de référence à même de les aider à élaborer des lois et règles de procédure harmonisées. Il existe également une publication de l'UIT intitulée « Guide pour la cybersécurité à l'intention des pays en développement »[16] visant à aider les pays en développement à mieux comprendre les incidences de la multiplication des cybermenaces aux plans national et international, à évaluer les besoins au regard des instruments juridiques existants et à aider les pays à mettre en place des bases juridiques solides. De même, l'initiative de l'UIT d'outil d'auto-évaluation de la cybersécurité/CIIP sur le plan national[17] vise à aider les États-Membres de l'UIT souhaitant consolider leur approche nationale envers la cybersécurité et la protection des infrastructures essentielles de l'information. M. Obiso a également mentionné le kit pour atténuer les effets des "botnet" ou réseaux zombies [18]; la publication du Guide de la cybersécurité pour les pays en développement ; un kit pour promouvoir une culture de la cybersécurité, ainsi que diverses manifestations régionales prévues pour sensibiliser le public et renforcer les capacités dans le domaine de la cybersécurité et de la protection des infrastructures essentielles de l'information. L'UIT œuvre actuellement à diffuser auprès des États Membres l'ensemble de ces ressources, outils de formation et autres produits et services.

21. Dans son intervention intitulée « Mettre en place une capacité de cybersécurité dans les pays en développement aujourd'hui »[19], Benoit Morel, professeur d'applications techniques et de politique générale (Université Carnegie Mellon, États-Unis d'Amérique), a fait valoir la complexité des cybermenaces, la pluri-dimensionnalité de la cybersécurité (avec ses volets juridique, technique, etc.) et la diversité des compétences et capacités qui s'imposent pour résoudre les problèmes à l'échelle nationale. Vu les ressources humaines, institutionnelles et financières qu'il faut mobiliser pour mettre en place une capacité nationale en matière de cybersécurité, que faire pour aider les pays en développement à cet égard ? M. Morel a noté que si les États-Unis et les pays occidentaux avancés ne constituent pas forcément un bon exemple, la Tunisie, avec la création d'une équipe nationale de réponses aux urgences informatiques – Centre de coordination tunisien (CERT/TCC) et de l'Agence nationale pour la sécurité informatique (ANSI) est un modèle intéressant pour les pays en développement souhaitant mettre en place une capacité de veille, d'alerte et d'intervention en cas d'incident. D'une manière plus générale, M. Morel a passé en revue des modalités récentes de cyberattaques – tel le Conficker -, relevant que l'art de mener des cyberattaques progresse plus rapidement que les moyens dont nous disposons pour y riposter. Il s'est arrêté aux raisons pour lesquelles ces exemples devraient inciter les pays à coopérer de manière plus efficace et plus efficiente, au-delà des frontières. La coopération internationale vise notamment à faire du cyberespace un lieu où les auteurs de ces attaques auront du mal à se cacher. Or, on en

---

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

[14] http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[15] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

[16] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

[17] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

[18] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

[19] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/morel-capacity-building-june-09.pdf

est encore bien loin. L'amélioration de la cybersécurité dans les pays en développement n'est pas chose aisée, mais elle est néanmoins essentielle pour la cybersécurité au plan mondial. Plus on laisse de vastes pans de l'infrastructure mondiale à l'abandon, plus il sera difficile de résoudre les problèmes a posteriori. Le renforcement des capacités, l'éducation et la formation sont des aspects importants dans ce contexte. En effet, au plan mondial, le mal en est désormais à un stade aigu, car il nous faudrait bien plus de spécialistes de la cybersécurité que nous n'en avons. Les pays en développement connaissent des difficultés particulières à cet égard.

22. Abraham Djekou, conseiller technique de l'Agence des Télécommunications de Côte d'Ivoire, a ensuite fait une intervention sur le thème "Enseignements et données d'expérience retenus à l'occasion d'une rencontre régionale sur la cybersécurité tenue en Côte d'Ivoire : État des besoins de la région"[20] rédigée de concert avec Didier Kla, ingénieur télécom, Côte d'Ivoire Telecom (Côte d'Ivoire). M. Djekou a dit que d'après le taux de pénétration et d'utilisation des TIC en Côte d'Ivoire, pays en développement comptant plus de 20 millions d'habitants, on constate une augmentation manifeste du volume des activités tributaires des TIC. Le rôle de l'Internet gagne en importance, et le volume des activités délictueuses progresse parallèlement. Le pays met actuellement au point les divers volets d'une stratégie nationale en matière de cybersécurité. La première étape a été la tenue, en juin 2008, d'un forum visant à sensibiliser les différentes parties prenantes à la problématique de la cybersécurité (organismes publics, secteur privé, société civile, milieu universitaire). Le principal résultat de ce forum a été la constitution d'un groupe de travail comptant des représentants des secteurs public et privé et de la société civile, sous les auspices de l'Agence des télécommunications de Côte d'Ivoire (ATCI). Le groupe a été chargé de proposer une législation relative à la cybersécurité, d'identifier et de définir les structures institutionnelles, judiciaires et juridiques qu'il faut impérativement mettre en place pour la cybersécurité (y compris la création d'une agence nationale pour la sécurité, d'un CERT national, d'une agence nationale de certification, etc.) ; mais aussi de formuler une proposition pour la contribution de la Côte d'Ivoire à la coopération internationale dans le domaine de la cybersécurité.

23. Ayant à l'esprit ce mandat, M. Djekou a donné des précisions sur un certain nombre d'activités ayant trait à la cybersécurité qui ont déjà été mises en œuvre ou qui en sont au stade de projet. Par exemple : un projet de loi sur la cybersécurité a été soumis à l'approbation du Gouvernement ; une structure officielle mettant en place une collaboration entre les différents organismes concernés par la cybersécurité est en cours de création ; l'identification des abonnés des opérateurs mobiles sera en place au 1er juillet 2009, alors que les propriétaires de cybercafés sont d'ores et déjà tenus de demander une pièce d'identité à leurs clients ; une convention d'assistance est en cours de signature entre l'ANSI (Tunisie) et l'ATCI (Côte d'Ivoire) dans l'optique de la création d'un CERT national. M. Djekou a également fait le point des conclusions d'une rencontre sur la cybersécurité tenue dans le pays en novembre 2008. Les pays africains qui y avaient assisté ont retenu quatre domaines d'action prioritaires : renforcement des capacités humaines (éducation et formation) ; création d'un environnement favorable (y compris les volets juridique, réglementaire, politique et de plaidoyer), sensibilisation (renforcement de la confiance et de la sécurité et des directives relatives au cyberespace) ; et aspects mondiaux de la cybersécurité (partage de l'information et initiatives de coopération régionale et internationale). Les pays concernés mènent actuellement ces actions au niveau national.

Session 3 : La cybersécurité dans les programmes nationaux et les mesures à envisager lors de l'élaboration d'une stratégie nationale en matière de cybersécurité

24. La nécessité de renforcer la confiance et la sécurité dans l'utilisation des TIC, de promouvoir la cybersécurité et de protéger les infrastructures essentielles sur le plan national est généralement reconnue. Alors que les professionnels des secteurs public et privé ont leur propre conception de ces questions importantes, dans un souci de cohérence, certains pays ont, dans le domaine de la cybersécurité/CIIP, mis en place des cadres institutionnels, tandis que d'autres ont préféré une approche plus souple et moins formelle. Quels sont les problèmes à prendre en compte dans l'élaboration d'une stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information ? Quels professionnels doivent prendre part à cette réflexion ? C'est sous cet angle que les participants à la session 3 ont examiné certains des éléments nécessaires pour déployer et mobiliser sur le plan national les efforts dans le domaine de la cybersécurité /CIIP. Belhassen Zouari, Directeur général de l'Agence nationale pour la sécurité informatique et du CERT-TCC de Tunisie en a assuré les fonctions de modérateur.

25. Le premier exposé a été celui de Taieb Debbagh, Secrétaire général du Département de la poste, des télécommunications et des technologies de l'information (DEPTTI) du Maroc, sur le thème « Système national de gestion de la cybersécurité : structure, modèle de maturité et guide d'exécution » [21] . M. Debbagh a fait part de son expérience en qualité d'ancien membre d'un groupe d'experts de haut niveau[22] et de responsable du secteur de travail 3 du GCA consacré aux structures organisationnelles. Le cadre régissant un système national de gestion de la cybersécurité (NCSecMS) qu'il propose s'articule autour de quatre grands axes : un Cadre national

---

[20] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/kla-cote-divoire-overview-june-09.pdf

[21] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/debbagh-morocco-cybersecurity-june-09.pdf

[22]

pour la cybersécurité (NCSec) ; un modèle de maturité ; les rôles et responsabilités ; un Guide d'exécution. Dans le cadre de l'élaboration du NCSecMS, M. Debbagh et son équipe ont tenu compte des normes et du matériel déjà existants, dont la documentation de l'UIT et celle de l'OCDE, les normes ISO 27001, 27002, 27003, COBIT v 4.1, la matrice RACI permettant de définir les rôles et responsabilités, etc. Le cadre NCSec, par exemple, comprend cinq volets principaux : 1) Stratégie et politiques ; 2) Mise en œuvre et organisation ; 3) Sensibilisation et communication ; 4) Conformité et coordination ; 5) Évaluation et suivi. M. Debbagh a en outre souligné à quel point il importait d'avoir accès à l'information et aux ressources et de sensibiliser le public et les parties prenantes pour pouvoir mettre ce cadre en œuvre. Pour chacun des processus recensés, 17 parties prenantes différentes ont été identifiées, et à chacun de ces processus correspond par ailleurs un niveau de maturité fondé sur le cadre existant COBOLT 4.1.

26. Le volet coopération et collaboration est important pour le cadre d'ensemble ; y correspondent 6 processus. Une fois le système mis en place dans un pays, celui-ci peut utiliser le cadre pour procéder à une auto-évaluation de l'état de préparation en matière de cybersécurité, aux plans national et régional. Dans ce contexte, M. Debbagh et son équipe ont analysé de près l'outil d'évaluation de la cybersécurité/CIIP mis au point par l'UIT [23]. Il a également précisé la manière dont des liens ont été crées entre cette approche et la mise en place, au Maroc, d'une capacité en matière de sécurité. Aussi, la politique nationale en la matière est-elle axée sur la mise en place d'une sécurité des systèmes d'information, la lutte contre la cybercriminalité et le renforcement de la confiance dans l'économie numérique (secteurs public et privé). M. Debbagh a fait savoir que le CERT Maroc serait lancé courant 2009.

27. Mohammed Umar Maska, Directeur de la cybersécurité du Bureau du Conseiller en matière de sécurité nationale, Direction de la cybersécurité, est intervenu sur le thème « Mise en place au Nigéria d'une capacité nationale en matière de cybersécurité : le chemin parcouru à ce jour»[24], faisant un état des lieux de la situation au Nigéria dans le domaine de la cybersécurité. Il a relevé qu'au au Nigéria les particuliers comme les entreprises ont été nombreux à être affectés par les problèmes de cybersécurité, et ce à cause du clonage de sites Web, des escroqueries au phishing ou « hameçonnage », des fraudes sur l'Internet, des fraudes par carte de crédit, des fraudes de type paiement à l'avance (« l'arnaque Nigéria 419 »), etc. C'est dans ce contexte que le Président du Nigéria a créé en 2003 une Commission chargée d'enquêter sur les activités des cybercriminels, ainsi que la Commission d'enquête sur les crimes économiques et financiers pour lutter contre la corruption, les fraudes de type paiement à l'avance et le blanchiment d'argent. Cet appui au plus haut niveau de l'État a permis la mise en place de l'Initiative nationale en matière de cybersécurité, dont les six principaux objectifs sont la sensibilisation ; la promulgation d'une nouvelle législation pour lutter contre la cybercriminalité, la mise en place d'un cadre juridique et technique pour la cybersécurité et la protection des infrastructures essentielles de l'information ; la création d'une plateforme pour la collaboration entre les parties prenantes des secteurs public et privé au plan national ; la mise en place de formations dans tous les organismes représentant la force publique ; l'instauration, au plan mondial, d'une coopération entre les organismes de police.

28. En 2004, le Gouvernement a constitué le Groupe de travail sur la cybercriminalité au Nigéria (NCWG) pour aider à atteindre les objectifs de l'Initiative nationale en matière de cybersécurité et, en 2006, la Direction de la cybersécurité, rattachée au Bureau du Conseiller national en matière de sécurité. L'une des fonctions de la Direction de la cybersécurité est la création d'un CERT ; l'équipe responsable est en train d'établir un cadre possible à cette fin. M. Maska a également fait observer que la Direction défendait actuellement la loi relative à la sécurité informatique et à la protection des infrastructures essentielles de l'information en attendant qu'elle ne soit soumise à l'Assemblée nationale. Au nombre des autres difficultés qui se posent figurent notamment l'acquisition des technologies et des outils modernes requis pour empêcher et surveiller en permanence les cybermenaces et les activités délictuelles en ligne et pour procéder aux enquêtes en la matière. La formation spécialisée pour toutes les parties prenantes nationales concernées a également été citée comme étant un volet important pour que les activités menées au titre de l'Initiative nationale en matière de cybersécurité puissent aboutir.

29. Sherif Hashem, Vice-président exécutif de l'Agence pour le développement de la technologie de l'information (ITIDA) (Égypte), dans son exposé ayant pour titre « Vers une structure égyptienne pour la cybersécurité »[25], a présenté certain des principaux éléments de la démarche égyptienne pour contrer les cybermenaces. Il a fait observer que, comptant comme elle le fait 14 millions d'utilisateurs de l'Internet, l'Égypte a de fortes raisons économiques de développer plus encore son infrastructure. Le nombre d'applications conçues et utilisées est par ailleurs en augmentation et, s'il importe de sensibiliser le public aux menaces qui existent sur l'Internet, il est tout aussi important de ne pas en décourager l'utilisation. M. Hashem a rappelé que même les systèmes non raccordés à l'Internet peuvent être compromis à l'aide de clefs USB et d'autres dispositifs. Il a mentionné l'identification numérique et la confidentialité et les raisons pour lesquelles ces questions sont importantes dans toute réflexion sur les mesures relatives à la cybersécurité, mais aussi l'importance de tenir compte de l'élément coût des différentes solutions envisagées. S'agissant des lois et

---

[23] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

[24] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf

[25] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashem-cybersecurity-framework-egypt-june-09.pdf

règlements ayant trait aux TIC, l'Égypte s'est dotée d'une loi polyvalente sur les droits de propriété intellectuelle (Loi No. 82/2002), d'une loi sur les communications (Loi No. 10/2003), d'une loi sur les signatures électroniques (Loi No. 15/2004). Sont également à l'état de projet des lois sur la protection des données, sur la confidentialité, sur la cybersécurité, sur la cybercriminalité et sur l'accès à l'information. À ce sujet, M. Hashem a recommandé que toutes les parties prenantes soient mobilisées lors de l'élaboration de nouvelles lois sur la cybersécurité et la cybercriminalité.

30. Étant donné la priorité élevée accordée à la question de la cybersécurité, l'Égypte l'a intégrée au Conseil de la sécurité nationale et, en 2007, a créé une Commission de la cybersécurité rattachée au Ministère des technologies de l'information et des communications. En avril 2009, une équipe d'intervention en cas d'urgence informatique a été créée au niveau national. Initialement chargée d'évaluer et de mesurer les taux de pénétration pour les réseaux d'infrastructures essentielles de l'information, de gérer les incidents, de constituer un portail de sensibilisation et d'alerte, l'équipe aura bientôt d'autres responsabilités, dont la coordination internationale de l'ensemble des activités, le renforcement des capacités et la formation.

Session 4 : Mesures concrètes visant à faciliter la coopération aux niveaux régional et international

31. La coopération régionale et internationale est fondamentale pour encourager les efforts en matière de cybersécurité et faciliter le dialogue et les échanges. Les problèmes posés par les cyberattaques et la cybercriminalité, qui ont une envergure universelle et sont lourds de conséquences, ne peuvent être traités que dans le cadre d'une stratégie cohérente placée sous le contrôle de la coopération internationale, compte tenu des rôles des différentes parties prenantes et des initiatives existantes. En tant que coordinatrice de la grande orientation C5 du SMSI, dont le thème est « Établir la confiance et la sécurité dans l'utilisation des TIC », l'UIT procède à des échanges de vues avec les principales parties prenantes quant à la meilleure façon de riposter de manière concertée aux problèmes de plus en plus fréquents qui pèsent sur la cybersécurité. Les participants ont passé en revue certaines des initiatives régionales pour alimenter les débats, afin de déterminer les mesures éventuelles et les actions concrètes à prendre pour promouvoir la coopération régionale et internationale en vue de renforcer la cybersécurité.

32. Ali Drissa Badiel, Conseiller principal/Chef par intérim du Bureau de zone de l'UIT pour l'Afrique centrale, a ouvert la session en faisant le point des activités menées dans la région par l'UIT dans le domaine de la cybersécurité et de la coopération régionale dans l'optique d'un cyberespace sécurisé pour tous. Il a noté que grâce au Programme mondial cybersécurité, l'UIT ouvre la voie à une coopération mondiale intensifiée pour parvenir à un cyberespace sécurisé et plus sûr. Comptant 191 Membres et plus de 700 Membres de secteurs, y compris les principaux acteurs du secteur des télécommunications, l'UIT est idéalement placée pour constituer la tribune pour la coopération internationale sur la cybersécurité. Certaines activités de l'UIT visant à renforcer la coopération régionale dans le domaine de la cybersécurité prévoient une assistance à des pays tels que le Cameroun, la Côte d'Ivoire, le Sénégal, la Zambie et le Burkina Faso pour la mise en œuvre de solutions de sécurité des réseaux s'appuyant sur les infrastructures publiques essentielles. L'organisation de forums, de séminaires et d'ateliers régionaux pour renforcer la capacité en matière de cybersécurité et pour regrouper les différentes parties prenantes régionales et nationales est un autre volet important des travaux de l'UIT. Une assistance est également octroyée à différents pays pour l'élaboration de CERT/CSIRT/CIRT nationaux.

33. Dans le cadre d'un projet conjoint entre l'Union européenne et l'UIT portant sur l'harmonisation des politiques en matière de TIC en Afrique sub-saharienne (HIPSSA), les pays de la région travaillent dans l'optique d'une harmonisation globale des règlements, des télécommunications et des TIC, grâce notamment à l'octroi d'une assistance aux pays de l'Afrique sub-saharienne pour l'intégration des directives régionales dans les législations nationales. M. Badiel a en outre souligné l'importance de la participation active de toutes les administrations aux réunions régionales préparatoires, qui se tiendront en Ouganda en juillet 2009 et en Syrie en janvier 2010. Ces réunions préparatoires constituent une excellente occasion de définir les besoins des pays au niveau régional, y compris dans le domaine de la cybersécurité.

34. Ali Yahyaoui, Responsable des TIC à la Banque africaine de développement (BAD), dans son intervention ayant pour titre « La stratégie d'opérations de la Banque africaine de développement en matière de TIC »[26], a poursuivi le débat en présentant ce que la Banque africaine de développement était en mesure de faire pour aider les pays dans le domaine de la cybersécurité et d'autres aspects du déploiement des TIC. Chef de file dans la région pour tout ce qui touche au développement des infrastructures, la BAD a pour objectif de promouvoir l'accès aux TIC grâce au renforcement des infrastructures nationales et régionales, compte tenu des grandes orientations générales et du cadre réglementaire et de favoriser la participation du secteur privé dans le cadre de partenariats, dans le but général d'appuyer les pays dans leurs applications des TIC comme instrument du développement. La BAD n'a pas mis en place de programme spécifique d'appui à la cybersécurité, mais dispose de ressources pour aider tous les pays à déployer les TIC en toute sécurité tout en mettant en place les infrastructures et en créant un environnement propice au développement des TIC.

[26] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/yahiaoui-afdb-strategy-june-09.pdf

35. M. Yahyaoui a noté que l'Afrique restait à la traîne pour ce qui est de l'accès aux TIC et de leur utilisation. S'il existe des câbles sous-marins tout autour du continent, il n'y en a quasiment aucun à l'intérieur. Il y aurait par ailleurs de nombreuses améliorations à apporter au niveau des grandes orientations et du cadre réglementaire, bien au-delà de la simple pose de câbles à fibres optiques. La cybersécurité, a précisé M. Yahyaoui, est une dimension supplémentaire de cette équation. Alors que la plupart des pays africains ont mis en place une stratégie électronique sous une forme ou l'autre, ce n'est pas vrai de la totalité d'entre eux, et pour ceux qui disposent effectivement d'une stratégie dans le secteur des TIC, la cybersécurité n'est le plus souvent hélas pas une de leurs grandes priorités. M. Yahyaoui a également noté que de nombreux pays n'ont toujours pas d'organisme de réglementation des télécommunications. Il se trouve aussi que de nombreux pays sont en guerre, et manquent de stabilité. L'aide concrète que la BAD peut apporter aux États Membres comprend le financement d'études visant à mieux comprendre les spécificités nationales. Elle peut aussi envisager de financer des études de préinvestissement détaillées dans les domaines de la mise en place d'infrastructures, de la création de centres régionaux d'excellence pour les TIC et de renforcement des capacités des TIC d'une manière plus générale, etc. M Yahyaoui a conclu son intervention en décrivant la méthodologie utilisée par la BAD pour octroyer des prêts aux pays et la manière dont la BAD travaille avec les pays pour accéder aux sources potentielles de financement.

36. Mohamed Timoulali, Conseiller régional sur les politiques en matière de TIC du Bureau pour l'Afrique du Nord de la Commission économique des Nations Unies pour l'Afrique (CEA), a fait une intervention sur le thème « Les efforts concertés de la CEA dans le domaine de la cybersécurité »[27], présentant l'action de la CEA dans ce domaine. La CEA, en collaboration avec d'autres parties prenantes, mène diverses activités dans le cadre du suivi de la grande orientation C5 du Sommet mondial sur la société de l'information, consacrée au renforcement de la confiance et de la sécurité dans l'utilisation des TIC. À cet égard, M. Timoulali a fait savoir que la CEA travaille de concert avec des pays pour mettre au point et élaborer des politiques et stratégies nationales et régionales dans le domaine des TIC et aide les pays à élaborer une législation à l'appui de ces politiques et stratégies. S'il est vrai que plusieurs pays ont mis en place des mécanismes pour renforcer la confiance et la sécurité en optant pour un processus de développement de stratégies en la matière, très rares sont ceux qui ont promulgué des lois sur la cybersécurité. M. Timoulali a noté que l'exécution de la grande orientation C5 appelle d'importantes ressources dans les pays, non seulement pour l'élaboration de stratégies nationales, mais aussi, et de plus en plus, pour l'exécution de ces stratégies. Une stratégie ne vaut en effet que par son exécution, a-t-il souligné.

37. Dans le cadre de la mise en place d'une structure juridique harmonisée, la CEA a apporté une assistance à la CEDEAO pour l'élaboration d'une structure juridique harmonisée pour les TIC ; d'autres Commissions économiques régionales ont sollicité une aide dans l'optique d'adapter cette structure. Une coopération est également en place avec l'Union africaine (UA) dans le but de créer une structure juridique harmonisée régionale pour la société du savoir, comprenant notamment des directives en matière de cybercriminalité, de protection des renseignements personnels, de transactions électroniques, de signatures électroniques et de certification et de cybersécurité d'une manière générale. En ce qui concerne la coopération dans le domaine de la cybersécurité, la CEA a aidé certains pays (le Kenya, le Mozambique, le Burkina Faso, le Ghana) à élaborer des politiques nationales relatives à la cybersécurité, et a lancé un projet de coopération sur la cybersécurité dans la région du Maghreb. M. Timoulali a précisé que la CEA souhaitait continuer de travailler avec des partenaires pour fournir une assistance technique aux organisations régionales afin de mettre en œuvre des politiques harmonisées en matière de TIC, et a demandé l'intensification de la collaboration avec l'UIT et d'autres acteurs dans le cadre d'activités spécifiques ayant trait à la cybersécurité.

38. Le premier jour du forum, l'ANSI a convié les participants à une soirée-cocktails sur les lieux de la réunion. Les délégués nationaux assistant au forum ont également été invités à visiter le CERT-TCC tunisien. Cette visite du CERT-TCC, fort appréciée, a été organisée par l'ANSI et le Directeur général du CERT-TCC, Belhassen Zouari, et son équipe.

Session 5 : Établir des bases juridiques et mettre en place des moyens d'application efficaces

39. Pour prévenir, détecter et réprimer la cybercriminalité et l'utilisation délictueuse des TIC, il faut une législation nationale adaptée, ainsi qu'une coordination juridique et des mesures exécutoires sur le plan international. À cette fin, il est nécessaire d'actualiser les dispositions, procédures et grands principes du droit pénal afin qu'ils prennent en compte les incidents en matière de cybersécurité et luttent contre la cybercriminalité. De nombreux pays ont par conséquent modifié leur code pénal ou se sont engagés à le faire, conformément aux cadres et recommandations existant sur le plan international. Les participants à la session 5 ont réfléchi à la nécessité d'établir de bonnes bases juridiques et d'adopter des mesures exécutoires efficaces, examiné certaines méthodes juridiques adoptées sur le plan national et se sont demandé dans quels domaines la coordination juridique pourrait être intensifiée entre les pays. C'est Nébila Mezghani, professeur de sciences politiques à l'Université de Tunis, qui a assuré les fonctions de modérateur de cette session, dont les participants ont souligné également la nécessité d'actualiser la législation en vigueur et, lorsque le besoin s'en

[27] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/timoulali-eca-cooperative-actions-june-09.pdf

fait sentir, adopter de nouvelles lois pour résoudre le problème croissant que pose l'utilisation malveillante des TIC.

40. Marco Gercke, Maître de conférences à l'Université de Cologne (Allemagne), a présenté la nouvelle publication de l'UIT, « Comprendre la cybercriminalité : guide à l'intention des pays en développement »[28,29]. Ce guide vise à aider les pays en développement à mieux comprendre les conséquences aux plans national et international des cybermenaces, qui se multiplient, à évaluer les besoins s'agissant des instruments nationaux, régionaux et internationaux, et à établir des bases juridiques solides. M. Gercke a également fait le point de ce qui se passe dans la communauté internationale et dans le cadre des efforts déployés par les pays pour réviser les lois existantes et adopter de nouvelles lois visant à faire de l'utilisation malveillante des TIC une infraction pénale. Il a noté que de nouveaux délits et de nouvelles difficultés apparaissent en permanence dans le contexte de l'Internet ; de ce fait, la législation nationale doit être constamment révisée et mise à jour. Les pays et parties prenantes concernés doivent d'abord scruter de près les technologies en jeu et les mauvais usages qu'on en fait, puis protéger les utilisateurs en adoptant de nouvelles lois, en étant bien conscients qu'il existe toujours un laps de temps entre le moment où un crime est identifié et celui où la législation suit. Alors que bien des problèmes liés à l'Internet appellent des solutions d'ordre juridique, il en est d'autres qui n'appellent pas ce genre de solution. Les pays doivent donc veiller à ne pas conférer un caractère d'infraction pénale à des activités sur l'Internet qui ne l'auraient pas en dehors de l'Internet. M. Gercke a précisé que l'existence de bases juridiques permet de procéder à des enquêtes, d'engager des poursuites et de prévenir la cybercriminalité, de promouvoir la cybersécurité mais aussi de favoriser le commerce.

41. Faisant le point de la législation qui existe aux niveaux national, régional et international sur la cybercriminalité, M. Gercke a souligné l'importance et la nécessité d'harmoniser plus encore la législation. Il a noté l'existence d'un certain nombre d'initiatives internationales sur la cybersécurité et la lutte contre la cybercriminalité ; toutes ces initiatives, chacune différente, ont leur rôle à jouer. Il a en outre noté que la recherche de solutions idoines pour répondre à la menace que constitue la cybercriminalité représente un véritable défi pour les pays en développement. L'élaboration et la mise en œuvre d'une stratégie nationale en matière de cybersécurité, comprenant la lutte contre la cybercriminalité, prennent du temps et peuvent s'avérer très coûteuses, ce qui peut éventuellement empêcher des pays de prendre des mesures qui s'imposent. Il est toutefois de plus en plus important pour chaque pays de se doter de la capacité et des compétences requises pour réviser leur législation, enquêter en cas d'abus ou d'utilisation malveillante des réseaux et veiller à ce que les criminels qui s'en prennent aux réseaux et les exploitent soient sanctionnés. L'adoption par tous les pays d'une législation appropriée contre l'utilisation malveillante des TIC à des fins criminelles et autres, y compris les activités visant l'intégrité des infrastructures nationales essentielles de l'information est impérative si l'on veut garantir la cybersécurité au plan mondial. La raison d'être des ressources spécialisées de l'UIT dans le domaine de la législation sur la cybercriminalité [30], du guide sur comment mieux comprendre la cybercriminalité et du kit de l'UIT pour la législation en matière de cybersécurité est d'aider les pays à comprendre les aspects juridiques de la cybersécurité et d'harmoniser les structures juridiques dans le but de lutter contre la cybercriminalité et de faciliter la coopération internationale.

42. Mwende Njiraini, Ingénieur en nouvelles technologies, Commission des communications du Kenya (Kenya) a pris la suite avec une intervention consacrée à« L'élaboration de bases juridiques et la prise de mesures d'exécution efficaces : étude de cas sur le Kenya »[31], en expliquant comment le Kenya s'y prend pour mettre en place les bases juridiques et les mécanismes correspondants pour appliquer les dispositions de la loi de 2009 sur les communications. Mme Njiraini a situé la révision de la loi dans son contexte, précisant les défis que représentent les TIC dans le contexte du développement national et les objectifs spécifiques visés par le Kenya avec cette loi. Mme Njiraini a relevé en outre qu'avec l'amélioration de la connectivité internationale que le Kenya va connaître grâce à la pose de nouveaux câbles sous-marins à la fin de juin 2009, le pays accorde une importante plus grande encore à la cybersécurité. La loi ainsi révisée va élargir le mandat de la Commission des communications, qui portera désormais également sur la réglementation de la télédiffusion et les transactions électroniques et qui accordera une reconnaissance officielle aux ressources Internet et à la cybercriminalité. La façon d'aborder ces questions varie d'un pays à l'autre, et Mme Njiraini a noté que, au Kenya, ces responsabilités relevaient désormais de la Commission des communications.

43. Spécifiquement dans le domaine de la cybersécurité, la loi charge la Commission de promouvoir la confiance du public ainsi que l'élaboration d'un cadre national solide pour la cybersécurité. La loi ne donne pas de définition de la cybercriminalité, mais énumère un certain nombre de thèmes qui y sont liés, dont, entre autres, l'accès non autorisé aux données informatiques ; l'accès non autorisé aux services informatiques et

---

[28] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/gercke-undertstanding-cybercrime-june-09.pdf

[29] La publication de l'UIT, Comprendre la cybercriminalité: Guide à l'intention des pays en développement, est sortie en mai 2009 dans le cadre des ressources spécialisées de l'UIT sur la législation en matière de cybercriminalité. Le guide peut être téléchargé gratuitement sur le site suivant: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

[30] On produira un complément d'information sur les ressources de l'UIT dans ce domaine en ligne: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[31] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/njiraini-kenya-legal-foundation-june-09.pdf

l'interception; la modification non autorisée de contenus informatiques. Mme Njiraini a également relevé que deux secteurs importants ne sont pas couverts par la loi : la coopération internationale dans le domaine de la lutte contre la cybercriminalité, pour laquelle une loi d'assistance juridique mutuelle devrait être promulguée dans les mois à venir, et les procédures visant à diligenter les enquêtes et les poursuites en cas de cybercriminalité. Elle a également mentionné des mesures concrètes que le pays s'est engagé à prendre pour donner effet à la loi. Elle a notamment évoqué les activités menées par le groupe de travail sur la cybersécurité de l'EARPTO (East Africa Regulatory, Post and Telecommunications Organization – Organisation de l'Afrique de l'Est pour la réglementation des postes et des télécommunications), prévoyant notamment un plan pour la création de CERT nationaux dans les pays concernés (Kenya, Ouganda, Tanzanie, Burundi et Rwanda), ainsi qu'un éventuel CERT régional d'ici 2011.

44. David Weitzel, Ingénieur principal en sécurité et confidentialité de l'information, MITRE (États-Unis d'Amérique) et Vice-président de la Commission sur la confidentialité et la cybercriminalité de l'American Bar Association (ABA), a fait un exposé sur le « Kit de l'UIT pour la législation en matière de cybercriminalité »[32,33]. Le kit a pour objet de mettre à la disposition des pays un langage législatif modèle et des documents de référence à même de les aider à élaborer des lois et des règles de procédure harmonisées en matière de cybercriminalité. Le kit est un instrument pratique que les pays peuvent utiliser pour mettre en place un cadre juridique pour la cybersécurité et les lois correspondantes. Le langage modèle a été établi après analyse des cadres juridiques régionaux et internationaux les plus pertinents. Le langage est conforme à ces lois et censé servir de guide pour les pays souhaitant élaborer, rédiger ou modifier leurs propres lois sur la cybercriminalité. M. Weitzel a noté que le kit vise à favoriser l'harmonisation mondiale des lois relatives à la cybercriminalité en constituant une ressource centrale pour aider les législateurs, les avocats, les fonctionnaires, les spécialistes de l'élaboration de grandes orientations et les représentants du secteur à faire progresser leur pays vers un cadre juridique cohérent les protégeant contre l'utilisation délictueuse des TIC.

45. Le langage modèle utilisé dans le kit peut être adapté aux lois de tel ou tel pays. Les pays qui calquent leurs lois relatives à la cybercriminalité sur le langage modèle utilisé dans le kit aideront à faire progresser un cadre mondial harmonisé, à faciliter la coopération internationale, à résoudre les questions de compétence et de preuve, et à prévenir l'action des cybercriminels. Outre le langage modèle, le kit comporte trois sections d'information servant d'aide concrète pour l'élaboration d'une législation relative à la cybercriminalité : a) des explications concernant certaines dispositions ou certains aspects du langage modèle ; b) une matrice de lois sur la cybercriminalité comparant les dispositions des lois de différents pays ; et c) une liste de documents de référence utiles énumérant divers ouvrages, lois, livres et articles consacrés aux lois et questions relatives à la cybercriminalité. M. Weitzel a noté que l'UIT est toujours contente de recevoir des observations sur ces ressources portant sur la législation en matière de cybercriminalité, qui permettent à l'UIT de veiller à l'utilité des documents qu'elle publie pour les États membres de l'UIT déployant d'importants efforts en faveur de la cybersécurité au plan national.

Session 6 : Réfléchir aux solutions techniques relatives à la résilience des réseaux d'information et de communication

46. L'expansion et l'évolution des télécommunications ouvrent de nouvelles perspectives mais, dans le même temps, sont source de nouveaux problèmes. La convergence et le passage aux réseaux fondés sur le protocole Internet (IP) ou aux réseaux de prochaine génération (NGN) imposent de redéfinir les stratégies sectorielles et commerciales. De nouveaux services et de nouvelles applications, comme le protocole voix sur Internet (VoIP), remettent en question les modèles économiques et les cadres réglementaires. Face à cette transition, les pouvoirs publics, les organismes de réglementation, les opérateurs et les équipementiers s'efforcent d'anticiper et de s'adapter aux enjeux de demain. Cette session-ci avait pour objet d'aider les pays à mieux comprendre comment atténuer l'impact des menaces sur la sécurité et faire en sorte que les communications utilisant les réseaux publics de télécommunication restent fiables, sûrs, interopérables et faciles à utiliser. La session 6, animée par Ali Drissa Badiel, conseiller principal/chef par intérim du Bureau de zone de l'UIT pour l'Afrique centrale, a dressé un portrait des menaces qui pèsent sur les réseaux et envisagé les mesures et normes techniques à prendre pour rendre les réseaux plus résilients.

47. M. Drissa a ouvert la session en présentant certaines des activités menées dans la région au cours des années écoulées et des initiatives auxquelles l'UIT a pris part ou qu'elle a soutenues à divers titres. Parallèlement aux nouveaux débouchés crées par le développement des télécommunications et des TIC, surgissent de nouveaux problèmes, dont l'obligation de redéfinir les stratégies industrielles et les modèles de gestion, l'impact de la convergence de technologies, faisant une plus grande place aux fournisseurs d'informations (IP), la croissance du VoIP et, plus encore, la migration de réseaux dans le monde entier vers les réseaux fournisseurs d'information de prochaine génération. Cette évolution oblige les États, les organismes de réglementation, les opérateurs et les fabricants à se préparer aux enjeux à venir. C'est dans ce contexte qu'ont été organisés un forum sur la

---

[32] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/weitzel-cybercrime-legislation-toolkit-june-09.pdf

[33] Le kit de l'UIT pour la législation en matière de cybercriminalité est sorti en mai 2009 dans le cadre des ressources spécialisées de l'UIT sur la législation en matière de cybercriminalité. Le kit peut être téléchargé gratuitement à l'adresse suivante: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

réglementation des télécommunications consacré aux réseaux IP et aux enjeux pour les organismes de réglementation en Afrique (Cameroun, 2006), un forum de développement régional sur le thème « Combler l'écart de normalisation des TIC dans les pays en développement », avec des sessions sur les réseaux de nouvelle génération (Ghana, 2008) et un forum de développement régional sur le thème « Réseaux de nouvelle génération et réseaux à haut débit : débouchés et enjeux » (Zambie, mai 2009).

48. Patrick Mwesigwa, Directeur des technologies et des licences de la Commission de l'Ouganda pour les communications et Vice-président du groupe d'étude 17 de l'UIT-T consacré à la sécurité, a fait une intervention intitulée « Le point des travaux du groupe d'étude 17 de l'UIT-T »[34] et a présenté certaines des activités menées en Ouganda dans le domaine de la cybersécurité dans son intervention ayant pour titre « Les initiatives juridiques et générales en matière de cybersécurité – La situation en Ouganda »[35]. Le secteur de la normalisation de l'UIT (UIT-T) s'efforce de rapprocher le secteur privé et les États pour coordonner les travaux menés et promouvoir l'harmonisation de normes en matière de politique sécuritaire et de sécurité à l'échelle internationale. Les organismes d'élaboration de normes jouent un rôle irremplaçable s'agissant de relever dans le protocole les points vulnérables face à la sécurité, a-t-il dit. Outre les nombreuses recommandations importantes en matière de sécurité, l'UIT a fait le point des besoins en matière de sécurité, des directives relatives à la sécurité pour les auteurs de protocole, des spécifications en matière de sécurité pour les systèmes fondés sur les fournisseurs d'information, des directives sur les moyens de repérer les cybermenaces et de prendre les mesures pour atténuer les risques. M. Mwesigwa a mentionné certaines des résolutions pertinentes orientant les travaux de l'UIT-T en matière de sécurité ainsi que certaines des initiatives en cours, telle la feuille de route pour les normes en matière de sécurité régissant les TIC[36] visant à promouvoir une collaboration plus étroite entre les organismes internationaux d'élaboration des normes. La feuille de route encourage le renforcement des normes en matière de sécurité en soulignant les normes existantes, les travaux en cours et les normes à venir au sein des grandes organisations. En faisant le point des initiatives prises par le groupe d'étude 17 de l'UIT-T, M. Mwesigwa a fait valoir la nécessité d'une collaboration étroite avec d'autres pays de la région et a encouragé les pays en développement à participer aux activités menées par ce groupe d'étude.

49. Décrivant certaines des activités en cours en Ouganda, M. Mwesigwa a fait part des progrès réalisés dans le domaine de la législation ayant trait à la cybersécurité. Depuis 2003, le groupe de travail national, dont le chef de file est la Commission ougandaise pour la réforme législative, travaille à l'élaboration d'une loi sur la cybersécurité. Le groupe d'étude national compte des représentants de différentes parties prenantes, dont les ministères ougandais de la justice ; du commerce et de l'industrie ; de l'eau, de l'aménagement du territoire et de l'environnement ; des finances ; des travaux publics, du logement et des communications ; des TIC, ainsi que de la Commission ougandaise pour les communications, la Société juridique d'Ouganda, le Bureau national des normes, la Banque d'Ouganda, l'Autorité ougandaise pour les investissements ; l'Université Makerere ; la Commission ougandaise des assurances, etc. Il existe trois instruments principaux en Ouganda : la loi sur les transactions électroniques (2003), la loi sur les usages délictueux de l'informatique (2003) et la loi sur les signatures électroniques (2003). Ces lois ont déjà été approuvées par le gouvernement et sont actuellement à l'étude par le parlement, qui devrait les approuver d'ici la fin de 2009.

50. M. Mwesigwa a également donné des précisions sur les travaux menés dans les pays de la région de l'Afrique de l'Est (Burundi, Kenya, Rwanda, Tanzanie et Ouganda) pour harmoniser les lois et la législation sur les questions informatiques. Les lois en vigueur dans les pays d'Afrique de l'Est vont être harmonisées en deux temps : la première phase étant axée sur la législation en matière de transactions électroniques, de signatures électroniques et d'authentification, de protection et de confidentialité des données, de protection des consommateurs et de cybercriminalité et la deuxième phase portant sur les droits de propriété intellectuelle, les noms de domaine, la fiscalité et l'accès à l'information. Dans le cadre des efforts ainsi déployés, des réunions régionales ont été organisées ; les États partenaires devraient promulguer de nouvelles lois sur les TIC d'ici 2010. M. Mwesigwa a conclu son intervention en soulignant la nécessité de sensibiliser les décideurs, les opérateurs de réseaux et les particuliers aux questions ayant trait à la cybersécurité ; il a encouragé tous les pays à mettre en place des structures juridiques solides pour lutter contre les menaces pesant sur la cybersécurité. Il a également relevé qu'étant donné le caractère transnational du cyberespace, la coopération internationale est impérative pour garantir la sécurité des activités en ligne.

51. Garry Mukelabai, Directeur des systèmes d'information de l'Autorité chargée des communications de Zambie (Zambie) est intervenu sur le thème « Les efforts déployés par la Zambie en matière de cybersécurité »[37]. À l'issue du Forum régional UIT sur la cybersécurité pour l'Afrique de l'Est et l'Afrique australe tenu à Lusaka (Zambie), en août 2008[38], un groupe de travail sur la cybersécurité avait été créé. Ce groupe de travail , qui

---

[34] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mwesigwa-itu-sg-17-overview-june-09.pdf

[35] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mwesigwa-uganda-case-study-june-09.pdf

[36] http://www.itu.int/ITU-T/studygroups/com17/ict/index.html

[37] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/mukelabai-cybersecurity-efforts-zambia-june-09.pdf

[38] Voir le site web pour le Forum régional UIT sur la cybersécurité pour les pays d'Afrique de l'Est et d'Afrique australe tenu à Lusaka (Zambie) (25-28 août 2008) à l'adresse suivante: www.itu.int/ITU-D/cyb/events/2008/lusaka/

jouit du plein appui du gouvernement, compte 14 membres issus de diverses organisations et dotés de compétences dans des domaines divers, le tout sous les auspices de l'organisme chargé de la réglementation des télécommunications, à savoir l'Autorité chargée des communications (CAZ). M. Mukelabai est actuellement Président du groupe de travail national sur la cybersécurité. Des ateliers de renforcement des capacités et des séances de formation sont actuellement prévus pour tous les membres du groupe de travail. Le programme de sensibilisation déjà mené prévoyait un atelier sur le paiement électronique organisé conjointement avec la Société informatique de Zambie, un atelier sur l'audit des systèmes d'information organisé par KPMG auquel les membres du groupe de travail ont été invités, un atelier sur la cybersécurité organisé conjointement avec le forum d'intelligence électronique et la célébration de la journée mondiale des télécommunications et de la société de l'information consacrée à la protection de l'enfance en ligne, le 18 mai 2009 [39], de concert avec l'Autorité chargée des télécommunications, sans parler de diverses émissions de radio et de télévision et de tribunes libres.

52. S'agissant du renforcement des capacités nationales de gestion des incidents, la Zambie est en train de créer une équipe nationale d'intervention en cas d'urgence informatique (CERT), ainsi que d'un système de compte rendu de secteurs spécifiques au CERT national. Ce CERT national vise à mettre en place une organisation centrale jouissant de la plus grande confiance et à même de coordonner l'intervention nationale en cas d'incident de cybersécurité. Le CERT devrait être équipé de manière à pouvoir prendre des mesures proactives visant à réduire les risques, fournir des services de veille, d'alerte et d'intervention en cas d'incident, ainsi que des ressources permettant d'analyser les incidents, de procéder à des enquêtes et d'y riposter de manière efficace. Par ailleurs, trois lois différentes sont actuellement examinées par la Commission de révision parlementaire. La loi sur les TIC met en place un nouveau régime d'homologation neutre du point de vue technologique, annule la loi sur les télécommunications et renforce la loi sur les radiocommunications. La loi sur les communications et les transactions électroniques, s'appuyant sur la loi type de la CNUDCI annule et améliore la loi sur les usages délictueux de l'informatique (2004), introduit et réglemente les prestataires de services de cryptographie et d'authentification et met en place un environnement favorable pour le commerce électronique, la santé électronique, la banque électronique, le gouvernement électronique et d'autres applications électroniques, et charge le CAZ d'administrer le .zm ccTLD. Par ailleurs, la loi sur les services postaux réglemente le service postal, favorise la concurrence dans les services postaux et les services non réservés et autorise la création d'une banque postale. À mesure que le recours aux ordinateurs et à l'internet progresse, les cyberincidents vont eux aussi se multiplier. À ce sujet, M. Mukelabai a noté que les pays et les nations ont une plus grande chance d'atténuer les effets correspondants s'ils forgent une alliance concertée inspirant totalement confiance.

Session 7 : Définir des structures administratives solides et mettre en place des capacités de gestion des incidents

53. La solution aux problèmes de cybersécurité passe par la mise en place de capacités de veille, d'alerte et de réaction en cas de cyberincident afin de prévoir, de détecter et de gérer ce type d'incident, et d'y remédier. Une gestion efficace de ces incidents nécessite une réflexion sur de multiples éléments: financement, ressources humaines, formation, capacités technologiques, collaboration entre secteur public et secteur privé et impératifs juridiques. Une collaboration à tous les niveaux de l'État ainsi qu'avec le secteur privé, les universitaires et les organisations régionales et internationales est nécessaire pour sensibiliser le public aux attaques potentielles et aux mesures à prendre pour y remédier. Les participants à cette session ont examiné les meilleures pratiques, les structures administratives et les normes connexes en ce qui concerne les aspects techniques, administratifs et financiers de la création d'équipes nationales, régionales et internationales ayant des responsabilités en matière de veille, d'alerte et d'intervention en cas d'incident. Le modérateur était Nabil Sahli, enseignant (Tunisie).

54. Haythem El Mir, Directeur technique de l'Agence nationale de la sécurité informatique et représentant du CERT-TCC de Tunisie, a fait un exposé sur le « Renforcement des capacités nationales de CSIRT – Étude de cas sur la Tunisie[40]. Dans son exposé, M. El Mir a donné des renseignements sur l'expérience tunisienne de la création du CERT national en privilégiant certains aspects concrets et techniques. Il a fait observer que l'ensemble des services de gestion des incidents sont fournis gratuitement, à titre de service public, aux différentes parties prenantes (organismes publics, utilisateurs des secteurs public et privé, particuliers, professionnels, banques, etc.). Le CERT-TCC veille à assurer une approche nationale coordonnée en prévoyant la coordination centralisée des questions relatives à la sécurité informatique (point de contact jouissant d'une grande confiance), une unité centralisée et spécialisée pour l'intervention en cas d'incident, la sensibilisation de la toutes les catégories d'utilisateurs, la veille technologique et sécuritaire, la surveillance du cyberespace et l'expertise requise pour l'appui et l'assistance afin de permettre une récupération rapide en cas d'incident de sécurité. M. El Mir a fait savoir que lors de la création du CERT tunisien, sa principale activité était la sensibilisation aux questions de sécurité, et le CERT continue à voir dans les activités de sensibilisation l'une de ses responsabilités les plus importantes. En sa qualité de représentant de la seule équipe d'intervention en cas

[39] http://www.itu.int/wtisd/index.html

[40] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/elmir-ansi-csirt-june-09.pdf

d'urgence informatique (CERT) (membre du réseau FIRST sur le continent africain) - le CERT-TCC tunisien - M. El Mir a incité les pays d'Afrique et les États arabes à créer des centres nationaux pour coordonner les activités de veille, d'alerte et d'intervention en cas d'incident.

55. M. El Mir a dit qu'il continuait de constater une absence générale de prise de conscience et de compréhension de la cybersécurité dans la région. Certains des problèmes auxquels la Tunisie a été confrontée concernent ce manque de prise de conscience, et aussi le manque d'experts locaux dans le domaine de la sécurité et la pénurie de moyens financiers. À cet égard, le CERT-TCC a créé un lien entre la cybersécurité et certains des grands projets et manifestations menés dans le pays et aide d'autres pays de la région et au-delà à renforcer des capacités spécifiques, à mener des activités de sensibilisation et des initiatives de formation. Il s'agit notamment de l'assistance fournie et des données d'expérience partagées avec le Rwanda (2007, partage de données d'expérience), avec le Sénégal (2008, formation), avec l'Afrique du Sud (2009, ECS-CSIRT), de l'adhésion aux centres d'excellence de la CNUCED (2008, partage de l'information), de la création de l'OIC-CERT, CERT-AFRICA, etc. M. El Mir a conclu son exposé en partageant un certain nombre d'enseignements concrets retenus dans le cadre de l'expérience acquise par la Tunisie. Parmi ceux-ci : la nécessité de définir une stratégie s'accompagnant d'objectifs clairs, de veiller à ce que le pays bénéficie de l'autorité de la loi et d'un appui au plus haut niveau, de veiller à la meilleure utilisation possible de ressources limitées (adoption d'une approche à faible coût grâce au recours aux solutions à source ouverte), d'attribuer aux activités de sensibilisation une priorité élevée, d'améliorer la formation et l'enseignement, de compter le plus possible sur les capacités locales, d'assurer une collaboration avec les partenaires nationaux (mobilisant tous les secteurs et créant des partenariats public-privé), et de fournir un appui technique gratuit afin de renforcer les capacités de gestion des incidents des différentes parties prenantes.

56. Mohamed Shihab, Conseiller technique, IMPACT et Anuj Singh, Directeur du Global Response Center (GRC), IMAPCT, ont continué avec un exposé sur le thème « The Global Response Center (GRC) » et traitant également de l'aide au renforcement des capacités nationales en matière de veille, d'alerte et d'intervention en cas d'incident. Ils ont donné des renseignements sur certaines des nouvelles possibilités qu'offre la collaboration entre l'UIT et IMPACT grâce aux ressources du GRC et au renforcement des capacités et de la formation correspondantes. L'UIT et IMPACT ont signé un mémorandum d'entente en vertu duquel le siège mondial d'IMPACT, situé à Cyberjaya (Malaisie) dans un immeuble de haute technicité, accueillera le Programme mondial cybersécurité de l'UIT. L'un des premiers services qui sera partagé avec les États membres est le Global Response Center (GRC) (Centre mondial d'intervention) conçu pour être le tout premier centre de ressources contre les cybermenaces. Travaillant de concert avec des partenaires de haut niveau, y compris le milieu universitaire et les pouvoirs publics, le GRC fournit à la communauté mondiale un système d'alerte précoce en temps réel. Ce système d'alerte précoce en réseau (NEWS) peut aider les États membres à identifier rapidement les cybermenaces et fournir des consignes essentielles sur les mesures à prendre pour atténuer ces menaces. Grâce au GRC les membres peuvent accéder à des outils et systèmes spécialisés, y compris un système qui vient d'être élaboré : Electronically Secure Collaborative Application Platform for Experts (ESCAPE) – Plateforme d'application en collaboration sécurisée à l'intention des experts.

57. ESCAPE est un outil électronique qui permet aux cyberexperts autorisés dans les différents pays de regrouper leurs ressources et de collaborer à distance dans un environnement sécurisé auquel ils peuvent faire confiance. En mobilisant très rapidement les ressources et l'expertise de nombreux pays, le système ESCAPE permet à un pays particulier et à la communauté mondiale d'intervenir immédiatement face à une cybermenace, notamment dans une situation de crise. Outre ce que le GRC a à offrir, IMPACT propose des bourses aux États membres en développement pouvant y prétendre leur donnant accès à des formations dispensées par l'institut SANS. Cette formation vise à constituer une réserve de ressources dans le cadre duquel on peut ensuite partager les connaissances acquises avec d'autres pour renforcer les capacités et l'expertise nationales dans le domaine de la cybersécurité. Anuj Singh a poursuivi en faisant le point des activités opérationnelles requises pour créer un centre national fonctionnel d'intervention en cas d'incident informatique (CIRT). Il a expliqué brièvement l'importance de ces CIRT nationaux, les différents types de CIRT et les avantages qu'il y a à créer un CIRT national. Étant donné la situation mondiale en ce qui concerne les menaces, la création de CIRT nationaux est impérative ; un effort concerté s'impose pour aider les pays qui n'en ont pas encore à un créer un, a dit M. Singh.

58. Pour susciter un dialogue créatif entre les pays qui donnerait une impulsion à la création de CIRT, IMPACT a examiné plusieurs modèles de CIRT s'étant avérés un succès et a recensé les quelques éléments fondamentaux indispensables. S'appuyant sur cette recherche, un ensemble fondamental d'activités requises est proposée : la planification initiale de la structure du CIRT, les séries de solutions techniques ; la planification des effectifs et le renforcement des capacités ; et la mise en place d'un cycle permanent d'amélioration. M. Singh a fait valoir que la collaboration IMPACT-UIT visait à éviter aux pays de faire les mêmes erreurs que certains ont fait dans la passé ; à ce titre, quatre principaux éléments ont été recensés pour la création d'un CIRT national : 1) une solution technique, 2) une structure organisationnelle et la planification des effectifs, 3) les politiques et procédures et 4) la formation du personnel du CIRT. La solution CIRT sera instaurée au sein du GRC et compte un portail public, un portail de gestion des incidents, des conseils, des solutions de type liste de diffusion pour les différentes parties prenantes, pour ne citer que quelques-uns de ces éléments. Il importe de noter que l'ensemble des solutions est ensuite intégré au GRC. Pour la mise en route de ces services IMPACT-UIT, la phase 1 porte sur la mise en place d'une infrastructure, l'intégration des alimentations et l'apprentissage de la

gestion des incidents. Quant aux phases 2 et 3, il s'agit d'aider les pays à mettre en place un CIRT pleinement opérationnel. Les participants ont été incités à contacter l'UIT et IMPACT à l'adresse électronique suivante : cybmail@itu.int, pour tout complément d'information.

Session 8 : Promouvoir une culture de la cybersécurité dans le cadre de partenariats novateurs

59. Au vu de la réalité du cyberespace, il est évident que nous devons tous collaborer. Pour trouver une parade efficace aux cybermenaces, il faut pouvoir disposer de ressources, de compétences techniques et d'investissements solides visant à développer les capacités - tous efforts qui ne peuvent être entrepris par une entité à elle seule. L'élément clé consiste à réunir les secteurs public et privé dans le cadre de forums et d'activités communes afin de faire face aux problèmes de cybersécurité et de mettre au point de solides programmes de renforcement des capacités. Tous les internautes devraient participer à ces efforts, qu'il s'agisse de particuliers ou d'entreprises, de représentants de la force publique ou encore de fournisseurs d'infrastructures essentielles. La clé de la réussite d'un partenariat est la confiance, qui est nécessaire pour établir, développer et entretenir des relations de partage entre les différentes parties. Les participants à cette session ont examiné de près les avantages et les problèmes liés à la création de partenariats durables et innovants visant à améliorer la cybersécurité et se sont demandé comment les efforts conjoints permettent de progresser concrètement.

60. Mohamed Shihab, Conseiller technique, IMPACT, voulant montrer comment les partenariats novateurs peuvent fonctionner concrètement lorsque les partenaires y apportent leurs compétences fondamentales, a procédé à une « vue d'ensemble d'IMPACT – Partenariat international multilatéral contre les cybermenaces »[41]. M. Shihab a noté que l'exposé précédent avait présenté une série de produits et de services offerts par IMPACT alors que cet exposé-ci fait le point de ce qu'est IMPACT et de la manière dont l'organisme s'efforce d'aider les pays du monde entier à mettre en place une capacité en matière de cybersécurité. Lancée en mars 2009, IMPACT est une tribune internationale ouverte aux États, aux entreprises et aux universitaires pour collaborer dans le domaine de la cybersécurité. Il s'agit d'une organisation à but non lucratif, de portée internationale et multilatérale. C'est aussi un partenariat public-privé, le secteur privé et le milieu universitaire s'associant pour aider les pays membres à sécuriser leurs infrastructures informatiques. Les pays souhaitant s'inscrire et profiter des services proposés dans le cadre du partenariat IMPACT-UIT devraient contacter le Bureau de développement des télécommunications de l'UIT à l'adresse électronique suivante : cybmail@itu.int, précisant le domaine et les services spécifiques auquel ils s'intéressent.

61. Angus Goldfinch, Consultant en sécurité publique et en sécurité nationale, Intercai Mondiale, dans son exposé intitulé « Partnerships for Consumer Online Safety for the Internet (COSI)» (Partenariats pour la sécurité des consommateurs sur l'Internet) »[42] a poursuivi un faisant le point de ce qu'est un modèle de partenariat réussi pour améliorer la sécurité des utilisateurs sur l'Internet. La réussite d'un partenariat se fonde sur la confiance, indispensable pour établir, développer et entretenir des relations équitables entre les différentes parties. M. Goldfinch Il a souligné la nécessité de profiter des acquis des partenariats existants pour ne pas avoir à recommencer à zéro à chaque fois. À titre d'exemple, il a cité le COSI, dans le cadre duquel les parties prenantes des secteurs public et privé doivent répondre aux diverses menaces qui se posent aux consommateurs comprenant, sans s'y limiter, les suivantes : le contenu et la protection de l'enfance ; les messages commerciaux non sollicités (pourriels) ; les escroqueries (le phishing, ou « hameçonnage » et le détournement de domaine) ; le téléchargement illégal de musique et de films, etc. Il a fait valoir que le partenariat se devait d'avoir une finalité, un modèle opératoire et un trajet clairement définis. Il faut en effet définir clairement les buts de l'association, ses obligations en vertu de la loi et des règlements ainsi que les obligations implicites en vertu d'éventuelles licences lors de l'élaboration de principes et de règlements exécutifs spécifiques, le modèle de référence, le code des pratiques et le cadre général régissant son fonctionnement. Le partenariat va ensuite pouvoir obtenir les résultats correspondant à ces objectifs. M. Goldfinch a précisé les modalités permettant de promouvoir les activités menées en partenariat, à l'échelle nationale et internationale, s'associant éventuellement à des activités et organisations existantes.

62. Le dernier exposé, celui de Naoufel Frikha, Ingénieur, Agence nationale pour la sécurité informatique (ANSI) (Tunisie), était consacré à « L'expérience tunisienne en matière de sensibilisation dans le domaine de la cybersécurité »[43]. M. Frikha a constaté que les parties prenantes et les utilisateurs connaissent mal les risques auxquels les gens sont exposés sur l'Internet. Sur le plan de la cybersécurité, les risques sont à la fois culturels et techniques et, dans ce contexte, se pose la question de savoir comment les pays doivent sensibiliser leur public ? S'agissant des menaces pesant sur la cybersécurité, les pays ne sont pas confrontés à un problème purement technique : se pose en effet également un problème humain et c'est l'individu qui est le maillon faible de cette équation. Tout d'abord, a dit M. Frikha, le pays doit définir l'acteur, c'est-à-dire l'organisme responsable de la gestion des programmes et initiatives. Il faut ensuite identifier les destinataires de la communication et déterminer le contenu du message. Il importe de choisir le nom utilisé et d'engager une réflexion sur la manière dont le message sera perçu, par exemple, s'il est question de pédophilie dans les pays

---

[41] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/impact-overview-june-09.pdf

[42] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/goldfinch-partnerships-consumer-safety-june-09.pdf

[43] http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/frikha-ansi-awareness-june-09.pdf

arabes et musulmans. Enfin, il faut choisir et élaborer l'approche et les moyens de transmettre ce message aux destinataires. Ce faisant, l'agence responsable de la campagne doit s'assurer que les organismes partenaires, les collaborateurs du secteur privé et les spécialistes de la question sont mobilisés aux différents stades. Si les initiatives de sensibilisation à la cybersécurité visent d'une manière générale à promouvoir une culture de la cybersécurité, il est manifeste qu'il faut également prévoir des moyens de sensibilisation spécifiques et ciblés.

63. M. Frikha a conclu en faisant le point d'un certain nombre de moyens de sensibilisation à la cybersécurité mis au point par l'ANSI et les partenaires tunisiens visant certains groupes cibles distincts. Parmi ces initiatives figure la mise en place d'un personnel spécialisé chargé d'élaborer des documents visant spécifiquement les journalistes, la radio et la télévision, prévoyant des dessins animés pour les enfants, un CD-rom pour les parents, la création et la diffusion d'affiches de sensibilisation aux questions informatiques, pour ne citer que quelques exemples. M. Frikha a également donné des précisions sur des manifestations organisées par les CERT-TCC destinées au monde des affaires dans le but de promouvoir une culture de la cybersécurité. Ce sont là des exemples intéressants de moyens que les pays de différentes régions du monde peuvent élaborer pour engager un dialogue avec les utilisateurs et les différents groupes cibles de manière innovante.

Session 9 : Synthèse du Forum, recommandations et solutions

64. La dernière session du forum a été animée par Belhassen Zouari, Directeur général de l'Agence nationale pour la sécurité informatique de Tunisie, Miloud Ameziane, Chef du Bureau régional de l'UIT pour les États arabes et Marco Obiso, Conseiller, Division des applications TIC et de la cybersécurité, Bureau de développement des télécommunications (BDT). Ensemble, ils ont rendu compte des principales conclusions du forum, et proposé une série de recommandations pour l'avenir afin d'améliorer la cybersécurité et la protection des infrastructures essentielles de l'information en Afrique et dans les États arabes.

65. Le Forum régional sur la cybersécurité avait pour objet de constituer une tribune ouverte pour les parties prenantes intéressées dans des États arabes et sur le continent africain, mais aussi un suivi des activités lancées à l'occasion du Forum régional IUT sur la cybersécurité pour les pays d'Afrique de l'Est et d'Afrique australe tenu à Lusaka (Zambie) (25-28 août 2008)[44] , auxquelles les pays s'étaient engagés, ainsi que l'atelier régional UIT correspondant sur les cadres pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP) pour les États arabes tenu à Doha (Qatar) (18-21 février 2008) [45]. Lors de ces deux manifestations il avait été demandé aux pays de la région d'élaborer une stratégie nationale en matière de cybersécurité, de procéder à un examen et à une révision éventuelle de la législation en vigueur dans ce domaine, de rédiger une nouvelle législation tendant à faire de l'utilisation abusive des TIC une infraction pénale, compte tenu de l'évolution rapide des menaces contre la cybersécurité, ainsi que de mettre au point une capacité nationale de gestion des incidents ou des équipes d'intervention en cas d'incident informatique (CIRT), et de s'inspirer de CIRT, de CSIRT et de CERT nationaux existants pour ce faire.

66. Au Forum régional UIT 2009 sur la cybersécurité pour l'Afrique et les pays arabes, les représentants de pays ont axé leurs débats et leur réflexion sur les prochaines mesures concrètes à prendre, articulées autour de ces trois grandes questions. Ils ont recensé les besoins s'agissant du renforcement des capacités spécifiques en matière de cybersécurité et des besoins dans le domaine de la formation pour l'ensemble des pays de la région et les moyens de répondre à ces besoins. Les mécanismes permettant de financer ces activités ont eux aussi été passés en revue. Les participants et orateurs ont recensé un certain nombre de recommandations concernant les mesures concrètes que les pays de la région doivent prendre, dont les suivantes :

- Dans le domaine de **l'élaboration d'un cadre juridique et de l'exécution effective**, les pays ont invité les gouvernements de la région à se joindre aux efforts déployés au niveau international, en coordination et coopération avec les efforts menés au niveau régional et international. Ils ont noté qu'une assistance plus directe aux pays s'imposait ; avec l'aide des outils existants, dont le récent kit de l'UIT pour un modèle de législation sur la cybercriminalité et pour mieux comprendre la cybercriminalité, les pays de la région sont à même de prendre des mesures dans ce domaine. Il a été décidé de faire une place aux contributions nationales sur les activités en matière de cybersécurité nécessaires dans les réunions régionales préparatoires de l'UIT en vue de la conférence mondiale sur le développement des télécommunications, qui se tiendront en Ouganda en juillet 2009, puis en Syrie en janvier 2010.
- À l'issue de la réunion et des débats qui se sont déroulés au cours des quelques semaines écoulées, les pays ont fait savoir qu'ils avaient besoin d'une aide directe pour l'élaboration de **capacités en matière de veille, d'alerte et de gestion des incidents** et pour l'établissement des structures organisationnelles à responsabilité nationale qui s'imposent, dont des équipes d'intervention en cas d'incident informatique (CIRT). Ces efforts nationaux peuvent parallèlement être l'occasion d'activités menées en coopération aux niveaux régional et international, dont la création éventuelle de centres régionaux. Un certain nombre de

---

[44] Voir le site web pour le Forum régional UIT sur la cybersécurité pour les pays d'Afrique de l'Est et d'Afrique australe tenu à Lusaka (Zambie) (25-28 août 2008) à l'adresse suivante: www.itu.int/ITU-D/cyb/events/2008/lusaka/

[45] Voir le site web pour le forum régional UIT sur les cadres pour la cybersécurité et la protection des infrastructures essentielles de l'information (CIIP) pour les États arabes tenu à Doha (Qatar) (18-21 février 2008) à l'adresse suivante: www.itu.int/ITU-D/cyb/events/2008/doha/

pays de la région (Afrique du Sud, Arabie saoudite, Burkina Faso, Burundi, Côte d'Ivoire, Égypte, Émirats arabes unis, Iraq, Kenya, Maroc, Maurice, Ouganda, Nigéria, Rwanda, Tanzanie, Tunisie et Zambie) travaillent actuellement de concert avec l'UIT, en collaboration avec des partenaires clés, dont l'International Multilateral Partnership Against Cyber Threats (IMPACT), dans le but de faciliter le renforcement des capacités en matière de cybersécurité, y compris par la création de CIRT nationaux.

- Par ailleurs, les pays se sont engagés à prendre des mesures concrètes visant l'élaboration d'une **stratégie nationale en matière de cybersécurité** et de veiller à l'harmonisation dans le respect des principes fondamentaux régissant la coopération internationale. L'élaboration des stratégies nationales bénéficiant de l'engagement de décideurs nationaux essentiels facilite le processus permettant la mise en place des mesures, législations et capacités qu'il faut aux pays pour intervenir efficacement contre les cybermenaces. À cet égard, les pays peuvent mettre à profit l'expertise et les ressources que l'UIT et d'autres organisations régionales ou internationales ainsi que le secteur privé peuvent leur assurer, afin de bénéficier de l'assistance qu'il leur faut pour mettre en place une politique nationale en matière de cybersécurité. Il a également été souligné que ces mesures doivent être prises au sein d'une structure de coopération internationale bien établie se fondant sur l'œuvre déjà accomplie dans les pays, dans le cadre d'organisations régionales ou internationales.

- Des pays ont noté le besoin de **procéder au renforcement de capacités** dans tous les domaines ayant trait à la cybersécurité, en tenant particulièrement compte des parties prenantes ayant des besoins spécifiques. Il nous faut lancer des actions susceptibles d'aider les États Membres à identifier les risques que les enfants et les jeunes courent en ligne et à renforcer les activités nationales dans le domaine de la protection de l'enfance en ligne.

67. Les questions ayant trait à la cybersécurité constituent un ensemble complexe de problèmes d'ordre à la fois technologique, politique et culturel. Les pays d'Afrique et les États arabes se trouvent assurément à des étapes différentes dans la mise en place d'interventions efficaces et de capacités institutionnelles et humaines pour répondre aux problèmes ayant trait à la cybersécurité, mais on constate de nets progrès et les pays sont optimistes quant à l'évolution de leur état de préparation et à l'appui dont ils bénéficient. Les participants au forum étaient tous convaincus que pour garantir la cybersécurité au niveau national, une approche mondiale s'impose. L'UIT s'efforce de comprendre les besoins spécifiques des pays de la région afin de pouvoir offrir une tribune permettant de dégager un accord sur la manière dont l'UIT peut, avec ses partenaires, tenir compte des besoins de tous les pays.

Clôture de la réunion

68. En prononçant la clôture de la réunion, M. Zouari a fait quelques remarques au nom de l'Agence nationale tunisienne pour la sécurité informatique, qui a accueilli le Forum régional UIT sur la cybersécurité pour l'Afrique et les États arabes.

69. Dans les remarques de clôture qu'il a prononcées au nom de l'UIT et du Directeur du Bureau de développement des télécommunications de l'UIT, Miloud Ameziane, Chef du Bureau régional de l'UIT pour les États arabes, a exprimé l'espoir que les participants auront trouvé cette rencontre de deux jours instructive et utile. M Ameziane a remercié tous ceux qui, directement ou indirectement, avaient contribué à faire du forum une réussite, et a remercié tout particulièrement les hôtes locaux d'avoir tout mis en œuvre pour avoir rendu possible le Forum régional sur la cybersécurité. Il a également remercié les orateurs d'avoir pris le temps de rédiger le texte de leur intervention et partagé leurs expériences et leur expertise avec les autres participants. L'UIT, a-t-il ajouté, espère continuer de fournir cette tribune au sein de laquelle les vues des États, du secteur privé et des autres parties prenantes concernées par la cybersécurité et la protection des infrastructures essentielles de l'information peuvent faire l'objet d'une réflexion à l'occasion des diverses activités, initiatives et manifestations organisées.

L'adresse électronique pour l'envoi de toute observation sur cette réunion est la suivante : [46] **cybmail(at)itu.int**[47].

À des fins de partage de l'information, le nom de tous les participants sera ajouté aux listes de diffusion électronique cybersecurity-arab-states@itu.int et cybersecurity-africa@itu.int [48] pour toutes les questions concernant les activités de l'UIT-D dans le domaine de la cybersécurité. Si vous n'avez pas participé directement au forum, ou si votre nom ne figure pas déjà sur la liste de diffusion électronique, et que vous souhaitez participer à ces discussions dans le cadre de la liste de diffusion et du forum, veuillez nous envoyer un courrier électronique à l'adresse: cybmail@itu.int.

---

[46] Le présent rapport sur le Forum peut être consulté en ligne: http://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/tunis-cybersecurity-forum-report-june-09-fr.pdf

[47] Prière de faire parvenir toute observation sur le rapport consacré au forum à l'adresse suivante: cybmail@itu.int

[48] Listes régionales de diffusion électronique sur la cybersécurité: cybersecurity-arab-states@itu.int et cybersecurity-africa@itu.int. Prière d'envoyer un courrier électronique cybmail@itu.int, pour qu'on rajoute vos coordonnées sur la liste correspondante.