
CONFERENCE REGIONALE AFRICAINE SUR LA CYBERSECURITE AF-CYBERSEC-08

« Bâtir un espace numérique de confiance en Afrique »

Yamoussoukro, du 17 au 20 novembre 2008

RAPPORT DE LA CONFERENCE

Les pays africains conscients de l'importance de la société de l'information dans leur développement économique et social, ont entrepris plusieurs actions pour adresser la problématique de la cybercriminalité qui crée un risque sécuritaire dans la société numérique. C'est dans cette optique que l'Agence des Télécommunications de Côte d'Ivoire (ATCI), l'Organisation Internationale de la Francophonie (OIF) et l'Union Africaine (UA) ont organisé la conférence régionale africaine sur la cybersécurité (Af-Cybersec-08) du 18 au 20 novembre 2008 à l'Hôtel Président de Yamoussoukro (Côte d'Ivoire). Cette conférence avait pour thème: "**Bâtir un espace numérique de confiance en Afrique**" avec pour objectif général la proposition d'un Plan d'actions de cybersécurité et de lutte contre la cybercriminalité.

La présente conférence a consisté en des ateliers, des conférences, des échanges débats et le partage d'expérience des certains pays.

1. Cérémonie d'ouverture

La cérémonie d'ouverture de la conférence régionale africaine sur la cybersécurité (AF-CYBERSEC 08) a eu lieu le 18 novembre 2008. Elle a été marquée par l'intervention du :

- Directeur Général de l'ATCI, Président du comité d'organisation ;
- Représentant de l'Union Africaine;
- Ministre des Nouvelles Technologies de l'Information et de la Communication ;
- Président de la République de Côte d'Ivoire.

Dans son discours, le Directeur Général a décrit la problématique de la cybersécurité en illustrant ses propos par une fiction dans laquelle une attaque informatique viendrait bouleverser tout le système informatique des banques à la veille des fêtes de fin d'année empêchant ainsi les citoyens d'effectuer leurs opérations bancaires. Il a mis l'accent sur l'initiative prise par les pays africains de mettre en place un cadre légal de lutte contre la cybercriminalité à l'instar des pays des autres continents. Les travaux de cette conférence font donc l'objet d'une attention particulière de la part de la communauté internationale notamment de l'UA et de l'OIF. Il a donc invité les participants à faire des propositions et recommandations à leurs gouvernements afin de doter les différents pays africains de cadres légaux relatifs à la cybersécurité et à la lutte contre la cybercriminalité.

Le représentant de l'UA a exprimé sa satisfaction d'être associé à cette conférence. Il a préconisé la coopération internationale dans la lutte contre les cybercriminels car leurs crimes sont transfrontaliers.

Le Ministre des NTIC a félicité les organisateurs de cette conférence. Le développement des TIC peut entraîner une utilisation frauduleuse des réseaux et systèmes d'information. Il faut par conséquent, réduire cette menace en opposant la cybersécurité à la cybercriminalité. Il a souhaité le renforcement du code pénal national afin de prendre en compte cette nouvelle forme de criminalité. Il a remercié le Président de la République de Côte d'Ivoire pour avoir rehaussé de sa présence la présente cérémonie.

Dans son allocution, le Président de la République a exprimé sa disponibilité à soutenir les projets de lois relatifs à la cybersécurité. Il a souhaité que ces projets soient prêts avant la fin de l'année 2008. Il a mis l'accent sur l'importance des TIC dans la vie économique et sociale d'une nation. En ce qui concerne la Côte d'Ivoire, l'énergie et les TIC constitueront les bases de l'économie de demain. Aussi, a-t-il donné des instructions au Ministre des NTIC pour que le Directeur Général de l'ATCI prenne des dispositions pour l'identification des abonnés mobiles. Il a enfin exhorté les participants à rester proches des objectifs de cette conférence qu'il a déclarée ouverte.

2. Ordre du jour de la réunion

- Cérémonie d'ouverture
- Atelier 1 : Infrastructures à clés publiques (ICP)
- Atelier 2 : Convention du Conseil de l'Europe sur le Cybercrime
- Conférence 1 : Stratégies nationales de Cybersécurité : le cas Nigérian
- Conférence 2 : Coopération internationale
- Conférence 3 : Différents types de menaces liées à la Cybersécurité
- Conférence 4 : Moyens juridiques de protection contre la Cybersécurité
- Conférence 5 : Cadre réglementaire, cas du Canada
- Conférence 6 : Libertés, vie privée et Cybersécurité
- Session plénière
- Cérémonie de Clôture

3. Les ateliers et conférences

Plusieurs conférences ont été dites les 18, 19 et 20 novembre 2008 sur la cybercriminalité, la cybersécurité et l'expérience de certains pays en matière de stratégie de cybersécurité. Ces conférences ont été précédées, le 17 novembre 2008, par deux ateliers dont l'un sur les infrastructures à clés publiques (ICP), ou Public Key Infrastructure (PKI) en Anglais, et l'autre sur la Convention du Conseil de l'Europe sur le cybercrime.

3.1. Les ateliers

3.1.1. Atelier 1 : Infrastructures à clés publiques (ICP)

Cet atelier a porté d'une part, sur la cryptographie à clés publiques et d'autre part, sur les infrastructures à clés publiques à proprement dit.

Cryptographie à clé publique

Ce thème a été présenté par le Dr Kla Sylvanus, Directeur Général de l'ATCI (Côte d'Ivoire). Dans son intervention, le conférencier a montré l'importance de la cryptographie dans les échanges électroniques entre les nations, les organisations et les entreprises. En effet, elle permet de garantir l'authenticité, l'intégrité, la non répudiation et la confidentialité des échanges qui ont une importance capitale dans certains domaines d'activités tels que la sécurité, la défense et la banque. Le conférencier a ensuite présenté les principes de cette cryptographie à clés publiques et ressorti le fait que son utilisation requiert l'existence d'une autorité de certification qui inspire confiance par la rigueur qui devra être une de ses valeurs principales. Pour finir, il a invité les pays africains à entrer dans l'économie numérique en mettant en place des autorités nationales de certification.

Infrastructures à clés publiques

Ce thème a été présenté par Dr Yao Eric de la Côte d'Ivoire et monsieur Ukpong Imo du Nigéria. Dans son intervention, Dr Yao Eric a présenté les infrastructures à clés publiques comme un ensemble de composants physiques, de procédures humaines et de logiciels qui permettent d'instaurer des relations de confiance en vue de favoriser les transactions électroniques. Il a aussi présenté l'objectif et la valeur des certificats, le processus de certification, le cycle de vie d'un certificat et quelques modèles de confiance. Il a recommandé la mise en place d'une autorité de certification et d'un cadre juridique approprié pour l'effectivité de cette confiance en la société de l'information. Cette autorité devra permettre la mise en place des ICP pour établir un cadre de confiance dans les échanges électroniques.

Quant à monsieur Ukpong Imo, il a retracé le parcours pour mettre en place de telles infrastructures avec les difficultés y afférentes. Il a également mis en exergue la nécessité d'une politique commune sous régionale voire africaine en matière de ICP. Il a mis l'accent sur la politique, le cadre législatif et réglementaire pour la mise en place des ICP. Il a recommandé le soutien de toute initiative africaine relative aux ICP telle que prévue par l'assemblée mondiale de la société de l'information en 2005 et l'établissement de partenariats pour l'assistance et le partage d'expérience en la matière. Il a aussi recommandé que les Gouvernements africains :

- accordent une importance capitale à la politique et au cadre légal et réglementaire relatif aux ICP ;
- mettent en place la e-gouvernance, la lutte contre le cybercrime, la cybersécurité et les lois relatives aux échanges électroniques ;
- développent l'expertise par la formation et l'infrastructure de télécommunications.

3.1.2. Atelier 2 : Convention du Conseil de l'Europe sur le cybercrime.

Ce thème a été présenté par Me Sarr Abdul de la Côte d'Ivoire et monsieur Udotai Basil du Nigéria. Dans son intervention, Me Sarr a mis l'accent sur l'utilisation des TIC dans la commission des infractions traditionnelles et décrit les types d'infractions et la procédure pénale de la Convention du Conseil de l'Europe sur la cybercriminalité de Budapest en 2001. Ces infractions, même si elles ne sont pas réprimées dans certains pays, elles sont transfrontalières. D'où la nécessité d'une coopération dans la lutte contre ces nouvelles formes d'infractions appelées cybercriminalité. Ce qui a abouti à ladite convention dont l'objet principal est l'harmonisation des lois nationales par l'identification des nouvelles infractions et la mise en place d'une procédure de coopération internationale.

Quant à Monsieur Udotai Basil, il a présenté la coopération internationale en matière de cybercriminalité. Il a relevé que l'Europe y a pensé et l'a fait à travers ladite convention qui ne peut à elle seule résoudre les problèmes liés à la cybercriminalité à cause des vides juridiques dans certains pays. Il est donc nécessaire que ces pays s'adaptent à cette nouvelle donne en sollicitant l'aide des autres pays qui en ont déjà l'expérience. La restructuration des lois nationales pour répondre aux problèmes qui viennent de l'extérieur et inversement, s'impose parce qu'un acte illégal dans un pays peut ne pas l'être dans un autre.

En somme, la Convention Européenne sur le cybercrime interpelle les africains mais avant d'y adhérer, il est nécessaire que déjà chaque pays africain élabore des lois relatives aux infractions liées aux TIC. Etant donné que les accords de coopération en matière d'infractions traditionnelles sont difficilement applicables pour ne pas dire inapplicables aux infractions commises à partir des TIC. Pour ce faire, le Conseil de l'Europe est prêt à assister les pays africains dans la lutte contre la cybercriminalité.

3.2. Les conférences

Les huit (8) conférences faites ont porté sur les thèmes suivants :

3.2.1. Stratégies nationales de cybersécurité : cas du Nigéria

Cette conférence dite par monsieur Udotai Basil du Nigéria a concerné la présentation de la stratégie nationale de cybersécurité au Nigéria. Dans son intervention, le conférencier a présenté les bases de cette stratégie, les actions déjà entreprises et celle restant à faire. Cette stratégie est basée sur :

- la définition une politique qui donne l'orientation en matière de cybersécurité et définit les structures devant coordonner les actions ;
- la mise en place des lois appropriées pour lutter contre la cybercriminalité ;
- le renforcement des capacités institutionnelles et en ressources humaines par la formation des personnes, des autorités judiciaires et policières.
- la sensibilisation et la prise de conscience de la population. Cette sensibilisation est ciblée et sectorielle. Elle concerne les institutions gouvernementales et la société civile;
- la collaboration entre secteur public et secteur privé ;
- le renforcement de la coopération internationale ;

La mise en place d'un système de gestion des preuves numériques, l'identification des abonnés et la mise en place de mécanismes de localisation des utilisateurs des TIC, en cas de nécessité, sont des actions cette stratégie. Celle-ci met à contribution les structures spécialisées dans la lutte contre la criminalité (Police, Douane, etc.) et met en place un organe suprême de coordination des activités de cybersécurité. En ce qui concerne la coopération internationale, beaucoup d'efforts ont été faits en la matière. Cependant, le Nigéria n'a pas encore signé la convention du Conseil de l'Europe mais il l'expérimente à ce jour.

3.2.2. Coopération internationale

Cette conférence a été dite par Monsieur Joël Schwarz des USA. Dans son intervention, le conférencier a présenté un cas pratique de coopération internationale entre les USA et l'Argentine dans le cadre d'une enquête relative à un enlèvement (kidnapping). Il a mis en exergue la démarche administrative et des mécanismes techniques pour détecter et localiser en temps réel une activité sur

internet. Il a aussi recommandé de la célérité dans les actions de recherche des cybercriminels et dans la coopération entre des structures judiciaires et policières des pays. La mise en place d'un point de contact 24h/24 et 7j/7 dans la coopération internationale est une solution efficace dans la prévention et la lutte contre la cybercriminalité dans le monde. Les cybercafés constituant un point d'accès à Internet prisé par les cybercriminels, il serait judicieux d'envisager la possibilité de les faire enregistrer auprès d'une autorité publique nationale.

3.2.3. Différents types de menaces liées à la cybersécurité

Cette conférence a été dite par monsieur Joel Schwarz des USA. Dans son intervention, le conférencier a relevé les avantages de l'Internet dans la croissance économique des Etats notamment dans la télé-médecine, le e-commerce et l'enseignement à distance. Mais pour être efficaces, les réseaux et systèmes d'information doivent bénéficier d'une bonne sécurité car les menaces sont réelles. Ces menaces sont entre autres, les virus, les vers, la fraude sur l'identité, la pornographie infantile mais aussi les attaques contre les infrastructures critiques. Il a illustré ces propos par l'exemple de l'attaque du réseau électrique canadien qui a eu des conséquences désastreuses au Canada et aux USA. Par conséquent, les pays doivent mettre en place une stratégie de cybersécurité et une politique et des lois pour lutter contre la cybercriminalité. Celles-ci devront porter une attention particulière aux infrastructures critiques.

3.2.4. Moyens juridiques de protection contre la cybercriminalité

Cette conférence a été animée par Pr Cissé du Sénégal, Messieurs Schwarz Joel et Udotai Basil du Nigéria.

Dans son intervention, le Professeur Cissé a ressorti la nécessité d'élaborer des stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques dans un environnement global de gestion des risques, menaces et crimes. La cybersécurité touche au patrimoine numérique et culturel des individus, des organisations et des nations et requiert une volonté politique. Laquelle vise à l'obtention d'un niveau de sécurité technologique suffisant pour prévenir et maîtriser les risques, à l'édification d'une société de l'information respectueuse des valeurs et protectrice des droits et libertés et à la contribution à l'économie du savoir. L'environnement ainsi créé doit, en vue d'inspirer confiance, être prévisible, organisé, protecteur, sécurisé et intégré à l'ordre international. Il a aussi présenté les cinq axes relatifs aux moyens juridiques de la cybersécurité que sont, une politique de cybersécurité, une cyberéthique, un cyberdroit pénal, une procédure pénale adaptée et des institutions appropriées.

Le second conférencier, monsieur Schwarz Joël a présenté la stratégie de cybersécurité mise en place par la Communauté Economique Asie-Pacifique (APEC). Cette stratégie approuvée par les ministres en 2002, comprend le développement des normes juridiques, le partage de l'information, l'élaboration de directives sécuritaires et techniques, la formation et l'éducation (des enquêteurs aux techniques d'investigation dans le domaine, des personnes ressources dans le public et le privé) et la planification des systèmes sans fil et des technologies émergentes. Il a aussi présenté la stratégie de l'Organisation des Etats Américains (OAS) qui comprend dix (10) recommandations adoptées par les ministres dont un point de contact 24/7 auquel six (6) pays africains (Nigeria, RSA, Namibie, Tunisie, Maurice et Congo-Brazza) ont déjà adhéré. Ces recommandations peuvent être utilisées comme lignes directrices dans l'élaboration des stratégies nationales ou sous régionales africaines.

Quant au dernier conférencier, monsieur Udotai Basil, il a présenté la nature des TIC qui est globale, peu sûr, anonyme et à l'échelle illimitée, concurrentielle et à bas coup de communication, neutre et partagée, etc. Il a préconisé d'une part l'élaboration de cadres juridiques qui prennent en compte toutes ces spécificités et d'autre part, le renforcement de la coopération transfrontalière et le renforcement des capacités institutionnelles et en ressources humaines (formation des personnes ressources dans la lutte contre la cybercriminalité : police scientifique, gendarmerie, etc.). En outre, il a recommandé que les fournisseurs d'accès Internet disposent d'une capacité à préserver, conserver et communiquer l'information à l'autorité désignée par les pouvoirs étatiques.

3.2.5. Cadre réglementaire, cas du Canada

Cette conférence a été animée par les professeurs Kablan Serge et Oulai Arthur du Canada. Ils ont axé leur présentation sur l'expérience canadienne en matière de lutte contre la cybersécurité. Le code criminel canadien actuel pourrait couvrir les infractions du cyberespace. Dans le cyberespace, il est difficile de rendre effectif la protection des droits car tous les critères juridiques (matérialité, localisation, imputation) ne peuvent être observés dans le monde virtuel.

Au Canada, il n'y a pas d'obligation de surveillance active du contenu imputé aux fournisseurs d'accès Internet et hébergeurs. Ils bénéficient d'une exemption de responsabilité quant aux contenus des sites qu'ils hébergent, sauf s'ils ont connaissance du caractère illicite. Dans ce cas, il pèse sur eux une obligation de faire cesser les services qu'ils hébergent. Depuis 2007, le législateur canadien a modifié sa législation afin de prendre en compte les nouvelles données émanant du cyberespace tout en impliquant tous les acteurs.

3.2.6. Libertés, vie privée et cybersécurité

Cette conférence a été animée par Dr Assoko de la Côte d'Ivoire et les professeurs Oulai et Kablan du Canada. Dans son intervention, Dr ASSOKO a relevé que l'existence de grand nombre de textes nationaux applicables sur le réseau mondial est source d'insécurité juridique, d'où la nécessité d'élaborer un cadre de coopération qui sera mis en œuvre par tous, car l'Internet et les TIC soulèvent de nouvelles menaces en matière de protection des données à caractère personnel et des libertés. Ce cadre de coopération internationale étant souvent difficile à mettre en œuvre, il serait judicieux de procéder à une harmonisation de textes nationaux existants afin d'aboutir à un modèle de lois applicables par tous.

Dans leur intervention les professeurs Oulai et Kablan ont relevé le fait qu'au Canada, la surveillance des employés peut être tolérée dans la mesure où l'employeur respecte le critère du caractère raisonnable de cette surveillance et que les employés soient clairement informés sur le but et la destination de la collecte d'information et que les personnes aient les moyens d'accéder aux informations collectées sur elles. Le Canada, dans sa législation en matière de données personnelles, soumet à des conditions exigeantes, la collecte des données personnelles dans le souci de la préservation des libertés individuelles. Ce pays exige une obligation régulière de réviser la loi en ce domaine conformément à la dimension dynamique et évolutive de la technologie, support de divulgation des données à caractère personnel.

3.2.7. Stratégies régionales et continentales

Cette conférence a été dite par Dr Solange GHERNAOUTI-HELIE de l'Université de Lausanne, Suisse. Dans son intervention, la conférencière a relevé l'Internet comme un outil de performance pour les organisations terroristes. Et qu'il y a une insuffisance d'adaptation au caractère dynamique

et évolutif de l'Internet, d'où la nécessité de réponse nationale et internationale. Il faut donc un cadre légal approprié afin d'éviter l'existence de « paradis digital ». Pour ce faire, il faut :

- mettre en place des processus de gestion pour protéger, prévenir et garantir le fonctionnement adéquat de toute infrastructure de système d'information. La nécessité d'une politique nationale de cybersécurité pour la protection des outils de production et la protection des individus ;
- mettre en place un cadre de coopération horizontale (international et régionale) en fédérant les ressources et en développant d'une part, celles existantes ailleurs et d'autre part, des ressources complémentaires en vue de l'adapter à notre propre système de coopération vertical (autorités publiques et secteur privé) ;
- faire le renforcement des capacités (logiciel, matériel, humaine) en matière de lutte contre la cybercriminalité (en se référant par exemple à ce qui est déjà fait ailleurs tel que la convention contre la cybercriminalité du Conseil de l'Europe) ;
- prendre conscience au niveau nationale de la nécessité de disposer d'un CERT national tout en sachant développer une bonne coopération régionale par la capitalisation des compétences.

L'UIT est un organe fédérateur dans le cadre d'une stratégie adéquate de cybersécurité et il serait opportun de se référer à ses travaux sur le sujet.

3.2.8. Stratégies nationales, cas de la Tunisie

Cette session a vu la présentation de la stratégie nationale tunisienne de la cybersécurité. Elle a été animée par monsieur Frika Naoufel de la Tunisie. Dans son intervention, le conférencier a relaté l'approche tunisienne de la cybersécurité. Les principales lignes directrices de la stratégie tunisienne sont les suivantes :

- la sécurité des systèmes d'informations nationaux ;
- la sécurité du cyberspace ;
- la consolidation du savoir faire en matière de sécurité informatique ;
- la formation et la sensibilisation en matière sécurité informatique ;
- la mise en place des dispositions juridiques et réglementaires.

Pour mener à bien la stratégie de cybersécurité, des actions qui ont déjà été menées par l'Etat tunisien. Il s'agit de la mise en place d'un CERT, d'une politique de formation et de sensibilisation auprès de la population en générale, de la création d'un centre d'observation et d'alerte. En outre, d'autres actions ont été révélées telles que la création d'une équipe pour la gestion d'incidents sécuritaires, une organisation du domaine de l'audit de sécurité avec une obligation d'audit périodique pour toutes les entités ayant des ressources disponibles via un réseaux et la mise à jour du cadre juridique tunisien en tenant compte des mesures prises. Le suivi de toutes ces mesures prises est assuré par l'Agence nationale de la sécurité informatique, spécialisée dans la sécurité des systèmes d'information, et créée en 1999.

4. Plénière de synthèse

Une session plénière s'est tenue le 20 novembre 2008 afin de valider et d'entériner le PLAN de YAMOUSSOUKRO sur la CYBERSECURITE (YCP) comprenant 3 axes stratégiques accompagnés d'une série d'actions prioritaires. Ces Axes stratégiques sont les suivants :

- Développement des capacités humaines (éducation et formation),
- Création d'un environnement favorable (cadres juridiques, réglementaires, politiques et de plaidoyer),
- Sensibilisation (renforcement de la confiance, de la sécurité et des directives) ;

(voir en annexe le YCP)

5. Recommandations de la conférence

La Conférence régionale africaine sur la cybersécurité

1. recommande à la Commission de l'Union africaine (CUA) de rédiger la charte africaine sur le Cybersécurité ;
2. recommande à la Commission de l'Union africaine (CUA) également de créer une unité spéciale dans le département des Ressources Humaines, la Science et la Technologie (HRST) pour traiter spécifiquement des problèmes de Cybersécurité ;
3. recommande à la Commission de l'Union africaine (CUA) d'instituer de la Conférence régionale africaine sur la cybersécurité comme un événement annuel tenu de façon tournante dans une des différentes régions de l'Afrique ;
4. demande à la Côte d' Ivoire devra travailler étroitement avec la Commission de l'Union africaine comme Secrétariat permanent de la conférence jusqu'à la prochaine session de la conférence.

6. Cérémonie de clôture

Dr. Sylvanus KLA, le Directeur Général de l'agence des Télécoms de Côte d'Ivoire (ATCI), a remercié tous les participants pour les débats enrichissants sur tous les sujets couverts et pour la production de recommandations fondamentales.

Il a aussi remercié l'Union Africaine et l'Organisation internationale de la francophonie pour leur soutien à l'ATCI, ainsi que tous ceux qui ont contribué au succès de la conférence régionale africaine sur la Cybersécurité (AF-CYBERSEC-08).

Il a clôturé la conférence et a souhaité à tous un bon voyage retour.
