Tunis, Tunisia
04-05 June 2009

REGIONAL CYBERSECURITY FORUM 2009

International Telecommunication Union

Expérience de la Côte d'Ivoire

Didier KLA
Ingénieur Télécom
padkla@gmail.com

SOMMAIRE

Introduction

- *Les réseaux numériques occupent aujourd'hui une place importante au sein des sociétés modernes*
- *Ils ont particulièrement transformé la société au niveau social, économique et politique engendrant de nouvelles menaces sécuritaires beaucoup plus complexes, transfrontalières et la plupart du temps imprévisibles.*
- *L'enjeu majeur pour les états africains au risque d'accentuer la fracture numérique avec les pays développés est de mettre en place une stratégie de cybersécurité au niveau national et de développer une coopération internationale.*

Etat des lieux du secteur des TICS en Côte d'Ivoire

Quelques chiffres (2008)

- ***Population estimée à 20 millions d'habitants***
- ***Nombre d'opérateurs fixes exerçant : 2***
- ***Nombre d'opérateurs mobiles exerçant : 5***
- ***Nombre d'ISPs exerçant : 11***
- ***Internet : 60 000 abonnés haut débit avec une progression de 100 % entre 2007 et 2008***
- ***Mobile : 10 millions d'abonnés avec une progression de 30 % chaque année au cours de ces trois dernières années***
- ***Taux de pénétration de 50%***
- ***Fixe : 350 000 abonnés mais un fort ralentissement de la croissance observé ces trois dernières années.***
- ***CA annuel : 1 milliards d'Euro***
- ***Secteur : 6 % du PIB***

Etat des lieux du secteur des TICS en Côte d'Ivoire

- ***Cadre légal et réglementaire date de 1995 (ne prend pas en compte les évolutions récentes au niveau des TICs)***
- ***Beaucoup d'actes répréhensibles commis sur (ou en utilisant) les réseaux numériques***
  - ***Arnaques sur Internet à partir des cybercafés (le plus développé)***
  - ***Diffusion de fausses informations troublant l'ordre public par envoi de SMS***
  - ***Attaques de sites web institutionnels***
- ***Inexistence de textes de lois sur la cybercriminalité***
- ***Pas de Stratégie Nationale de cybersécurité jusqu'en 2008***

Au vu de toutes ces faiblesses et mesurant l'impact que pourrait avoir l'absence au niveau national d'une stratégie de la cybersécurité, le gouvernement ivoirien a entrepris de mettre en place une stratégie depuis 2008.

Stratégie Nationale de Cybersécurité

- ***La démarche a consisté à sensibiliser les différents acteurs (secteur public, secteur privé, société civile et milieux académiques) en organisant un Forum national sur la cybersécurité du 18 au 19 Juin 2008 à Abidjan.***
- ***La principale résolution de ce forum a été la mise en place en urgence d'un groupe de travail regroupant le secteur public, le secteur privé et la société civile sous l'égide de l'ATCI (Agence de Télécommunication de Côte d'Ivoire)***

Les missions assignées à ce groupe de travail étaient :

- ***Proposer des textes de lois pour la cybersécurité***
- ***Identifier et définir le cadre institutionnel, juridique et légale des structures à mettre en place dans le cadre de la cybersécurité (CERT, Agence de certification, Agence de sécurité informatique, etc.)***
- ***Définir une stratégie de protection des infrastructures critiques nationales***
- ***Proposer une politique pour le renforcement des capacités (Ingénieurs, juristes, forces de sécurité, etc.)***
- ***Proposer un cadre de coopération internationale au niveau de la cybersécurité***

Stratégie Nationale de Cybersécurité

Suite aux travaux du groupe de travail la stratégie proposée se décline de la façon suivante :

- *Techniques*
- *Structurels*
- *Juridiques*
- *Renforcement des capacités et sensibilisation*
- *Coopération Internationale*

Stratégie Nationale de Cybersécurité

Techniques

- *Sécuriser les infrastructures de telles sortes qu'elles soient disponibles, assurent l'intégrité, la confidentialité des données qui y transitent et permettent l'identification et l'authentification des utilisateurs.*

- *Assurer une sécurité physique des infrastructures techniques*

Stratégie Nationale de Cybersécurité

Structurels

- *Mise en place au sein des ministères en charge de la sécurité de structures de lutte contre la cybercriminalité (police, gendarmerie, douane, etc.)*

- *Mise en place d'une agence de certification numérique*

- *Mise en place d'un CERT*

Stratégies Nationales de Cybersécurité

Juridique, légal et réglementaire

- *Rédiger des textes de loi prenant en compte les activités nées avec le développement des TICs (cybercriminalité, commerce électronique, protection des données personnelles, cryptographie, etc..)*

- *Inclure dans le nouveau code des télécoms toutes les questions liées à la cybersécurité*

Stratégie Nationale de Cybersécurité

Renforcement des capacités et sensibilisation

- *Formation des ingénieurs, des juristes et des forces de sécurité*
- *Développement d'un culture de cybersécurité au sein des populations par la sensibilisation*
- *Conférence annuelle sur la cybersécurité regroupant le secteur public, le secteur privé, la société civile et les milieux académiques*

Stratégie Nationale de Cybersécurité

Coopération Internationale

- *Bénéficier de l'expérience des pays ayant élaborer une stratégie*

- *Collaborer avec toutes les organisations Internationales travaillant dans le domaine de la cybersécurité pour une stratégie globale*

Actions réalisées ou en cours

- ***Projet de loi sur la cybercriminalité transmis au gouvernement pour adoption***
- ***Mise en place d'un cadre formel de collaboration entre les entités intervenants dans la cybersécurité (Forces de sécurité, Opérateur Télécom, Agence de régulation, Justice, etc.)***
- ***Identification des abonnés des opérateurs mobiles à partir du 01 Juillet 2009 (campagne de sensibilisation a démarré)***
- ***Identification des cybercafés et obligation pour leurs clients de s'identifier (Réunion de sensibilisation des propriétaires de cybercafés au mois de février 2009)***
- ***Renforcement de la capacité opérationnelle de la police scientifique (fourniture d'équipements et formation des agents par GTZ, Interpol et ATCI)***
- ***Mise en place d'un CERT avec l'appui de la Tunisie (une convention d'assistance est en cours de signature entre l'ATCI et l'ANSI)***
- ***Révision du cadre Institutionnel, légal et réglementaire en cours pour tenir compte des évolutions du secteur mais surtout de la cybersécurité.***
- ***Séminaires de renforcement des capacités des ingénieurs et techniciens sur la cybersécurité (plusieurs sessions ont déjà eu lieu)***

Actions réalisées ou en cours

- *Une stratégie de cybersécurité ne pouvant pas se limiter au cadre national, le gouvernement Ivoirien a entrepris des actions au niveau international. Ainsi avec l'appui de l'OIF et de CUA, il a organisé du 18 au 20 Novembre 2008 à Yamoussoukro une conférence régionale Africaine sur la Cybersécurité* ***(Afcybersec2008 : www.afcybersec.org****) sur le thème :*

<< Bâtir un Espace Numérique de Confiance en Afrique >>

- *Cette conférence a vu la participation d'une vingtaine de pays africains et d'organisations régionales et internationales (UA, CEDEAO, UE, ONU).*
- *A l'issue des travaux de Yamoussoukro un* ***Plan d'action*** *a été adopté qui comprend 4 principes stratégiques auxquels sont associés des actions prioritaires.*

Plan d'Action de Yamoussoukro de la Cybersécurité

Actions prioritaires

- ***Développer les capacités humaines (éducation et formation)***
- ***Environnement favorable (cadres juridiques, réglementaires, politiques et de plaidoyer)***
- ***Sensibilisation (Renforcement de la confiance, de la sécurité et des directives relatives au cyberespace)***
- ***Problèmes mondiaux (partage de l'information et initiative de coopération régionale et internationale)***

Plan d'Action de Yamoussoukro de la Cybersécurité

Principe stratégique I

- ***Développer les capacités humaines (éducation et formation)***
- ***Actions prioritaires :***

  - ***Jeter les bases africaines pour les programmes de certification de cybersécurité unanimement acceptés par le secteur public et le secteur privé.***

  - ***Identifier et organiser des programmes de formation aux questions techniques et juridiques que posent la cybersécurité et la protection de l'infrastructure essentielle.***

  - ***Promouvoir l'éducation des professionnels en sécurité technologique; examiner les programmes de certification professionnelle et de qualification pour ces professionnels; et promouvoir le développement et la distribution des supports éducatifs.***

Plan d'Action de Yamoussoukro de la Cybersécurité

Principe stratégique II

- ***Environnement favorable (cadres juridiques, réglementaires, politiques et de plaidoyer)***
- ***Actions prioritaires :***
  - ***Les États membres africains devraient élaborer et adopter des lois et des politiques de fond, procédurales et d'assistance mutuelle prenant en compte les initiatives nationales, régionales, continentales et internationales.***
  - ***La CUA, l'UIT et la CEA, en collaboration avec le Conseil de l'Europe et d'autres organes expérimentés, devraient faciliter les efforts des États membres africains visant à élaborer des lois et politiques de fond, procédurales et d'assistance mutuelle.***
  - ***Une base de données des lois de fond, procédurales et d'assistance mutuelle des États membres africains et son statut devraient être mise en place et définie sous les auspices de la CUA.***
  - ***Élaborer des stratégies de gestion des risques, y compris les stratégies d'évaluation de risques, de prévention, de transfert et de conservation***

Plan d'Action de Yamoussoukro de la Cybersécurité

Principe stratégique III

- ***Sensibilisation (Renforcement de la confiance, de la sécurité et des directives relatives au cyberespace)***
- ***Actions prioritaires :***

  - ***Identifier les normes et les meilleures pratiques de sécurité des TI.***

  - Sécuriser le cyberspace, y compris les protocoles Internet, le matériel physique,le système de nom de domaine et le protocole Border Gateway.

  - Examiner les problèmes juridiques et de politique concernant l'encodage, le PKI et l'authentification des transactions électroniques.

  - Formuler les directives de cybersécurité susceptibles d'améliorer la prise de conscience par le public et créer une culture de sécurité du cyberspace.

  - Du fait de la nature intersectorielle du secteur des NTIC, la sensibilisation de la population sur les menaces et les risques liés à la cyber-criminalité, la cyberéthique et les mesures connexes qui devraient être prises est également essentielle.

  - Circonscrire les menaces et les vulnérabilités, y compris en améliorant l'infrastructure et la technologie et en renforçant le contrôle de la technologie

Plan d'Action de Yamoussoukro de la Cybersécurité

Principe stratégique IV

- ***Problèmes mondiaux (partage de l'information et initiative de coopération)***
- ***Actions prioritaires* :**

- ***Apporter un appui aux États membres africains pour mettre en place un système national de réponse pour la sécurité du cyberespace permettant des échanges rapides d'informations et garantissant la résilience pour rétablir rapidement l'ensemble des opérations, en tenant compte de l'élaboration de plans de continuité et d'urgence comme objectifs clés.***
- ***Aider les États membres africains à mettre en place des institutions qui échangent les informations d'évaluation des menaces et des vulnérabilités comme, par exemple, les CERT ; élaborer des programmes pour partager l'expérience et l'expertise en matière de création de telles institutions ; impliquer aussi bien le secteur public que le secteur privé dans cet effort.***
- ***Aider les États membres africains à mettre en place des cellules qui leur permettront de créer des réseaux de point de contact, maintenant une unité de lutte contre la cybercriminalité et un point de contact 24h/24 et 7j/7 désigné aux fins d'apporter une assistance aux investigations sur les cas urgents nécessitant des preuves électroniques et également pour lui permettre de contacter le réseau de point de contact de lutte contre la criminalité High-tech accessible 24h/24 et 7j/7.***

Plan d'Action de Yamoussoukro de la Cybersécurité

Acteurs pour la mise en oeuvre

- *Pour la mise en œuvre de ces recommandations, il est nécessaire qu'il y ait une forte collaboration entre les différentes structures au niveau international (UIT, ICANN, UA, CEA, OIF, etc.)*

Merci