

PLAN DE YAMOOUSSOUKRO SUR LA CYBERSÉCURITÉ YCP

**CONFÉRENCE AFRICAINE SUR LA CYBERSÉCURITÉ
DU 18 AU 20 NOVEMBRE 2008
YAMOOUSSOUKRO, COTE D'IVOIRE**

« BÂTIR UN ESPACE NUMERIQUE DE CONFIANCE EN AFRIQUE »

La Conférence africaine sur la cybersécurité a tenu sa première réunion à Yamoussoukro, en Côte d'Ivoire, du 18 au 20 novembre 2008 et a convenu du plan et d'un certain nombre de principes et d'actions qui sont comme suit :

VISION DE YAMOOUSSOUKRO CONSIGNEE DANS LE PLAN DE CYBERSECURITE

La Conférence africaine sur la cybersécurité propose sa vision pour un cyber-espace sécurisé afin d'assurer la prestation et la continuité de services essentiels de TIC comme composantes essentielles de ce plan dans lequel *« tous les citoyens sans discrimination, de quelque sorte, exercent et pratiquent leurs droits et leur liberté d'expression à rechercher, recevoir et transmettre toutes informations, données et idées légitimes par le truchement d'un cyber-espace sécurisé, pacifique et ne présentant pas de risque »*.

Le nombre total de services et d'applications fournis par le cyber-espace à la génération du millénaire connaît une croissance exponentielle et est sujet à débat. Ce vaste ensemble d'informations, de données, de services, de divertissements et d'arts a été une source d'émerveillement et de controverse et a transformé la manière dont nous menons notre vie. Et, si nous ne sécurisons pas ce cyberspace, nous allons simplement mettre en péril nos vies, nos activités et nos ressources.

Il ne fait guère de doute que les ressources et outils disponibles dans le cyberspace ont considérablement renforcé les opportunités offertes aux populations. La sécurisation du cyberspace est, en conséquence, extrêmement importante pour tout un chacun. Nous avons, à présent, accès à diverses sources de données chaque fois que nécessaire ; nous pouvons nous rendre électroniquement dans des pays qui auraient été géographiquement inaccessibles et nous connecter à des personnes issues de différentes régions du monde. Cette fonctionnalité favorise une compréhension mondiale et permet de nouer des amitiés pérennes.

Le cyberspace offre un grand potentiel pour la promotion du développement durable, la démocratie, la transparence, l'obligation redditionnelle et la bonne gouvernance. L'exploitation à fond de nouvelles opportunités qu'offrent les nouvelles technologies de l'information et de la communication (NTIC) et leur combinaison aux médias traditionnels devraient être favorisées et aller de pair avec la confidentialité, l'intégrité et la disponibilité d'informations à tous les échelons, aux niveaux national et international, afin d'arriver à garantir la sécurité de l'ensemble du cyberspace.

La cybersécurité comporte de nombreuses dimensions et les populations s'attendent, à terme, à ce que les systèmes de cyberspace soient fiables ; autrement dit, que l'on fasse ce qu'il faut et ce à quoi l'on s'attend en dépit des menaces potentielles. Les diverses façons d'appréhender la cybersécurité donnent lieu à de nouvelles orientations en matière d'éducation, de formation, de pratiques de développement, de pratiques opérationnelles, de contrôle, de législations sur la responsabilité et de réglementation par les pouvoirs publics. Dans ce contexte et en réponse à la nécessité pressante d'un plan africain clair de cybersécurité, les principes fondamentaux ci-après visent à définir les orientations, les priorités et actions principales pour l'élaboration d'un plan africain global de cybersécurité.

PRINCIPE STRATEGIQUE I

Développer les capacités humaines (éducation et formation)

Le développement des ressources humaines et le renforcement de ses capacités sont essentiels au succès des efforts visant à améliorer la cybersécurité. Les gouvernements et les institutions doivent disposer de personnels formés aux problèmes techniques et juridiques complexes que posent la cyber-criminalité et la protection des infrastructures essentielles. Les individus doivent comprendre les technologies et être capables de faire face aux incidents et aux menaces.

Il est important que les gouvernements élaborent des stratégies d'éducation et de formation globales et prospectives. Les populations devraient pouvoir acquérir les compétences nécessaires pour participer activement à la résolution des cyber-menaces et les comprendre. Les individus devraient être impliqués dans la définition de leurs propres besoins et dans l'élaboration de programmes pour satisfaire ces besoins. Ces efforts devraient intégrer l'éducation pratique à court terme ainsi que l'éducation et la formation professionnelle à long terme aussi bien pour le secteur public que le secteur privé.

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.

PRINCIPE STRATEGIQUE II

Environnement favorable (cadres juridiques, réglementaires, politiques et de plaidoyer)

Le cyberspace est, par nature, un phénomène mondial et les problèmes tels que la protection de la confidentialité, la confiance des usagers, la gestion des noms de

domaines, la facilitation de l'e-commerce, la protection des droits de propriété intellectuelle, les solutions de sources non protégées, etc. devraient être résolus avec la participation active de l'ensemble des parties prenantes.

Pour maximiser les avantages socioéconomiques du cyberspace dans l'ère de la société de l'information, les gouvernements africains doivent créer un environnement de confiance, transparent, non discriminatoire, fondé sur le droit, la réglementation et la politique, capable de promouvoir l'innovation et la compétition technologique sûres et sécurisées, favorisant ainsi les mesures nécessaires pour assurer la cybersécurité pour toutes les parties prenantes intervenant dans le secteur des NTIC, garantir le déploiement de l'infrastructure fiable et le développement de services sans risque.

La lutte contre les cyber-menaces et la protection des infrastructures essentielles reposent sur les cadres juridiques de chaque économie. La cybersécurité est conditionnée, en particulier, par l'adoption effective par chaque économie de lois et réglementations essentielles criminalisant tout type de cyber-menace, de lois procédurales pour garantir que les autorités policières disposent des pouvoirs nécessaires pour mener des enquêtes et poursuivre les délits facilités par la technologie, de lois et politiques favorisant la coopération internationale avec les autres parties dans la lutte contre la criminalité informatique.

Très peu de pays africains ont signé la Convention sur la cyber-criminalité du Conseil de l'Europe, le premier instrument multilatéral élaboré pour traiter des problèmes posés par l'expansion de l'activité criminelle sur les réseaux informatiques. Cette convention met en place une norme minimale de lois essentielles, procédurales et régissant la coopération internationale dont les économies devraient tenir compte dans l'élaboration de cadres juridiques globaux.

Actions prioritaires :

- | |
|---|
| <ul style="list-style-type: none">- 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. |
|---|

PRINCIPE STRATEGIQUE III

Sensibilisation (Renforcement de la confiance, de la sécurité et des directives relatives au cyber-espace)

Pour réaliser pleinement les avantages des NTIC, les réseaux et systèmes d'information devraient être suffisamment solides pour prévenir, détecter et réagir de manière adéquate aux incidents de sécurité. Toutefois, la cybersécurité effective des systèmes d'information est une culture mondiale et doit être développée, prise en main et soutenue à travers toutes les couches de la société de l'information et répondre à la nécessité de préserver la libre circulation de l'information.

Le renforcement de la confiance, de la sécurité et l'élaboration de directives techniques pour aider les États membres et les entreprises africaines à combattre la cyber-criminalité et à protéger les infrastructures vitales est fort déterminant et ces efforts devraient être encouragés, portés à la connaissance du public et, lorsque cela est approprié, coordonnés.

Dans le même ordre d'idées, pour renforcer la confiance dans le cyber-espace et la sécurité de celui-ci, les États membres africains devraient œuvrer à la sensibilisation au sein de leurs sociétés aux risques liés à la cybersécurité et s'atteler à renforcer la coopération internationale à tous les niveaux. Les participants au cyber-espace, que ce soit en tant que concepteurs, propriétaires, opérateurs ou usagers individuels, doivent avoir conscience des menaces et des vulnérabilités et assumer la responsabilité de protéger ce réseau selon leurs fonctions et leurs rôles.

Actions prioritaires :

- | |
|---|
| <ul style="list-style-type: none">- 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 cyber-éthique 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. |
|---|

PRINCIPE STRATEGIQUE IV

Problèmes mondiaux (partage de l'information et initiative de coopération)

Pour combattre avec succès la cyber-criminalité et protéger l'infrastructure d'information, les pays doivent avoir en place des systèmes pour évaluer les menaces et la vulnérabilité et diffuser les alertes et les sous-programmes de

modification requis. En identifiant et en partageant les informations sur une menace avant qu'elle ne cause un préjudice à large échelle, les réseaux de chaque pays peuvent être mieux protégés. L'on devra, en outre, veiller à mettre en place et à maintenir des cellules sur la cyber-criminalité pour se pencher sur les problèmes juridiques et d'investigation qui se posent dans la lutte contre la cybersécurité, à échanger les informations et à apporter assistance à des unités analogues dans d'autres pays.

Le dialogue international sur la cybersécurité à tous les niveaux devrait promouvoir l'échange d'expériences, l'identification et l'application de règles et normes compatibles, le transfert de savoir-faire et l'apport d'assistance technique dans l'optique de remédier au déficit de capacités et de mettre en place des programmes de coopération internationale, en particulier en matière de partage d'informations. Les expériences de partage d'informations et de meilleures pratiques prépareront également la voie à de nouvelles formes de coopération internationale.

Actions prioritaires :

- Apporter un appui aux États membres africains pour mettre en place un système national de réponse pour la sécurité du cyber-espace 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 cyber-criminalité 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.