Une approche globale sur la cyber sécurité et La cybercriminalité en Afrique

Introduction:

1. Au cours de la dernière décennie, le continent africain a connu de grandes réalisations dans la mise en place des infrastructures nécessaires aux technologies de l'information et de la communication (TIC) et un accès croissant et largement répandu d'Internet à haut débits. De moins de 5% en 2007, la pénétration d'Internet a atteint 28% en 2015. Pour combler l'écart entre l'Afrique et le reste du monde, si le taux de croissance actuel est soutenue, l'Afrique devrait avoir des taux d'accès comparables à ceux des pays développés d'ici la prochaine décennie.
2. Il est clair que l'Internet, les réseaux mobiles, les informations connexes et les technologies de communication (TIC) sont devenues des outils indispensables pour les gouvernements, les entreprises, la société civile et les individus à travers le monde. Ces technologies ont favorisé un développement économique considérable, ont augmenté la libre circulation des informations, et ont contribué à des gains réels sur le plan du rendement, de l'efficacité, de la productivité et la créativité à travers l'Afrique.
3. L'utilisation des TIC, en particulier Internet, est devenue une question d'importance stratégique pour les pays. Un Internet libre, ouvert et sécurisé représente un moteur de croissance économique et du développement social qui facilite la communication, l'innovation, la recherche scientifique et la transformation des entreprises. Cependant, l'importante croissance d'Internet a également conduit à de nouveaux défis pour la communauté mondiale. Plus nos sociétés sont interconnectées plus nous devenons vulnérables aux menaces cybernétiques d' où la nécessité de veiller à ce que la sécurité de nos infrastructures critiques soit constamment améliorée afin de maintenir leurs intégrité et leurs fiabilité ainsi que la confiance des utilisateurs.
4. La croissance rapide de l'Internet a également créé de nouvelles opportunités pour commettre des activités de cybercriminalité à grande échelle, qui sont due essentiellement à l'exploitation des vulnérabilités inhérentes d'une technologie en constante évolution. Comme les pays Africains ont de plus en plus accès à Internet haut débit, les questions liées à la cyber sécurité et à la cybercriminalité se posent et il est nécessaire de veiller à ce que les citoyens, les gouvernements et les entreprises soient protégés.
5. Au niveau mondial, l'augmentation des cyber-menaces et des cyber-attaques constituent aujourd'hui une menace pour la paix et la sécurité nationale, régionale et internationale. Les cyber-menaces représentent des préoccupations de sécurité qui affectent toute la planète et ils ont besoin de cadres globaux comme instruments pour promouvoir la sécurité et la stabilité dans le cyberespace. Les Problèmes de cyber sécurité ont une portée plus large que la sécurité nationale et pourtant, peu

d'initiatives en matière de cyber sécurité ont été mises en œuvre au niveau continental. Une stratégie et des cadres nationaux de cyber sécurité basés sur une approche commune et une interprétation commune de la terminologie de base relative aux questions de cyber sécurité sont nécessaires entre les États membres de l'Union africaine.

6. L'Afrique est confrontée à plusieurs défis liés à l'Internet, notamment les dispositions de sécurité pour prévenir et contrôler les risques technologiques majeurs et les risques de fuite de renseignements ; ces menaces ne peuvent être pleinement prises en charge que par le développement d'une solide culture de cyber sécurité, la création de capacités d'intervention robustes et l'adoption de politiques nationales appropriées et efficaces.
7. Compte tenu de la complexité et des dimensions multiples de la Cyber sécurité, la protection et la prévention contre les activités criminelles dans le cyberespace à travers le monde nécessite la coopération et la coordination de toutes les parties concernées aussi bien à l'intérieur et entre les pays. Étant donné l'importance du secteur des TIC et son impact direct et positif sur le développement social et économique des pays Africains, il existe un besoin urgent de développer une approche globale et une stratégie cohérente en matière de cyber sécurité au niveau continental pour promouvoir la paix et la sécurité dans la société de l'information.

II: Contexte:

2.1. La Convention de l'Union africaine sur la cyber sécurité et la protection des données a caractère personnelles.

8. Pour réagir aux difficultés liées à la législation posés par les activités criminelles, commises sur les réseaux de TIC , d'une manière compatible au niveau régionale et continentale et aussi en réponse à la nécessité d'harmoniser les législations dans le domaine de la cyber sécurité et la protection des données a caractères personnelles dans les États membres de l'Union Africaine, la 23 eme Assemblée des chefs d'Etat et des gouvernements de UA, tenue à Malabo les 26-27 Juin 2014 a adopté la "Convention sur la cyber sécurité et la protection des données a caractère personnelles" de L'Union Africaine qui est aussi appelé la « Convention de Malabo ».
9. La convention Malabo a pour objectif la mise en place d'un cadre juridique pour la cyber sécurité et la protection des données personnelles. Elle définit les grandes orientations pour l'incrimination et la répression de la cybercriminalité et des questions connexes. Elle incarne également les engagements existants des États membres de l'Union Africaine au niveau régional, continental et international pour construire une société de l'information qui : respecte les valeurs culturelles et les croyances des nations africaines, garantit un haut niveau de sécurité juridique et technologique, assure le respect de la vie privée et des libertés en ligne, tout en améliorant la promotion et le développement des TIC.
10. La Convention présente les règles de sécurité essentielles pour l'établissement d'un environnement numérique crédible et le renforcement des législations existantes en

matière de technologies de l'information et de communication (TIC) des États membres de l'UA et des Communautés économiques régionales (CER).

2.2. Rappel des recommandations de la première session ordinaire de la STC-CICT- 1

11. Le Premier comité technique spécialisé sur la communication et les technologies de l'information et de la communication (STC-CICT-1) tenue du 31 août au 4 septembre 2015 à Addis-Abeba, Éthiopie a demandé :

- A la Commission de l'Union africaine d'assurer le suivi de la ratification du projet de Convention de l'Union africaine sur la cyber sécurité et la protection des données personnelles par les États membres;

- Aux états membres d'accélérer la signature et la ratification de la Convention de l'UA sur la cyber sécurité et les données à caractère personnel et le développement des législations nationales sur la cyber sécurité et la création, au niveau national et régional, d'équipes d'intervention informatique d'urgence (CERT) et d'équipes de sécurité et d'intervention en cas d'incident informatique (CSIRT) ;

III: Les priorités de la politique de cyber sécurité en Afrique :

3.1 Approche Stratégique:

12. La cyber sécurité est devenu une préoccupation majeure dans le monde entier, la sophistication des cyber-attaques et les dommages financiers causés au pays ont augmenté à un rythme exponentiel. En effet, le rythme rapide de l'innovation dans le secteur des TIC peut se traduit par des lacunes dans les cadres législatifs et réglementaires liés à cyber-sécurité. Le grand défi pour les législateurs est de combler le retard dans la reconnaissance des nouveaux types d'infractions dans le cyberespace et l'adoption d'amendements aux législations applicables.
13. En raison du caractère transfrontalier et international de la cybercriminalité les législations nationales ne peuvent pas être rédigées de manière isolée et les gouvernements doivent chercher à harmoniser les législations nationales, les règlements, les normes et lignes directrices sur les questions de cyber sécurité afin de contribuer à la création de cadres régionaux et internationaux efficaces pour lutter contre la cybercriminalité.
14. Par conséquent, la Cyber sécurité et la cybercriminalité ne peuvent pas être traitées comme n'importe quel autre sujet réglementaire. La Cyber sécurité est devenu une priorité pour tous les gouvernements à travers le monde et beaucoup ont déjà développé des stratégies pour résoudre les problèmes de sécurité émergents liés à l'utilisation criminelle à des fins politiques des TIC. Pour les pays africains, il est nécessaire de considérer la cyber sécurité comme un problème important au niveau national et régional qui affecte leurs souverainetés et leurs sécurités nationales, ainsi que la protection des sociétés et des infrastructures critiques.

15. Une stratégie efficace pour lutter contre la cybercriminalité et les activités malveillantes dans le cyberespace nécessite une approche multipartite où les rôles et les responsabilités des organismes et institutions gouvernementaux et les autres partenaires potentiels doivent être définis au plus haut niveau. De plus, la stratégie doit refléter les valeurs culturelles et les croyances des Nations africaines; elle doit aussi avoir un ensemble clair de principes qui aident à encadrer les décisions sur la façon d'identifier, de gérer et d'atténuer les risques liés à la cyber sécurité.
16. Par ailleurs , la complexité et la dimension internationale des politiques de cyber sécurité ainsi que les discussions en cours et les débats sur les politiques internationales et régionales liées aux questions de cyber sécurité et cybercriminalité pour la création d'un cadre mondial devraient être prises en compte lors de l'élaboration des législations nationales et régionales tout en tenant compte des instruments internationaux et les meilleures pratiques.

3.2 Cadre National de Cyber Sécurité:

17. Le cyberespace est devenu une composante essentielle de la société moderne. Cependant, ses bénéfices sont accompagnés de menaces. Le nombre croissant de cyber-incidents signalés exige que les gouvernements procurent des réponses stratégiques pour contrer les cyber-menaces.
18. Les gouvernements Africains sont à de différents niveaux pour l'établissement d'instruments politiques et de cadres législatifs. Pour la majorité, le manque de savoir-faire en matière de cyber-sécurité pour surveiller et défendre leurs réseaux nationaux et le manque de compétence pour développer des cadres juridiques pour lutter contre la cybercriminalité ainsi que le manque de ressources financières sont les principaux facteurs qui contribuent à rendre les pays africains vulnérables aux incidences de cyber-terrorisme et de cyber espionnage.
19. Bien que de nombreux pays aient proposé des législations, le niveau de déploiement des systèmes de sécurité à la fois dans le secteur privé et le secteur public reste faible. Pour promouvoir la culture de la cyber sécurité et mettre en place des mesures efficaces visant à renforcer la confiance et la sécurité dans l'utilisation des réseaux de télécommunication / TIC, les États membres de l'UA doivent accélérer la ratification et la transposition des dispositions de la Convention de l'UA dans leurs cyber-législations nationales.
20. Au niveau continental, il est nécessaire d'atteindre un haut niveau de politiques harmonisées , de législations et des procédures réglementaires visant à prévenir et à lutter contre l'utilisation illicite de l'Internet et des TIC.
21. Au niveau national, les États membres peuvent envisager les mesures suivantes:
    i. Élaborer des stratégies nationales de cyber-sécurité, conformément aux normes et pratiques internationales et en tenant compte de la convention de l'UA sur la cyber sécurité et la protection des données à caractère personnelles ;

ii. Soutenir la création d'une gouvernance nationale pour la cyber sécurité et la définition des rôles et responsabilités de toutes les parties concernées ;
iii. Élaborer les cadres juridiques et réglementaires et prendre des dispositions spécifiques relatives au cyber législations ;
iv. Améliorer les capacités techniques pour surveiller et défendre les réseaux nationaux ;
v. Développer une équipe nationale d'intervention informatique d'urgence (CERT) et /ou une équipes nationale de sécurité et d'intervention en cas d'incident informatique (CSIRT) ;
vi. Encourager le partage efficace des informations et des preuves numériques de manière bilatérale ou multilatérale.
vii. Protéger les institutions pertinentes et l'intégrité des infrastructures nationales critiques contre les menaces et les attaques susceptibles de mettre en danger leur survie et leur efficacité;
viii. Fournir et à long terme un programme de renforcement des capacités et assistance technique afin de renforcer les autorités nationales pour combattre la cybercriminalité et faire face aux questions liées à la cyber sécurité.
ix. Les États membres qui ne disposent pas des accords d'assistance mutuelle dans la cybercriminalité devront s'engager dans la signature d'accords d'entraide judiciaire.
x. Désigner un point focal pour faciliter la coopération régionale et internationale

3.3 : lutte contre tous types de cybercriminalité au niveau continental:

22. Les cyber menaces se multiplient rapidement et sont de plus en plus sophistiquées. Pour renforcer la prévention et la lutte contre la cybercriminalité, les pays africains doivent intensifier, en toute urgence, les efforts visant à lutter efficacement contre toutes sortes d'activités criminelles dans le cyberespace africain et cela à travers une approche multi- parties prenantes et de manière intégrée et globale, impliquant les gouvernements, l'industrie, la communauté universitaire, la société civile et les organisations.
23. Pour contrer l'utilisation criminelle des réseaux Internet et des TIC, les gouvernements africains peuvent envisager l'élaboration et l'adoption de législations complètes et efficaces pour améliorer les composantes de la cybercriminalité dans la stratégie nationale sur cyber sécurité. De plus, les législations devraient soutenir les efforts nationaux visant à assurer une justice pénale efficace pour remédier aux infractions liées aux mauvais usages de l'internet et des TIC.
24. Pour lutter contre la cybercriminalité et pouvoir enquêter de façon efficace sur les délits cybernétiques au niveau national, les gouvernements peuvent envisager les mesures suivantes:

a. Appliquer les lois pénales déjà existantes au niveau national et les adapter à la réalité de l'environnement numérique pour lutter efficacement contre tous types de cyberattaques et toutes formes de la cybercriminalité.
b. Renforcer les capacités des autorités judiciaires , tels que : les procureurs , les juges et les services chargés de l'application des lois afin de leur permettre d'enquêter efficacement, de poursuivre et de juger les cas de cybercriminalité ainsi que d'autres infractions liées à la collecte de la preuve électronique et d' expertise informatique.
c. Améliorer les procédures d'enquête sur la cybercriminalité, la manipulation de la preuve électronique et la coopération entre les différents organismes chargés de l'application des lois.
d. Faciliter le partage de l'information entre le public et le privé et favoriser la coopération entre les services chargés de l'application de la loi et les fournisseurs de services Internet (ISP).
e. Évaluer régulièrement l'efficacité des législations et la stratégie de lutte contre la cybercriminalité et tenir des statistiques en la matière.

3.4 Protection des Données Personnelles (PDP)

25. Dans le monde numérique d'aujourd'hui, les données personnelles sont devenues le carburant qui alimente beaucoup d'activités en ligne. Chaque jour, une grande quantité de données sont collectées, stockées et transmises à travers le monde.
26. Étant donné que de plus en plus d'activités économiques et sociales se déplacent dans l'espace numérique, l'importance de la protection des données personnelle et celle de la vie privée en ligne est reconnue comme essentielle pour le développement de l'économie numérique.
27. Dans le même temps, le volume des flux transfrontaliers de données, plus précisément les données personnelles sont en augmentation chaque année, faisant ainsi des réglementations sur la protection des données un élément central des transactions électroniques.
28. En plus des lois types sur la protection des données personnelles mises au point au niveau régional et au sein des communautés économiques régionales (CER), la convention de l'UA exprime une partie de la pertinence de la protection des données dans l'environnement numérique et souligne l'importance d'assurer une protection efficace des données personnelles et la vie privée en ligne et de garantir que toute forme de traitement des données dans les États Membres de l'Union Africaine respecte les libertés et les droits fondamentaux des personnes physiques.
29. Au niveau continental, la convention de Malabo vise à créer un système harmonisé de traitement de données et de déterminer un ensemble de règles communes pour régir le transfert transfrontalier des données personnelles afin d'éviter des approches réglementaires divergentes entre les États membres de l'UA.

30. La collecte, l'enregistrement, le traitement, le stockage et la transmission des données personnelles doivent être menées régulièrement, de façon équitable et non-frauduleuse. Dans tous les cas le traitement des données personnelles doit être effectué dans le respect du principe de transparence et de confidentialité. Pour ce faire, chaque État Membre devrait élaborer un cadre juridique et institutionnel pour la protection des données personnelles et devrait établir une autorité nationale de protection sous forme d'autorité administrative indépendante chargée de veiller à ce que tout traitement de données à caractère personnel soit effectué conformément aux dispositions de la Convention de Malabo
31. Toute interconnexion des fichiers de données personnelles devrait être soumise à des mesures de sécurité appropriées pour empêcher que ces données soient altérées, détruites ou accessibles par des tiers personnes non autorisés. Les autorités de protection nationales devraient veiller à ce que les TIC ne constituent pas une menace pour les libertés publiques et la vie privée des citoyens en réglementant les fichiers de traitement des données, particulièrement les fichiers relatifs aux données sensibles , en établissant des mécanismes de coopération avec les autorités de PDP des pays tiers et aussi en participant aux négociations internationales sur la protection des données personnelles (PDP).
32. La plupart des pays africains ne disposent pas encore de législations sur la PDP, pour assurer la confidentialité en ligne et de la protection des données personnelles et aussi permettre aux citoyens africains d'utiliser les TIC et Internet pour leur développement socio-économique (santé, éducation, gouvernance, etc.) en toute sécurité.

    Pour sécuriser le cyberespace et résoudre le problème de la protection des données au niveau continental, il est nécessaire de mettre en œuvre la convention de l'UA et de mettre en place des cadres juridiques et institutionnels au niveau national.

3.5 Renforcement des capacités et sensibilisation:

33. Pour créer un climat de confiance en ligne et permettre le partage ouvert des connaissances, d'informations et d'expertises entre les citoyens africains, il est indispensable de sécuriser les réseaux et les systèmes d'information et de promouvoir la culture de la cyber-sécurité entre tous les acteurs, à savoir les gouvernements, les entreprises et la société civile qui se développent, s'approprient, gèrent, opérationnalisent et utilisent les systèmes et réseaux d'information.
34. Pour la protection de l'infrastructure critique et pour permettre au pays de répondre au nombre croissant de cyber-menaces en particulier dans les secteurs critiques, il est nécessaire de construire des compétences nationales pour la cyber sécurité. Le développement d'une main-d'œuvre compétente et hautement qualifiée est essentiel pour réduire les cyber-risques nationaux. Chaque employé du gouvernement ou des entreprises devrait avoir des responsabilités en matière de cyber sécurité pour assurer que les systèmes et les réseaux sont protégés de manière adéquate.

35. Alors qu'il est important de développer de fortes compétences en matière de cyber sécurité et de sensibiliser les professionnels, les États membres devraient aussi s'engager à assurer le leadership pour le développement de la culture de la cyber-sécurité au sein des utilisateurs finaux et contribuer à sensibiliser et à diffuser l'information au public.
36. La stratégie nationale doit identifier un organisme ou une entité pour la sensibilisation du public sur les nombreuses menaces liées à l'utilisation des ordinateurs .Cela devrait inclure le renforcement des capacités des utilisateurs individuels en fournissant une formation et une éducation sur les mesures qu'ils peuvent prendre dans leur vie de tous les jours pour assurer l'utilisation en toute sécurité du cyberespace.
37. Dans le cadre de la promotion de la culture de la cyber sécurité, les États membres peuvent adopter les mesures suivantes:

i. Élaborer et mettre en œuvre des programmes et des initiatives pour sensibiliser sur la sécurité des systèmes et réseaux d'utilisateurs au sein des institutions nationales;
ii. Encourager le développement d'une culture de la cyber sécurité dans les entreprises et favoriser la participation de la société civile;
iii. Lancer un programme complet et détaillé de sensibilisation nationale, y compris des campagnes de sensibilisation du grand public et des mesures préventives à tous les niveaux pour atténuer les Cyber risques au niveau des utilisateurs d'Internet soit les petites entreprises, les écoles et les enfants.
iv. Déployer des efforts nationaux en matière de formation et d'éducation en introduisant des programmes d'études de cyber sécurité par exemple sous forme de cours dans les universités et les établissements universitaires.

3.6 Renforcement de la coopération régionale et internationale:

38. Le monde d'aujourd'hui est globalisé, complexe et surtout dominé par l'utilisation intensive des outils TIC en termes d'infrastructures et de services. La dépendance croissante aux TIC et l'interconnexion des infrastructures critiques a introduit de nouvelles vulnérabilités pour les sociétés et fait de la sécurité du cyberespace une priorité pour le fonctionnement des États modernes.

39. De nos jours, les technologies de l'information sont devenues le dénominateur commun de toutes les disciplines; tout le monde utilise le même Internet pour des applications personnelles et professionnelles, pour la santé, l'éducation, l'énergie et même la sécurité. Cela a augmenté le niveau de complexité de la façon dont nous pouvons sécuriser, protéger et défendre nos activités vitales menées aux niveaux politiques, économiques, sociaux et individuels.

40. Dans ce contexte, il est nécessaire de comprendre que les cyber-risques sont devenus une urgence planétaire amplifiant les risques traditionnels tels que le terrorisme. Par conséquent, il y a une nécessité d'agir pour relever les défis de sécurité de l'ère numérique.

41. Alors qu'un cyberespace sécurisé nous offre de nombreuses possibilités, il est rapporté que plus de 100 États développent des capacités du cyberespace militaires, une perspective qui menacent à la fois la sécurité nationale et internationale .Les aspects clés des outils informatiques résident dans la difficulté d'attribuer une attaque à ses auteurs ou identifier les commanditaires et aussi la double utilisation de la technologie.

42. La coopération internationale sur les questions de Cyber sécurité se réfère aux efforts intergouvernementaux visant à prévenir l'utilisation des TIC de manière à affecter la paix et la sécurité internationales. Il y a actuellement un débat international sur l'établissement d'une réglementation et d'un code de conduite ou des normes de comportement des États dans le cyberespace et sa relation à la sécurité internationale.
43. Afin de promouvoir la stabilité internationale dans le cyberespace mondial et parvenir à une compréhension commune sur les questions du cyberespace basées principalement sur la transparence et la confiance en ligne, le Groupe d'experts gouvernementaux des Nations Unies (UNGGE), a convenu en Juin 2013, sur un rapport de consensus où il est dit que le droit international, en particulier la Charte des Nations Unies, est applicable dans le cyberespace. En outre, le groupe a convenu que les mesures de renforcement de la confiance et la communication de haut niveau et le partage de l'information en temps réel peut accroître la confiance et l'assurance entre les États. Le groupe a également souligné l'importance du renforcement des capacités pour améliorer la coopération internationale dans la protection du cyberespace et a réaffirmé l'importance de l'édification d'un cyberespace mondial ouvert, libre et sécurisé car c'est un catalyseur pour le développement économique et social.

44. Conformément aux discussions internationales, une réponse efficace aux problèmes complexes de Cyber sécurité ne peut pas être mis en œuvre efficacement à un niveau purement local; elle exige une coopération transnationale en développant une culture de la cyber sécurité appropriée et par l'amélioration des mesures complémentaires et cohérentes d'une manière holistique et globale. Au niveau continental, il est essentiel de promouvoir l'échange d'informations et la communication entre les pays notamment au niveau de la politique étrangère (pas seulement technique) , développer des capacités de cyber diplomatie et de la tenue de consultations en vue de réduire les risques d'utilisation criminelle des TIC notamment le cyber espionnage et le Cyber terrorisme. Une approche continentale harmonisée sur les principales

questions de cyber sécurité est nécessaire du point de vue stratégique pour renforcer la coopération régionale, continentale et internationale qui est nécessaire pour mener les enquêtes et les poursuites transfrontalières de la cybercriminalité.

45. L'approche globale et harmonisée doit fournir aux pays africains une compréhension claire des risque et des vulnérabilités des technologies intelligentes et l'internet des objets (IOT) et aider les pays à créer un Cyber environnement sécurisé et résilient en fournissant une assistance à l'élaboration des éléments clés d'un cadre national de cyber sécurité nécessaires pour prévenir et lutter contre toutes les activités malveillantes dans les réseaux Internet.

46. Pour lutter contre les cyber-attaques mondiales, la cybercriminalité et les utilisations abusives ou inappropriées des réseaux TIC et en phase avec les mécanismes de coopération internationale et les meilleures pratiques déjà existants, la Commission de l'Union Africaine, les communautés économiques régionales et les institutions spécialisées de l'UA peuvent adopter les mesures suivantes:

i. Développer des mécanismes régionaux pour partager les expériences et les meilleures pratiques sur les questions de cyber sécurité entre les États Membres de l'UA pour renforcer la coopération régionale et internationale.
ii. Développer des équipes d'intervention d'urgence aux incidents Informatiques (CERT / CIRT); et promouvoir l'échange formel et informel de l'information.
iii. Travailler avec les États Membres pour l'harmonisation des lois sur la cybercriminalité au niveau régional et continental et renforcer la coopération en matière d'application des lois à la fois aux niveaux régional et continental.
iv. Concevoir un modèle de renforcement des capacités en matière de cyber sécurité qui prend en considération tous les aspects (politique, technologie, développement des compétences ...) et qui peut être facilement adapté aux besoins des États membres.
v. Soutenir les organisations inter-gouvernementales et les entreprises privées pour développer des normes et standards pour l'échange d'informations au cours de l'enquête et des poursuites des cybers criminels transnationaux.

vi. Encourager les États Membres de l'UA à développer des capacités en matière de cyber diplomatie et à participer à des discussions menées au niveau international comme le Groupe d'experts gouvernementaux des Nations Unies.

IV: <u>Conclusions and Recommandations</u>:

47. L'utilisation croissante des technologies de l'information et de la communication et l'augmentation de l'accès à Internet pour la prestation et délivrance de services tels que l'administration en ligne, la banque, la santé ou l'éducation a inévitablement

conduit à l'émergence de nouveaux risques liés aux cyber-attaques qui se produisent rapidement et qui se propagent à travers le monde en quelques minutes indépendamment des frontières, la géographie, ou les juridictions nationales. L'Afrique représente 10% des cybers incidents mondiaux.

48. La cybercriminalité ne peut être vaincue par aucune loi ou convention seule, il est devenu clair que la collaboration de toutes les parties prenantes dans la gouvernance et le fonctionnement de l'Internet est nécessaire pour préserver la sécurité et la confidentialité des utilisateurs d'Internet. Un environnement numérique sûr et sécurisé est une responsabilité partagée et collective au sein du continent, et c'est une condition nécessaire pour tirer profit des avantages de la transformation numérique de l'Afrique et aussi pour soutenir son impact positif sur le développement humain et économique.

Recommendations:

49. Au niveau National:

a. Accélérer la ratification et la mise en œuvre de la Convention de l'UA sur la cyber sécurité et la protection des données personnelles (1).
b. Élaborer une stratégie nationale sur la cyber sécurité et un plan d'action opérationnel pour la lutte contre la cybercriminalité et le cyber terrorisme.
c. Rédiger ou revoir les Cyber législations existantes pour criminaliser toutes les infractions liées à l'usage illicite des TIC (1)
d. Créer une équipe nationale de prévention et de réaction d'urgence aux incidents Informatique (CERT) pour la surveillance de réseaux et l'échange de bonnes pratiques et une collaboration efficace (1)
e. Mettre en place un cadre juridique et institutionnel pour la protection des données à caractère personnel et établir l'autorité nationale de protection.
f. Développer et promouvoir une solide culture de cyber sécurité qui reconnaît et répond efficacement aux menaces et aux défis mondiaux liés à l'Internet et réseaux mobiles interconnectés et technologies connexes.
g. Développer des capacités en cyber diplomatie et participer aux discussions menées au niveau international comme le Groupe d'experts gouvernementaux des Nations Unies.

50. Au niveau régional :

a. Créer des centres de Cyber sécurité régionaux dans le but de servir de catalyseurs pour renforcer la coopération régionale, la coordination et la collaboration.

b. Développer des équipes d'intervention d'urgence aux incidents informatiques régionaux (R-CERT / R-CIRT); et promouvoir l'échange formel et informel d'informations entre les pays (1).

c. Travailler avec les Etats Membres pour l'harmonisation des lois sur la cybercriminalité au niveau régional et continental et renforcer la coopération dans l'application des lois à la fois aux niveaux régional et continental.

Au niveau continental:

a) Développer une approche globale et harmonisée sur les principales questions de cyber sécurité et promouvoir la création d'un Cyber environnement sécurisé, robuste et résilient au niveau continental.

b) Promouvoir le dialogue au sein des parties concernées par la cyber sécurité en Afrique et coordonner toutes les initiatives liées à la cyber sécurité.

1: Une partie des recommandations de la première session ordinaire de la STC-CICT-1