SOMMET DE LA CYBERSECURITE-LOME 2022
23 ET 24 MARS 2022

DECLARATION DE LOME SUR LA CYBERSECURITE ET LA LUTTE CONTRE LA CYBERCRIMINALITE
REV.1

NOUS, Ministres réunis dans le cadre du Sommet de la Cybersécurité-Lomé 2022, à Lomé (Togo), co-organisé par la République Togolaise et la Commission Économique des Nations Unies pour l'Afrique (CEA) les [23 et 24] mars 2022 ;

AYANT *A* L'ESPRIT la Déclaration Assembly/AU/Decl.11(XIV) sur les Technologies de l'information et de la Communication en Afrique « *Défis et perspectives pour le développement* », adoptée lors de la 14ème Session ordinaire de la Conférence ***des Chefs d'État et de Gouvernement*** de l'Union Africaine, tenue à Addis-Abeba, en Éthiopie, du 31 janvier au 02 février 2010 ;

CONSID*E*RANT les travaux menés par l'Organisation des Nations Unies, notamment dans le cadre de la Résolution ***RES/74/247***, relative à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles adoptée par son Assemblée générale le 27 décembre 2019, qui a décidé de l'établissement d'un comité intergouvernemental spécial d'experts ayant pour mission d'élaborer une Convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ;

CONSID*E*RANT les travaux menés par l'Union Internationale des Télécommunications, ***couronnés par*** le lancement en 2007 d'un cadre de coopération internationale destiné à accroître la confiance et la sécurité dans la société de l'information, le « *Global Cybersecurity Agenda* » (Programme mondial cybersécurité) ainsi que la rédaction en 2021 de***s*** « *Draft Guidelines* » (Lignes Directrices) pour sa mise en œuvre ;

RAPPELANT l'importance et la multiplication des initiatives africaines en matière de cybersécurité et de lutte contre la cybercriminalité, et notamment la rédaction par la Commission de l'Union Africaine et l'Internet Society (ISOC) des Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique du 30 mai 2017 et la définition par AFRIPOL (*African Union Mechanism for Police Cooperation*) d'une Stratégie en matière de lutte contre la cybercriminalité ;

RAPPELANT la Décision EX.CL/Dec.987(XXXII) sur les Rapports des Comités Techniques Spécialisés, adoptée lors de la 32ème Session ordinaire du Conseil exécutif de l'Union Africaine, tenue à Addis-Abeba, les 25 et 26 janvier 2018 ;

RAPPELANT la Déclaration AU/STC-CICT-3/MIN/Decl., dit***e*** « *Déclaration de Charm el-Cheick »*, adoptée lors de la 3ème Session ordinaire du Comité Technique Spécialisé sur la Communication et les Technologies de l'Information et de la Communication, tenue à ***Charm el-Cheick (Egypte),*** les 25 et 26 octobre 2019 ;

RAPPELANT la Décision Assembly/AU/Dec.755(XXXIII) sur le 5ème Rapport du Conseil de paix et de sécurité de l'Union Africaine sur la mise en œuvre de la feuille de route principale de l'Union Africaine sur les étapes pratiques en vue de faire taire les armes en Afrique d'ici 2020, et notamment son point 17, adoptée lors de la 33ème Session ordinaire du Conseil exécutif de l'Union Africaine, tenue à Addis-Abeba, les 09 et 10 février 2020 ;

CONSIDERANT que les technologies de l'information et de la communication et la transformation numérique constituent un formidable levier de croissance pour le continent africain et peuvent contribuer à la réalisation de la vision et des objectifs de l'Agenda 2063 de l'Union Africaine et des ***O***bjectifs de ***D***éveloppement ***D***urable ***(ODD)*** des Nations ***U***nies ;

CONSTATANT que la pandémie de Covid-19 a révélé l'urgence pour le continent africain de poursuivre sa transformation numérique, en particulier à travers le développement et la sécurisation des activités et services en ligne, et notamment en matière de santé, d'éducation, de commerce, d'agriculture, d'administration électronique ou encore de services financiers ;

PRENANT EN COMPTE l'accélération de la transformation numérique en cours sur le continent africain, en particulier l'émergence de services innovants proposés uniquement sous forme dématérialisée, dans un contexte de faible sensibilisation des utilisateurs et des acteurs aux risques en matière de cybersécurité et de cybercriminalité ;

RECONNAISSANT que la sécurité de l'Internet, des infrastructures et équipements numériques et des systèmes d'information est essentielle au développement de l'écosystème numérique africain ;

NOTANT que la cybercriminalité affecte tous les acteurs de la société de l'information, tant public que privé, et l'impact négatif de son coût sur les économies africaines;

NOTANT avec satisfaction les efforts du Centre d'excellence de la Commission économique pour l'Afrique pour l'identité numérique, le commerce et l'économie pour renforcer les capacités et la résilience des État membres à garantir la confiance numérique dans un univers en mutation rapide par la mise en place de stratégies nationale de cyber sécurité

D*E*SIREUX d'œuvrer à l'attractivité de leurs économies et au développement de leur écosystème numérique en veillant à la mise en place de solutions de protection et d'accompagnement adaptées à la transformation numérique en cours et aux contextes locaux ;

CONSCIENTS qu'un engagement politique au plus haut niveau, à travers notamment l'élaboration de stratégies globales, la définition de politiques volontaires et la consécration de cadres juridiques nationaux efficaces est indispensable à la prévention, la limitation et la répression des risques et incidents en matière de cybersécurité et de cybercriminalité ;

CONVAINCUS que l'existence de règles contraignantes et la mise en place d'organes dédiés en matière de numérique, de cybersécurité et de lutte contre la cybercriminalité est une condition indispensable au renforcement de la confiance des citoyens, entreprises et administrations dans l'économie numérique et au développement des investissements dans le secteur ;

CONSCIENTS que la mise en œuvre d'actions concertées à l'échelle internationale et régionale permettrait de se doter de moyens efficaces de diagnostic, de contrôle et de protection en matière de cybersécurité et de lutte contre la cybercriminalité, y compris à travers la mise en place de dispositifs de partage de bonnes pratiques, de diffusion des connaissances et de réponses concertées et coordonnées aux risques et incidents susceptibles d'affecter le secteur de l'économie numérique ;

NOUS NOUS ENGAGEONS PAR LA PR*E*SENTE *A* :

1. **SIGNER ET RATIFIER** la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel dite « *Convention de Malabo* », adoptée le 27 juin 2014 par la vingt-troisième Session ordinaire de la Conférence ***des Chefs d'État et de Gouvernement*** de l'Union Africaine à Malabo, en Guinée Équatoriale, afin de permettre l'essor d'un cyberespace africain sûr ;

2. **METTRE EN PLACE ET VEILLER *A* LA MISE EN ŒUVRE EFFECTIVE** d'un cadre légal et réglementaire spécifique à la cybersécurité et à la lutte contre la cybercriminalité ainsi que les organes de régulation qui permettent notamment de susciter la confiance des investisseurs, de favoriser l'adoption des activités et services numériques par les utilisateurs et*,* plus généralement*,* d'accélérer la transformation numérique, en s'appuyant notamment sur :

    a. La stratégie de transformation numérique pour l'Afrique (2020-2030)

    b. Les lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique du 30 mai 2017 ***élaborées*** conjointement par l'Internet Society (ISOC) et la Commission de l'Union Africaine ;

    c. Les décisions et déclarations adoptées par la Conférence de l'Union Africaine, le Conseil exécutif et le Comité Technique Spécialisé sur la communication et les technologies de l'information et de la communication ;

    d. Les meilleures pratiques internationales, notamment celles qui peuvent être recommandées par l'Organisation des Nations Unies et l'Union Internationale des Télécommunications.

3. **DEVELOPPER** des stratégies et politiques de cybersécurité qui soient stables, prospectives et adaptées aux contextes et aux évolutions du secteur de l'économie numérique, avec notamment :

    a. La mise en place d'actions de sensibilisation aux risques relatifs à l'usage du numérique auprès des populations**,** notamment les catégories les plus vulnérables, des entreprises ainsi que des administrations ;

    b. La mise en place de formations universitaires et professionnelles et des compétences numériques pour lutter contre la pénurie de main d'œuvre en cybersécurité et assurer la formation de l'ensemble des acteurs des écosystèmes numériques ;

    c. Le développement de mesures incitatives en faveur des entrepreneurs du secteur, y compris sur le plan financier et fiscal, afin de favoriser l'émergence d'acteurs africains de la cybersécurité ;

    d. Le développement des partenariats publics-privés dans la mise en place des écosystèmes de cybersécurité afin d'avoir des modèles sécuritaires et économiques viables et efficaces.

4. **ÉTABLIR** un cadre permettant de lutter efficacement contre la cybercriminalité et promouvoir une culture de cybersécurité, avec notamment :

    a. La création et l'opérationnalisation des autorités, agences et équipes dédiées à la cybersécurité et, le cas échéant, le renforcement de leurs moyens humains, financiers, techniques et organisationnels ;

    b. La mise en place de structures de gouvernance permettant l'association d'experts interdisciplinaires (diplomatiques, militaires, juridiques milieu universitaires, société civile, etc.) aux prises de décisions en matière de cybersécurité et de lutte contre la cybercriminalité ;

    c. La mise en place d'équipes dédiées au recensement et à la coordination des incidents de cybersécurité***,*** tels que des Security SIEM (*Information and Event Management*) ou SOC (*Security Operations Center*) ainsi qu'aux réponses à apporter aux incidents de cybersécurité***,*** tels que des CSIRT (*Computer Security Incident Response Team*) ou encore des CERT (*Computer Emergency Response Team*).

    d. Soutenir des initiatives telles que le Réseau des femmes africaines dans la cybersécurité (NAWC) en amplifiant les voix et les contributions des femmes dans ce domaine critique du cyber développement de l'Afrique

5. **RENFORCER** la coopération africaine en matière de cybersécurité et de lutte contre la cybercriminalité en :

    a. Encourageant la signature et la ratification de la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel de 2014 par l'ensemble des États africains ;

    b. Promouvant auprès des autres membres de l'Union Africaine la création d'un Organe de coopération régionale et d'assistance mutuelle en matière de cybersécurité et de lutte contre la cybercriminalité ;

    b (bis). Promouvant auprès des régions la création d'un Organe de coopération régionale et d'assistance mutuelle en matière de cybersécurité et de *lutte contre la cybercriminalité*

    c. Multipliant les initiatives régionales et internationales permettant aux autorités et agences du secteur compétentes en matière de cybersécurité de renforcer leurs capacités, notamment à travers la mise en place de formations et le partage de leurs expériences respectives.

    d. Soutenir les efforts de la cyberdiplomatie africaine pour promouvoir la coopération régionale et internationale et s'engager dans l'établissement de normes au niveau international.

NOUS DEMADONS a la Commission Économique des Nations Unies pour l'Afrique d'appuyer les états Africains à mettre en œuvre la Déclaration de Lomé.

Fait à Lomé *(Togo)*, le 23 mars 2022