Priorités sur le renforcement des capacités en matière de cybersécurité en Afrique : Document sur les résultats de l'Édition 2022 de l'AfriSIG et de la Consultation multipartite sur la participation africaine au Groupe de travail à composition non limitée.

Lilongwe, du 16 au 18 Juillet 2022

VERSION FRANCAISE

Cette compilation contient deux versions du document sur les résultats élaboré et approuvé lors de la consultation multipartite à Lilongwe du 16 au 18 juillet 2022. La version intégrale est fournie en haut de ce document, avec les contributeurs listés à la fin de la version intégrale. Sous la version intégrale, une version résumée du document est annexée.

Table de matières

Version intégrale

Préambule

La cybersécurité est un catalyseur essentiel de la transformation et du développement socio-économiques. Il est donc important que l'Afrique identifie et hiérarchise les besoins spécifiques en matière de renforcement des capacités en matière de cybernétique, afin de réaliser son programme de transformation numérique. Certains de ces domaines prioritaires pour le renforcement des capacités cybernétiques comprennent : la gouvernance, l'élaboration des politiques, y compris l'harmonisation des politiques, de la législation et de la réglementation, les outils techniques et l'infrastructure, la compréhension, l'innovation, la planification et la recherche et développement. En outre, les acteurs étatiques et non étatiques en Afrique ont besoin de davantage de capacité pour être en mesure de participer efficacement et de manière cohérente aux processus pertinents des Nations Unies tels que le Groupe de travail à composition non limitée (GTCNL) et d'autres initiatives internationales connexes en matière de cybernétique et de sécurité.

Le renforcement des capacités est essentiel pour améliorer la qualité et la substance des discussions des États africains qui visent à agir et à influer sur les règles, normes et principes mondiaux pour un comportement responsable des États dans le cyberespace, et l'établissement de la résilience et de la culture de la cybersécurité. L'engagement multipartite à tous les niveaux, mondial, régional, sous-régional et national - mis en œuvre de manière inclusive, transparente et responsable - devrait être au cœur de l'approche africaine de la cybersécurité, en particulier dans l'élaboration de politiques, de lois et de stratégies de cybersécurité centrées sur l'humain et conscientes des droits humains.

Ces stratégies devraient être fondées sur le fait que les menaces à la cybersécurité peuvent être complexes et en constante évolution ; d'où la nécessité d'un apprentissage continu et d'un renforcement permanent des capacités. Cela permettrait aux acteurs étatiques d'être mieux préparés à répondre aux cybermenaces et aux cybercriminels tout en restant au fait de l'évolution des normes, standards et lois internationaux. De telles approches amélioreront donc la posture de l'Afrique en matière de cybersécurité et favoriseront l'investissement, le commerce et la confiance du public dans les TIC dans les États africains.

Ce document a été élaboré en tant que contribution au Groupe de travail à composition non limitée sur les TIC lors d'une consultation multipartite qui s'est tenue à Lilongwe, au Malawi, du 16 au 18 juillet 2022, juste avant le 11e Forum africain sur la gouvernance de l'internet. La consultation, liée à la 10e École africaine sur la gouvernance de l'internet[1], organisée par l'Association pour le progrès descommunications et le Global Partners Digital, a réuni un groupe diversifié de personnes issues de gouvernements africains, d'organismes d'application de la loi et de sécurité, de la Commission de l'Union africaine, d'organisations de la société civile, de groupes de défense des droits numériques et des médias, et d'experts en cybersécurité. Les participants à la consultation qui ont contribué au présent document à titre individuel sont énumérés dans l'annexe à la fin du document.

1 https://afrisig.org/afrisig-2022/

A - Besoins de renforcement des capacités en matière de cybersécurité en Afrique

Besoins généraux de renforcement des capacités, y compris les capacités institutionnelles

1. Il est important que l'Afrique identifie des besoins spécifiques dans le secteur du renforcement des capacités en matière de cybersécurité afin de réaliser son programme de transformation numérique. Les domaines prioritaires pour le renforcement des capacités cybernétiques comprennent : la gouvernance, le renforcement des compétences techniques et politiques, l'innovation, la recherche, la planification et le développement.
2. Le renforcement des capacités est également nécessaire dans la mise en place d'outils et d'infrastructures, ainsi que dans l'harmonisation des lois et des politiques.
3. Les acteurs africains ont également besoin d'une plus grande capacité pour contribuer efficacement aux processus des Nations Unies tels que le Groupe de travail à composition non limitée (GTCNL) et d'autres initiatives mondiales en matière de cybersécurité.
4. Nous recommandons donc d'établir et de renforcer les capacités en Afrique dans les buts suivants :
    a. Élaborer des stratégies, des politiques, une diplomatie et des réglementations progressistes exhaustives en matière de cybersécurité qui mettent l'accent sur la sécurité des individus et des communautés et qui intègrent les normes applicables, les mesures de restauration de la confiance et le droit international.
    b. Harmonisation des cadres juridiques aux niveaux national, sous-régional[2], régional et international.
    c. Mesures visant à assurer la résilience et la protection des Infrastructures Essentielles (IE) et des Infrastructures d'Information Essentielles (IIE).
    d. Prévenir les incidents de cybersécurité et y réagir, y compris par le partage d'informations, la minimisation des risques et l'atténuation des conséquences, aux niveaux national, sous-régional et régional.
    e. Préparation au sein des Équipes d'Intervention en cas d'urgence informatique (CERT) et des Equipes d'intervention en cas d'incident de sécurité informatique (CSIRT) pour mieux prédire et atténuer les menaces à la cybersécurité. Cela comprend une capacité accrue pour communiquer efficacement parmi les équipes d'intervention et entre celles-ci et les autres acteurs étatiques et non étatiques concernés.
    f. Mécanismes transparents de retour d'information pour tous les représentants des États qui participent à des activités sous-régionales, régionales et mondiales afin d'institutionnaliser le partage des connaissances et des informations.
    g. Éducation, plaidoyer et sensibilisation à la cybersécurité aux niveaux national, sous-régional (y compris les communautés économiques régionales) et régional.
    h. Développement de l'expertise en cybersécurité par le biais de pôles d'innovation, de centres d'excellence, de perfectionnement, de recherche et de développement.
    i. Coordination et collaboration aux niveaux national, sous-régional, régional et international entre les États et les acteurs non étatiques, en particulier au niveau sud-sud global.
    j. Normes, cadres de certification et d'accréditation complets et efficaces pour veiller à la protection pour toutes et tous en matière de cybersécurité.
    k. Formation et perfectionnement en matière de cybersécurité qui permettent au personnel de protéger et de sécuriser les infrastructures critiques et les infrastructures d'information critiques, qu'il s'agisse de compétences de base en TIC ou d'aptitudes et compétences avancées en matière de cybersécurité.

2 Dans le contexte africain, il s'agit de sous-régions qui sont également souvent appelées « communautés économiques régionales ».

5. Un développement spécifique des capacités est nécessaire pour renforcer la sensibilisation et les compétences nécessaires pour réorienter une conception traditionnelle de la cybersécurité centrée sur l'État vers une approche centrée sur l'humain et respectueuse des droits humains qui renforce également la cyber-résilience parmi les utilisateurs et utilisatrices.

6. D'autres domaines dans lesquels un renforcement spécifique des capacités est nécessaire :
    a. Mener des évaluations nationales complètes des besoins en cybersécurité afin de déterminer les lacunes et les besoins des différents acteurs et groupes de parties prenantes participant aux processus de cybersécurité.
    b. Élaborer des Mesures de renforcement de la confiance (MRC) pour la région africaine comme cela a été fait dans d'autres régions.
    c. Mise en œuvre et suivi de cette mise en œuvre des normes cybernétiques convenues.
    d. S'engager sur l'applicabilité du droit international et sur la manière de l'opérationnaliser dans le contexte africain.
    e. La convocation efficace d'équipes de négociation possédant l'expertise pertinente en la matière dans un éventail de compétences requises, telles que : les questions techniques ; des compétences en négociation ; le droit international des droits humains ; la diplomatie internationale ; et la rédaction de déclarations et de soumissions écrites ;
    f. La mobilisation des ressources nécessaires pour répondre aux besoins en matière de cybersécurité et mener des consultations nationales de fond avec les acteurs non étatiques dans le cadre de l'élaboration de positions et de stratégies nationales en matière de cybersécurité.

7. En plus des domaines susmentionnés qui impliquent un renforcement des capacités, nous pensons qu'il convient de donner la priorité aux éléments suivants :
    a. Intégrer une formation sensible au genre dans tous les processus visant à renforcer l'expertise en matière de cybersécurité.
    b. Des interventions visant à combler la fracture numérique, en particulier la fracture numérique entre les sexes.
    c. Élaborer, mettre en œuvre et améliorer des cadres de protection des données et de la vie privée qui compléteront les efforts de cybersécurité.
    d. Élaborer et mettre en œuvre des mesures et des mécanismes de notification sur les incidents de cybersécurité afin de permettre la transparence, l'accès à l'information (par exemple via des mécanismes de partage d'informations accessibles au public) et la responsabilité.
    e. Prioriser et budgétiser des ressources financières adéquates pour renforcer la capacité des ressources humaines des institutions responsables en matière de cybersécurité.
    f. Capacités de lutte contre la cybercriminalité, y compris par le biais de la coopération transfrontière et de l'échange de preuves.
    g. Harmoniser les lois à travers l'Afrique et adopter et mettre en œuvre la convention de Malabo.

Besoins spécifiques à des groupes de parties prenantes/acteurs/institutions en particulier

8. Différents acteurs étatiques et non étatiques ont des besoins spécifiques en matière de renforcement des capacités. Il s'agit notamment des éléments suivants :
    a. Entreprises et communauté technique :
        i. Connaissance des normes et standards applicables en matière de cybersécurité et de droits humains ainsi que des instruments

internationaux pertinents en matière de droits humains, y compris ceux initiés par l'industrie ;

ii. Produire des rapports de transparence sur les incidents de cybersécurité et les violations de données.

iii. Comprendre les possibilités qui existent pour s'engager dans les processus politiques multilatéraux et comment s'engager efficacement.

b. Société civile :

i. Comprendre les implications des résultats politiques contraignants et non contraignants au niveau des Nations Unies en ce qui concerne la sécurité de l'État en matière de TIC et les processus d'adoption de ces instruments et de contrôle du respect des dispositions.

ii. Comprendre les possibilités qui existent pour l'engagement dans les processus politiques multilatéraux et la façon de s'engager efficacement.

iii. Capacité à mener des recherches et contribuer au texte et aux commentaires sur la politique de cybersécurité en cours d'élaboration aux niveaux national, sous-régional, régional et international.

iv. Capacité à dialoguer avec les gouvernements de manière à instaurer un climat de confiance.

v. Accéder à des ressources pour participer à et organiser des processus politiques multilatéraux.

c. Professionnels des médias / journalistes

i. Comment suivre les traités et autres instruments et en rendre compte afin que le public puisse digérer l'information et comprendre comment elle se rapporte à eux.

ii. Comment signaler les menaces et les incidents de cybersécurité d'une manière qui sensibilise et favorise l'hygiène numérique.

d. Milieu universitaire

i. Ressources pour la recherche et le partage des résultats sur le long terme afin d'informer et de participer aux processus internationaux (p. ex. ONU) de cyber-diplomatie et de cybersécurité.

e. Gouvernement

i. Comment s'engager avec les acteurs non étatiques de manière à renforcer la confiance et assurer un processus inclusif.

ii. Comprendre la valeur des délégations expertes et multipartites à l'ONU et dans d'autres processus internationaux de cybersécurité et de diplomatie.

iii. Capacité institutionnelle à développer et soutenir la cyber-diplomatie et la politique étrangère numérique.

iv. Comment collaborer et parvenir à un consensus avec d'autres gouvernements à l'intérieur et à l'extérieur de leurs régions (notamment lorsqu'ils ont des intérêts communs).

v. Comment protéger les infrastructures essentielles, les infrastructures d'information essentielles et répondre aux urgences liées aux TIC.

f. Institutions nationales de sécurité

i. Formation sur des questions plus larges de cybersécurité, y compris sur l'application d'une approche multisectorielle centrée sur l'humain et sur l'intersection entre la cybersécurité et les droits humains.

ii. Connaissance des normes et standards applicables en matière de droits humains ainsi que des instruments internationaux, régionaux et nationaux pertinents relatifs aux droits humains.

iii. Comprendre comment aborder et mettre en place des mesures visant à instaurer un climat de confiance (CBM) et comment appliquer le droit international et les normes internationales dans leurs contextes nationaux.

g. Pouvoir judiciaire

i. Comprendre les questions de numérisation et de cybersécurité, les lois et la manière de poursuivre les infractions à la cybersécurité, y compris les infractions transfrontalières.

ii. Sensibilisation et soutien à la participation aux processus et conférences pertinents en matière de traités et de politiques.

iii. Comment tenir compte des droits de la personne dans le jugement des affaires de cybercriminalité.
iv. Gestion des preuves numériques
v. Connaissance des instruments et conventions régionaux, continentaux et internationaux liés à la cybersécurité, ainsi que des normes et des principes.

h. Institutions chargées de l'application de la loi
i. Comprendre les questions plus larges de cybersécurité et que la poursuite des infractions de cybercriminalité pourrait nécessiter des approches nouvelles et spécialisées.
ii. Capacité en criminalistique relative à la cybersécurité.
iii. Capacité spécialisée dans la détection, l'enquête et la poursuite des affaires de cybercriminalité.
iv. Comment tenir compte des droits humains dans les enquêtes sur les affaires de cybercriminalité.

i. Parlementaires
i. Capacité à comprendre les questions de cybersécurité et à sensibiliser leurs électeurs à la cybercriminalité, à la sécurité et à l'hygiène numérique.
ii. Comment travailler à l'harmonisation des lois sur la cybersécurité dans la région.
iii. Comment mieux coopérer avec d'autres parties prenantes pour élaborer des politiques qui correspondent à l'ère numérique, qui sont agiles, flexibles, centrées sur l'humain et qui tiennent compte des droits humains et de l'égalité des sexes.

j. La Commission de l'Union africaine et les Communautés économiques régionales
i. Comprendre les possibilités de participation aux processus de politique multilatérale et la façon de le faire efficacement.
ii. Capacité de coordination technique cohérente et efficace entre les États et les acteurs non étatiques pertinents.
iii. Continuer à soutenir et à donner une plus grande visibilité au Groupe d'experts sur la cybersécurité (AUCSEG) de la Commission de l'Union africaine.

B - Collaboration : au niveau régional et entre acteurs étatiques et non étatiques

9. Des efforts continus, inclusifs et transparents de coopération en matière de renforcement des capacités en cybersécurité et de partage de l'information devraient être établis et renforcés aux niveaux national, sous-régional, régional et international entre et au sein de différents groupes de parties prenantes. La priorité devrait être accordée à la collaboration et au partage de l'information entre :
    a. Gouvernements et diverses parties prenantes non étatiques concernées dans le pays ;
    b. Organisations de la société civile aux niveaux national, régional et continental ;
    c. Organisations de la société civile, organisations techniques et entreprises de l'État, y compris les autorités statutaires de cybersécurité telles que les CERT.

Participation actuelle d'acteurs non étatiques au soutien et/ou à la mise en œuvre d'initiatives de renforcement des capacités dans le contexte du paysage actuel du renforcement des capacités en matière de sécurité des TIC.

10. Les acteurs non étatiques participent largement au renforcement des capacités en matière de sécurité des TIC dans toute l'Afrique. Les domaines où une telle participation se démarque comprennent :
    a. Développer et partager des méthodologies de recherche pour les besoins en cybersécurité et les évaluations de l'état de préparation.
    b. Recherche et sensibilisation par les organisations de la société civile aux normes africaines et internationales en matière de droits humains qui devraient sous-tendre la législation, la politique, l'élaboration et la mise en œuvre de la réglementation en matière de cybersécurité.
    c. Sensibilisation et renforcement des capacités techniques assurés par les acteurs de la communauté technique.
    d. Les organisations de défense des droits humains contribuent à l'élaboration de lois, de politiques et de règlements dans le domaine cybernétique et numérique.
    e. Le Groupe d'experts sur la cybersécurité de la Commission de l'Union africaine (AUCSEG), un groupe multipartite d'experts qui conseille l'UA sur les questions et les politiques de cybersécurité.
    f. Les organisations de la société civile offrent une formation à la sûreté et à la sécurité numériques pour cultiver la cyber-résilience au sein des communautés, ainsi qu'une formation à la sécurité numérique pour les journalistes et les défenseurs des droits humains.
    g. Élaboration de produits de diffusion du savoir et de matériel de formation pour la sensibilisation communautaire et la littératie numérique.
    h. Renforcement des capacités sur la gouvernance de l'internet dans les Écoles régionales et nationales sur la gouvernance de l'internet (SIG)[3] et fourni par des organisations techniques.[4]
    i. Mobiliser des ressources financières pour soutenir le renforcement des capacités, en particulier parmi les acteurs non étatiques, mais pas seulement.
    j. Fournir une expertise thématique sur les questions émergentes de cybersécurité et leur impact sociétal à mesure que le paysage évolue.
    k. Soutenir l'alignement des activités liées à la cybersécurité par les nations et la hiérarchisation des priorités par les partenaires de développement, les organismes donateurs et d'autres acteurs non étatiques dans un pays en activité afin d'améliorer le renforcement des cyber-capacités.[5]
    l. Combler la fracture numérique, y compris la fracture numérique entre les sexes, renforcer la capacité des femmes et des filles à participer à des activités liées à la cybersécurité.
    m. Lutter contre la violence sexiste en ligne grâce à l'amélioration et au renforcement des compétences en matière de sécurité numérique fournies par les groupes de la société civile.

Quels types d'initiatives en matière de renforcement des capacités sont les plus adaptées pour des contributions significatives et efficaces des acteurs non étatiques ?

3 L'École africaine sur la gouvernance de l'internet (AfriSIG) - www.afrisig.org.

4 Outre de nombreuses initiatives menées par la société civile, l'ICANN et l'Internet Society dispensent également régulièrement des formations et des séminaires sur la gouvernance et la sécurité de l'internet en Afrique. La Fondation Diplo a dispensé une formation en cyberdiplomatie au niveau régional grâce à la collaboration avec la CUA, au niveau national et par le biais de leurs cours en ligne. FIRST et AfriNIC fournissent et encouragent également le renforcement des capacités sur une base régulière. Plusieurs écoles nationales sur la GI ont lieu en Afrique chaque année. Pour y avoir accès : https://www.igschools.net/mw-sig/wiki/Main_Page

5 Par exemple, le GFCE dispose d'un « Centre d'échange » qui permet aux pays bénéficiaires de hiérarchiser les besoins d'assistance en matière de cyber-capacité.

11. Les acteurs non étatiques, y compris la société civile, les entreprises et la communauté technique, peuvent, de manière significative et efficace :
    a. Analyser des politiques et élaborer des lois et des politiques types.
    b. Intégrer une approche centrée sur l'humain et les droits humains dans le droit, la politique et la réglementation en matière de sécurité des TIC.
    c. Développer et promouvoir des normes pour la sécurité des TIC
    d. Développer des capacités et des compétences, y compris la sécurité et l'hygiène numériques, dans des contextes formels et non formels.
    e. Élaborer du matériel de formation, y compris pour la sûreté numérique, la sécurité et l'alphabétisation.
    f. Effectuer des évaluations des besoins en matière de cybersécurité
    g. Convoquer et participer à des consultations communautaires sur les processus de cybersécurité.
    h. Convoquer et participer à des consultations avec les entreprises pour les sensibiliser aux cybermenaces et à la sécurité.
    i. Concevoir des programmes visant à atteindre l'équité et l'égalité de genre dans le secteur de la cybersécurité.
    j. Concevoir, développer et fournir des infrastructures, outils et appareils pour soutenir l'hygiène numérique et la cyber-résilience, par exemple les technologies blockchain.
    k. Former des équipes techniques pour soutenir la gestion de la réponse aux incidents de cybersécurité.
    l. Faciliter et soutenir l'engagement multipartite dans la formulation de politiques de nature inclusive.

Quelles formes de participation des acteurs non étatiques (par exemple, contribution par des ressources techniques, co-création de programmes, contribution de temps et d'expertise de personnes qualifiées) fonctionnent bien et quelles formes de participation des parties prenantes fonctionnent moins bien ?

12. La participation d'acteurs non étatiques ayant bien fonctionné a comporté les éléments suivants :
    a. Apport de ressources techniques et financières incluant une expertise spécialisée.
    b. Co-création de programmes, y compris l'organisation de formations pour renforcer les capacités des acteurs.
    c. Fournir une expertise, y compris une expertise spécialisée dans les processus d'élaboration de politiques et de stratégies cybernétiques.
    d. Assurer la surveillance en termes de suivi et d'évaluation.
    e. Évaluation de l'impact.
    f. Contribution à l'élaboration de structures, de cadres juridiques et politiques.
    g. Recherche pour soutenir l'élaboration de politiques fondées sur des données probantes

Les processus initiés par des acteurs non-étatiques qui ne sont pas inclusifs n'ont pas bien fonctionné. Le manque de ressources pour soutenir les processus au fil du temps peut également affaiblir leur efficacité. Le renforcement des cyber-capacités ne peut pas se faire sur une base « ponctuelle », il doit être continu et intégré dans tout développement des capacités lié à la numérisation.

C - Propositions d'actions collaboratives

Propositions spécifiques d'actions de collaboration - en référence aux propositions axées sur l'action faites jusqu'à présent par les États lors du 2e GTCNL et reflétées dans le projet de rapport d'avancement annuel.

13. Nous recommandons que les acteurs étatiques et non étatiques collaborent pour :
    a. Promouvoir la sensibilisation aux niveaux national, régional et international à la cybersécurité en tant que sécurité sociétale.
    b. Élaborer et mettre en œuvre des stratégies, des politiques et des règlements nationaux complets en matière de cybersécurité.
    c. Élaborer des positions nationales pour les processus mondiaux, tels que le GTCNL et le Comité spécial chargé d'élaborer une Convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.
    d. Donner la priorité à la cybersécurité dans les budgets nationaux afin de garantir des ressources suffisantes pour le développement des capacités de cybersécurité, notamment en intégrant la cyber-hygiène et la sûreté et la sécurité numériques dans les programmes d'enseignement standard aux niveaux primaire, secondaire, tertiaire et dans les programmes de formation professionnelle.
    e. Partager les ressources et l'expertise au niveau national, sous-régional et régional.
    f. Élaborer et mettre en œuvre des mécanismes de collaboration nationale, sous-régionale, régionale et continentale entre l'équipe d'intervention en cas d'incident de cybersécurité (CSIRT) ou l'équipe d'intervention en cas d'urgence informatique (CERT).
    g. Mettre en place des CSIRT et des CERT lorsqu'ils ne sont pas encore en place.
    h. Soutenir la collaboration avec les acteurs non étatiques dans l'élaboration de positions et d'apports nationaux dans les forums régionaux et mondiaux sur la sécurité des TIC.
    i. Examiner les cadres existants et, le cas échéant, établir une législation ou une réglementation visant à renforcer la sécurité et la stabilité du cyberespace.
    j. Élaborer des normes liées à la cybersécurité concernant les PME qui leur soient accessibles.
    k. Renforcer la coordination et la collaboration aux niveaux national, régional et international entre les acteurs étatiques et non étatiques, en particulier dans les pays du Sud
    l. Renforcer la capacité et les ressources des services répressifs pour lutter contre la cybercriminalité et la protection des enfants en ligne aux niveaux national, régional et international.
    m. Améliorer la résilience nationale sur la Protection des Infrastructures Essentielles (PIE) et la Protection des Infrastructures d'Information Essentielles (PIIE) en élaborant et en opérationnalisant des cadres nationaux d'atténuation des risques pour identifier les actifs et les secteurs essentiels nationaux.

Propositions visant à inclure les acteurs non étatiques dans les propositions concrètes et axées sur l'action faites par les États lors des première et deuxième sessions du GTCNL, telles qu'elles figurent dans le projet de rapport d'avancement annuel.

14. En ce qui concerne les propositions visant à inclure des acteurs non étatiques dans les propositions d'actions concrètes faites par les États, nous recommandons :
    a. Des consultations ouvertes inclusives pour recueillir les contributions pertinentes des acteurs non étatiques tout au long du reste du mandat du GTCNL sur toutes les questions à son ordre du jour, et pas seulement sur le renforcement des capacités. La contribution des non-parties prenantes peut également ajouter de la valeur aux discussions sur des questions telles que l'applicabilité du droit international, les mesures de renforcement de la confiance (MRC), l'élaboration et la mise en œuvre de normes.
    b. Une chaîne d'information continue de toutes les parties prenantes, y compris avec et parmi les communautés académiques et techniques.
    c. Que les États incluent des acteurs non étatiques dans les délégations nationales au GTCNL sur les TIC et, si cela n'est pas possible, de les inclure à tout le moins dans le processus national de préparation des positions ainsi que dans les négociations informelles avec d'autres États et acteurs non étatiques.
    d. Une coordination technique aux niveaux local, régional et intercontinental
    e. Renforcer le monde universitaire pour soutenir efficacement la recherche et le développement en matière de sécurité des TIC.
    f. Une approche centrée sur l'humain qui examine comment la cybersécurité affecte le bien-être, les droits, les moyens de subsistance, l'environnement, la culture, les systèmes de croyances et les mentalités des personnes.
    g. Examen du contenu de la formation pour les principaux acteurs impliqués dans les plans d'intervention en cas d'incidents cybernétiques.

15. Les pays devraient développer les capacités requises pour comprendre et mettre en œuvre efficacement les normes GGE sur le comportement responsable dans le cyberespace par les États.
16. Les États membres devraient éviter d'utiliser le droit de veto pour limiter l'engagement des organisations non gouvernementales sans accréditation de l'ECOSOC. Tout recours à ce droit devrait se faire de manière responsable, proportionnelle, transparente et en fournissant des justifications claires au cas par cas aux autres États et à la communauté au sens large.
17. Les gouvernements africains devraient contribuer à la facilitation et/ou participer à la création d'espaces multipartites aux niveaux national et continental qui rassemblent les parties prenantes intéressées, y compris les entreprises, les organisations non gouvernementales et de la société civile et les universités, afin de proposer des mesures visant à soutenir les efforts locaux et continentaux de renforcement des capacités en matière d'expertise, de partage d'informations et de formation en cybersécurité.
18. Réaliser et publier des rapports techniques et des livres blancs (par exemple, des rapports sur l'horizon des cybermenaces, etc.) sur l'état cybernétique national du pays.
19. Impliquer les parties prenantes dans l'élaboration de stratégies, de politiques et de réglementations pertinentes et complètes.
20. Élaborer un cadre durable pour l'amélioration des cyber-capacités. L'une des approches consiste à donner davantage de visibilité aux communautés d'experts existantes en Afrique - là où elles existent, et à les créer là où ce n'est pas le cas – et à leur permettre de s'approprier et diriger le maintien du renforcement des capacités en cybersécurité. Le Groupe d'experts sur la cybersécurité de la Commission de l'Union africaine est un exemple emblématique de ce type d'approche.

21. Établir un transfert de connaissances entre pairs dans les centres d'innovation, les centres d'excellence et les parcs technologiques afin d'encourager l'expertise locale en cybersécurité et dans des domaines connexes.
22. Promouvoir les stars et les champions de la cybersécurité éthique par le biais de compétitions, par exemple les initiatives TIC chez les filles en matière de technologie de genre, ainsi que le mentorat et le coaching afin d'influer sur la culture de cybersécurité et la résilience.

FIN

Signataires

Ce document a été élaborée par les personnes suivantes, qui ont participé à la consultation AfriSIG2022 sur les Priorités africaines pour le renforcement des capacités en matière de cybersécurité. Celle-ci s'est tenue à Lilongwe, au Malawi, du 16 au 18 juillet 2022.

Ababacar Diop	JONCTION	Sénégal
Abdul-Hakeem Ajijola	Groupe d'Experts de l'Union africaine sur la cybersécurité	Nigéria
Albert Antwi-Boasiako	Autorité de cybersécurité	Ghana
Anriette Esterhuysen	Association pour le progrès des communications	Afrique du Sud
Bala Fakandu	Bureau du Conseiller à la sécurité nationale	Nigéria
David Moepeng	Par l'intermédiaire de la Fondation InFuture	Botswana
Margaret Nyambura Ndung'u	PRIDA, Commission de l'Union africaine	Kenya/ Éthiopie
Edetaen Ojo	Media Rights Agenda	Nigéria
Élisabeth Kolade	Association des Experts en cybersécurité du Nigéria	Nigéria
Enrico Calandro	Cyber4Dev	Afrique du Sud
Frederico Links	Namibia Media Trust	Namibie
Geoffrey R Zgambo	Service de Police de la Zambie	Zambie
Grace Githaiga	KICTANet	Kenya
Jimmy Haguma	Force de Police Ougandaise/Commission Ougandaise des Communications	Ouganda
Khadijah El-Usman	Paradigm Initiative	Nigéria
Lillian Nalwoga	CIPESA	Ouganda
Martin Koyabe	Le Forum Mondial sur l'Expertise en Cybersécurité	Kenya / Pays-Bas
Moïse Owiny	Centre for Multilateral Affairs	Ouganda
Muheeb Saïd	Media Foundation West Africa	Ghana
Nompilo Simanje	MISA Zimbabwe	Zimbabwe
Obioma Okonkwo	Media Rights Agenda	Nigéria
Peterking Quaye	West Africa ICT Action Network	Libéria

Ruby Khela	Global Partners Digital	ROYAUME-UNI
Sheetal Kumar	Global Partners Digital	ROYAUME-UNI
Thobekile Matimbe	Paradigm Initiative	Zimbabwe
Victor Kapiyo	KICTANet	Kenya

Annexe 1 - Version résumée

Priorités sur le renforcement des capacités en matière de cybersécurité en Afrique : Résumé du Document sur les résultats de la consultation multipartite AfriSIG22 sur la participation africaine au GTCNL

Lilongwe, du 16 au 18 juillet 2022

Introduction

1. Ce document a été élaboré en tant que contribution au Groupe de travail à composition non limitée sur les TIC (GTCNL) lors d'une consultation multipartite qui s'est tenue à Lilongwe, au Malawi, du 16 au 18 juillet 2022, juste avant le 11e Forum africain sur la gouvernance de l'internet. La consultation, liée à la 10e École africaine sur la gouvernance de l'internet[6], organisée par l'Association pour le progrès des communications et Global Partners Digital, a réuni un groupe diversifié de personnes issues de gouvernements africains, d'organismes d'application de la loi et de sécurité, de la Commission de l'Union africaine, d'organisations de la société civile, de groupes de défense des droits numériques et des médias, et d'experts en cybersécurité. Le document identifie les besoins de divers acteurs étatiques et non étatiques en Afrique en capacités liées à la cybersécurité, puis répond aux questions proposées par l'Ambassadeur Gafoor, président du GTCNL, en préparation de sa deuxième session de fond qui débutera le 25 juillet 2022. Les participants ont contribué à ce document à titre individuel et sont énumérés dans l'annexe à la fin du document.

A - Besoins de renforcement des capacités en matière de cybersécurité en Afrique

Nous recommandons qu'il soit nécessaire d'établir et de renforcer les capacités aux niveaux national, sous-régional[7] (y compris les communautés économiques régionales) et régional en Afrique dans les buts suivants :

5.1 Élaborer des stratégies, des politiques, une diplomatie et des réglementations exhaustives en matière de cybersécurité qui mettent l'accent sur la sécurité des individus et des communautés et qui intègrent les normes applicables, les mesures de renforcement de confiance et le droit international.

5.2 Harmoniser les cadres juridiques et adopter la Convention de Malabo.

5.3 La protection des infrastructures essentielles (IE) et des infrastructures d'information essentielles (IIE).

5.4 Prévenir les incidents de cybersécurité et y réagir, notamment par l'échange d'informations, la minimisation des risques, l'atténuation des conséquences et la préparation au sein des équipes d'intervention en cas d'urgence informatique (CERT) et des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) afin de mieux prévoir et atténuer les menaces à la cybersécurité. Cela comprend une capacité accrue pour communiquer efficacement parmi les équipes d'intervention et entre celles-ci et les autres acteurs étatiques et non étatiques concernés.

5.5 Des mécanismes transparents de rapports de retour d'information pour tous les représentants des États qui participent à des activités sous-régionales, régionales et mondiales afin d'institutionnaliser le partage des connaissances et des informations.

5.6 Coordination et collaboration entre les acteurs étatiques et non étatiques, en

6. AfriSIG est une initiative de l'Association pour le progrès des communications, de la Commission de l'Union africaine et de Research ICT Africa - https://afrisig.org/afrisig-2022/

7. Dans le contexte africain, il s'agit de sous-régions qui sont également souvent appelées « communautés économiques régionales ».

particulier dans les pays du Sud.

6. D'autres domaines dans lesquels un renforcement spécifique des capacités est nécessaire sont les suivants :

6.1 Effectuer des évaluations nationales exhaustives des besoins en cybersécurité afin de déterminer les lacunes et les besoins des différents acteurs et groupes de parties prenantes participant aux processus de cybersécurité.

6.2 Élaborer des mesures de renforcement de confiance pour la région africaine, comme cela a été fait dans d'autres régions.

6.3 Mettre en œuvre et faire le suivi de cette mise en œuvre des normes cybernétiques convenues et s'engager sur l'applicabilité du droit international et la manière de l'opérationnaliser dans le contexte africain.

6.4 Mobiliser les ressources nécessaires pour répondre aux besoins en matière de cybersécurité et mener des consultations nationales de fond avec les acteurs non étatiques dans le cadre de l'élaboration de positions et de stratégies nationales en matière de cybersécurité.

6.5 Lutter contre la cybercriminalité, y compris par la coopération transfrontalière et l'échange de preuves.

7. Nous pensons que, dans le cadre de la réponse à ces besoins de renforcement des capacités, les considérations suivantes devraient être prioritaires :

7.1 Intégrer les questions de genre.

7.2 Combler la fracture numérique, en particulier la fracture numérique entre les genres.

7.3 Élaborer, mettre en œuvre et améliorer les cadres de protection des données et de la vie privée.

7.4 Élaborer et mettre en œuvre des mesures et des mécanismes de notification sur les incidents de cybersécurité afin de permettre la transparence, l'accès à l'information (par exemple via des mécanismes de partage d'informations accessibles au public) et la responsabilité.

7.5 Allouer des ressources financières suffisantes pour renforcer la capacité des ressources humaines des institutions responsables de la cybersécurité.

8. Différents acteurs étatiques et non étatiques ont des besoins spécifiques en matière de renforcement des capacités qui sont inclus dans la version plus longue du présent document (voir ci-dessous). Les besoins qui ont été identifiés comme communs aux acteurs étatiques et non étatiques comprennent :

8.1 Connaître les normes et standards applicables en matière de cybersécurité et de droits humains ainsi que les instruments internationaux pertinents relatifs aux droits humains, y compris les normes et standards non contraignants initiés par l'industrie et la société civile.

8.2 Comprendre les possibilités de participation aux processus stratégiques multilatéraux et la façon de s'engager efficacement.

8.3 Comment les acteurs étatiques et non étatiques peuvent s'engager les uns avec les autres d'une manière qui renforce la confiance.

9. Les besoins supplémentaires identifiés pour les acteurs étatiques (gouvernements et agences de sécurité nationale) comprennent : la compréhension de la valeur des délégations multipartites

et expertes aux Nations unies et dans d'autres processus internationaux de cybersécurité et de diplomatie ; l'applicabilité du droit international et des normes internationales dans leur contexte national ; la capacité institutionnelle de développer et de soutenir la cyber-déontologie et la politique étrangère numérique ; comment protéger les infrastructures critiques, les infrastructures d'information critiques et répondre aux urgences liées aux TIC ; comment appliquer une approche multisectorielle et centrée sur l'humain ; et comment établir des mesures pour renforcer la confiance.

10. Le pouvoir judiciaire doit comprendre les questions de numérisation et de cybersécurité, les lois et la manière de poursuivre les infractions à la cybersécurité, y compris les infractions transfrontalières, la gestion des preuves numériques et la manière de prendre en compte les droits humains dans le jugement des affaires de cybercriminalité.

11. Les institutions chargées de l'application de la loi doivent comprendre que la poursuite des infractions de cybercriminalité peut nécessiter des approches nouvelles et spécialisées pour la détection, les enquêtes et les poursuites en cas de cybercriminalité et la manière de respecter les droits humains dans les enquêtes sur les affaires de cybercriminalité.

12. Les parlementaires doivent être en mesure de comprendre les questions de cybersécurité et de promouvoir la sensibilisation de leurs électeurs à la cybercriminalité, à la sécurité et à la cyberhygiène; comment œuvrer à l'harmonisation des lois sur la cybersécurité dans la région; et comment mieux coopérer avec les autres parties prenantes pour élaborer des politiques qui correspondent à l'ère numérique et qui sont agiles, flexibles, centrées sur l'humain et qui tiennent compte des droits humains et de l'égalité des genres.

11. La Commission de l'Union africaine et les Communautés économiques régionales ont besoin de capacités pour : continuer à soutenir et à donner une plus grande visibilité au Groupe d'experts sur la cybersécurité de la Commission de l'Union africaine (AUCSEG) ; comprendre les possibilités qui existent pour s'engager dans les processus politiques multilatéraux et comment le faire efficacement ; et assurer une coordination technique cohérente et efficace entre les États et les acteurs non étatiques concernés.

B - Collaboration : au niveau régional et entre acteurs étatiques et non étatiques

Participation actuelle d'acteurs non étatiques au soutien et/ou à la mise en œuvre d'initiatives de renforcement des capacités

12. Les acteurs non étatiques participent largement au renforcement des capacités en matière de sécurité des TIC dans toute l'Afrique. Les domaines où une telle participation se démarque comprennent :

12.1 Élaborer et partager des méthodologies de recherche pour les besoins en matière de cybersécurité et les évaluations de l'état de préparation aux niveaux national, sous-régional et régional.

12.2 Sensibiliser aux normes africaines et internationales en matière de droits humains qui s'appliquent à la législation, aux politiques, à l'élaboration et à la mise en œuvre de la réglementation en matière de cybersécurité.

12.3 Renforcement des capacités techniques assuré par les acteurs de la communauté technique et formation à la sûreté et à la sécurité numériques pour cultiver la cyber-résilience.

12.4 Formation à la sécurité numérique pour les journalistes, les institutions et défenseurs des droits humains, dispensée par des organisations de la société civile.

12.5 Contribution à l'élaboration de lois, de politiques et de règlements dans le domaine cybernétique et numérique par des organisations d'experts des droits humains.

12.6 Formation du pouvoir judiciaire (dispensée par l'UNESCO).

12.7 Le Groupe d'experts sur la cybersécurité de la Commission de l'Union africaine (AUCSEG), un groupe multipartite d'experts qui conseille l'UA sur les questions et les politiques en matière de cybersécurité.

12.8 Renforcement des capacités en matière de gouvernance de l'internet au niveau régional et national par l'intermédiaire des Écoles sur la gouvernance de l'internet (SIG)[8] et assuré par des organisations techniques.[9]

12.9 Mobilisation de ressources financières pour soutenir le renforcement des capacités, en particulier parmi les acteurs non étatiques, mais pas uniquement.

12.10 Élaboration de produits de diffusion du savoir et de matériel de formation pour la sensibilisation de la communauté et la littératie numérique par la communauté technique, la société civile et les entreprises.

12.11 Soutenir l'harmonisation des activités liées à la cybersécurité par les pays et l'établissement de priorités par les partenaires de développement, les organismes donateurs et d'autres acteurs non étatiques pour aider les pays à renforcer les cyber-capacités.[10]

12.12 Combler la fracture numérique, y compris la fracture numérique de genre, en établissant et en maintenant des réseaux communautaires et en renforçant la capacité des femmes et des filles à participer à des activités liées à la cybersécurité.

12.13 Lutter contre la violence de genre en ligne grâce à la sensibilisation et au renforcement des compétences en matière de sécurité numérique fournies par les groupes de la société civile.

Quels types d'initiatives de renforcement des capacités sont les plus adaptées à des contributions significatives et efficaces de la part des acteurs non étatiques ?

13. Les acteurs non étatiques, y compris la société civile, les entreprises et la communauté technique, peuvent contribuer de diverses manières au renforcement des capacités. Cela comprend: l'analyse des politiques et l'élaboration de lois types ; l'intégration d'une approche centrée sur l'homme et les droits humains dans la législation, la politique et la réglementation en matière de sécurité des TIC ; l'élaboration et la promotion de normes pour la sécurité des TIC ; le développement des compétences et

8. L'École africaine sur la gouvernance de l'internet (AfriSIG) - www.afrisig.org.

9. L'ICANN et l'Internet Society dispensent régulièrement des formations sur la sécurité en matière de gouvernance de l'internet en Afrique. La Fondation Diplo a dispensé une formation en cyberdiplomatie au niveau régional grâce à la collaboration avec la CUA, au niveau national et par le biais de leurs cours en ligne. FIRST et AfriNIC fournissent et encouragent également un renforcement des capacités sur une base régulière. Plusieurs écoles nationales sur la GI ont lieu en Afrique chaque année. Pour y avoir accès, se rendre sur : https://www.igschools.net/mw-sig/wiki/Main_Page

10. Par exemple, le GFCE dispose d'un processus de « centre d'échange » qui permet aux pays bénéficiaires de hiérarchiser les besoins d'assistance en matière de cyber-capacités.

des capacités - y compris la sécurité numérique et la cyberhygiène - dans des contextes formels et non formels ; l'élaboration de matériel de formation, y compris pour la sûreté, la sécurité et l'alphabétisation numériques ; la conception de programmes visant à atteindre l'égalité de genre et l'équité dans le secteur de la cybersécurité – entre autres.

C - Propositions d'actions collaboratives

Propositions d'actions spécifiques de collaboration - en référence aux propositions axées sur l'action faites jusqu'à présent par les États lors du 2e GTCNL et reflétées dans le projet de rapport d'avancement annuel.

16. Nous recommandons que les acteurs étatiques et non étatiques collaborent pour :

16.1 Promouvoir la sensibilisation aux niveaux national, régional et international à la cybersécurité, vue comme une forme de sécurité sociétale et non seulement technique.

16.2 Élaborer et mettre en œuvre des stratégies, des politiques et des règlements nationaux complets en matière de cybersécurité.

16.3 Élaborer des positions nationales pour les processus mondiaux, tels que le GTCNL et le Comité spécial chargé d'élaborer une Convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

16.4 Donner la priorité à la cybersécurité dans les budgets nationaux afin de garantir des ressources suffisantes pour le développement des capacités en matière de cybersécurité, notamment en intégrant la cyberhygiène et la sûreté et la sécurité numériques dans les programmes d'enseignement standard aux niveaux primaire, secondaire, tertiaire et dans les programmes de formation professionnelle.

16.5 Partager les ressources et l'expertise à l'échelle nationale, sous-régionale et régionale.

16.6 Élaborer et mettre en œuvre des mécanismes de collaboration nationale, sous-régionale, régionale et continentale entre l'équipe d'intervention en cas d'incident de cybersécurité (CSIRT) ou l'équipe d'intervention en cas d'urgence informatique (CERT).

16.7 Établir des CSIRT et des CERT là où ils ne sont pas encore en place.

16.8 Soutenir la collaboration avec les acteurs non étatiques dans l'élaboration de positions et de contributions nationales dans le cadre de forums régionaux et mondiaux sur la sécurité des TIC.

16.9 Examiner les cadres existants et, le cas échéant, établir une législation ou une réglementation visant à renforcer la sécurité et la stabilité du cyberespace.

16.10 Élaborer des normes relatives à la cybersécurité qui traitent des PME et qui leur sont accessibles.

16.11 Renforcer la coordination et la collaboration aux niveaux national, régional et international entre les acteurs étatiques et non étatiques, en particulier dans les pays du Sud.

16.12 Renforcer la capacité et les ressources des organismes chargés de l'application de la loi pour lutter contre la cybercriminalité et la protection des enfants en ligne aux

niveaux national, régional et international.

16.13 Renforcer la résilience de la protection nationale des infrastructures essentielles (PIE) et de la protection des infrastructures d'information essentielles (PIIE) en élaborant et en opérationnalisant des cadres nationaux d'atténuation des risques pour identifier les actifs et les secteurs critiques nationaux.

Propositions visant à inclure les acteurs non étatiques dans les propositions concrètes axées sur l'action faites par les États lors des première et deuxième sessions de fond du GTCNL, telles qu'elles figurent dans le projet de rapport d'avancement annuel.

17. Nous recommandons :

17.1 Les États membres devraient éviter d'utiliser le droit de veto pour limiter l'engagement des organisations non gouvernementales sans accréditation de l'ECOSOC. Tout recours à ce droit devrait se faire de manière responsable, proportionnelle, transparente et en fournissant des justifications claires au cas par cas aux autres États et à la communauté au sens large.

17.2 Que des consultations ouvertes collaboratives et inclusives visant à recueillir les contributions pertinentes des acteurs non étatiques soient convoquées tout au long du reste du mandat du GTCNL sur toutes les questions à son ordre du jour, et pas seulement sur le renforcement des capacités. La contribution des non-parties prenantes peut également ajouter de la valeur aux discussions sur des questions telles que l'applicabilité du droit international, les mesures de renforcement de la confiance (MRC) et l'élaboration et la mise en œuvre de normes.

17.2 Un partage continu de l'information de la part de tous les intervenants, y compris avec et parmi les milieux universitaires et techniques.

17.3 Que les États incluent des acteurs non étatiques dans les délégations nationales au GTCNL sur les TIC et, si cela n'est pas possible, de les inclure à tout le moins dans le processus national de préparation des positions ainsi que dans les négociations informelles avec d'autres États et acteurs non étatiques.

17.4 Une approche centrée sur l'humain qui tient compte de la façon dont la cybersécurité affecte le bien-être, les droits, les moyens de subsistance, l'environnement, la culture, les systèmes de croyances et les mentalités des personnes.

17.5. Les pays développent la capacité de comprendre et de mettre en œuvre efficacement les normes GGE sur le comportement responsable dans le cyberespace par les États.

18. Nous proposons une collaboration entre les acteurs étatiques et non étatiques pour :

18.1 Faciliter et participer à la création d'espaces multipartites aux niveaux national et continental qui rassemblent les parties prenantes intéressées, y compris les entreprises, les organisations non gouvernementales et de la société civile et les universités, afin de proposer des mesures visant à soutenir les efforts locaux et continentaux de renforcement des capacités en matière d'expertise en cybersécurité, de partage d'informations et de formation.

18.2 Réaliser et publier des rapports techniques et des livres blancs (par exemple, des rapports sur les cybermenaces, etc.) sur le statut cybernétique national du pays.

18.3 Faire participer les intervenants à l'élaboration de stratégies, de politiques et de règlements pertinents et exhaustifs.

18.4 Élaborer un cadre durable pour l'amélioration des cyber-capacités. Une approche consiste à donner davantage de visibilité aux communautés d'experts existantes en Afrique - là où elles existent, et à les créer là où elles ne sont pas - pour s'approprier et diriger le maintien du renforcement des cyber-capacités. Le Groupe d'experts sur la cybersécurité de la Commission de l'Union africaine est un exemple emblématique d'une telle approche.

18.5 Établir un transfert de connaissances entre pairs dans les centres d'innovation, les centres d'excellence et les parcs technologiques afin d'encourager l'expertise locale en cybersécurité et dans des domaines connexes.

18.6 Promouvoir les cyber stars et les champions éthiques par le biais de compétition, par exemple les initiatives TIC en matière de technologies de genre chez les filles ou encore le mentorat et le coaching afin d'influencer la culture et la résilience en matière de cybersécurité.

FIN