AFRICA CENTER FOR STRATEGIC STUDIES
25 YEARS
IMPACT THROUGH INSIGHT

ATELIER SUR LA PROMOTION DE LA CYBERSECURITE ET DE LA STABILITE REGIONALES EN AFRIQUE

RAPPORT DE SYNTHESE

PORT LOUIS, MAURICE | 21-23 MAI

PRÉSENTATION DU PROGRAMME

Le Centre d'études stratégiques de l'Afrique (CESA) et le Département d'État américain ont organisé un atelier pour discuter des moyens de faire progresser la cybersécurité en Afrique, conformément au Cadre des Nations unies pour un comportement responsable des États dans le cyberespace. Cette table ronde a réuni 36 participants, dont des représentants de l'Union africaine (UA), de la Commission économique des États de l'Afrique de l'Ouest (CEDEAO), de la Communauté de développement de l'Afrique australe (SADC), de la Communauté de l'Afrique de l'Est (CAE), de l'Autorité intergouvernementale pour le développement (IGAD), des États-Unis, du Royaume-Uni, de l'Union européenne et de l'Union européenne, les États-Unis, le Royaume-Uni et l'Union européenne, ainsi que des représentants de premier plan des équipes d'intervention en cas d'urgence informatique (« computer emergency response teams » ou CERT) et d'autres agences civiles d'Afrique du Sud, du Bénin, de Côte d'Ivoire, du Ghana, du Kenya, de Maurice, du Mozambique, du Nigeria, du Sénégal et de Zambie. Cette table ronde a permis aux participants d'échanger les expériences et les enseignements tirés des efforts déployés pour faire progresser la cybersécurité sur le continent, et de discuter des moyens d'améliorer la coopération au sein de l'architecture de cybersécurité en pleine expansion de l'Afrique.

POINTS CLÉS

On assiste à une augmentation de la participation et de l'influence de l'Afrique dans les institutions qui façonnent la politique internationale en matière de cybersécurité. La représentation du continent dans les institutions où sont décidés les normes, traités et standards mondiaux en matière de cybersécurité est en constante augmentation. Les États africains soutiennent fermement l'idée d'une plus grande inclusion dans ces forums. Ils ont joué un rôle dans le déplacement du centre de gravité des forums des Nations unies sur la cybersécurité, qui est passé du groupe d'experts gouvernementaux (GEG) représentant jusqu'à 25 États membres au groupe de travail à composition non limitée (GTCNL), ouvert à la participation de tous les membres des Nations unies. Avec l'octroi à l'Union africaine d'un statut de membre permanent du G20, la discussion d'un siège africain permanent au Conseil de sécurité des Nations unies et la participation active de plus d'une douzaine d'États africains, ainsi que de l'Union africaine, aux

négociations du traité des Nations unies sur la cybercriminalité, cette influence est appelée à s'accroître.

La région africaine a progressé dans la mise en œuvre du cadre des Nations unies pour un comportement responsable des États dans le cyberespace. L'influence croissante de l'Afrique est en partie due aux progrès réalisés par le continent dans la mise en œuvre du cadre des Nations unies pour un comportement responsable des États dans le cyberespace. Sous l'effet des cybermenaces croissantes et des initiatives en cours de renforcement des capacités cybernétiques, l'Afrique a connu une croissance rapide de sa législation cybernétique, de ses stratégies nationales et de ses CERT nationales. Selon les participants, le nombre total de CERT nationales en Afrique a presque doublé au cours des cinq dernières années pour atteindre environ 37. L'Union africaine et les communautés économiques régionales ont mis en place des politiques, des traités et des positions communes en matière de protection des infrastructures critiques afin de permettre aux États membres de mettre en œuvre le cadre des Nations unies.

L'Afrique dispose d'une architecture régionale de cybersécurité en plein essor. Les participants ont souligné que la croissance des cybercapacités a conduit au développement d'une architecture régionale émergente de cybersécurité. Cette architecture se compose d'au moins trois éléments principaux:

1) **L'Union africaine.** Les participants ont comparé le rôle de l'Union africaine au « toit d'une maison », permettant une coopération en matière de cybersécurité à l'échelle du continent et définissant des politiques, des positions et des normes à mettre en œuvre par les États membres. Au cours des deux dernières années, la Convention de Malabo sur la cybersécurité et la protection des données personnelles de l'Union africaine est entrée en vigueur et une Position africaine commune (PAC) sur l'application du droit international dans le cyberespace a été adoptée. L'UA a également intégré la cybersécurité dans d'autres initiatives, telles que son Agenda 2063, l'Accord de libre-échange continental africain (AfCTFA) et un futur Pacte numérique mondial. Elle travaille actuellement à la mise en œuvre, à l'actualisation et à l'extension du nombre de pays adhérant à la Convention de Malabo, à la mise en œuvre du CAP sur l'application du droit international au cyberespace et à l'adoption d'une stratégie continentale en matière de cybersécurité.

2) **Communautés économiques régionales (CER).** Plusieurs communautés économiques régionales d'Afrique jouent un rôle dynamique dans le renforcement des cybercapacités de leurs États membres, en encourageant la coopération par le biais du renforcement des cybercapacités Sud-Sud et en contribuant à la mise en œuvre d'une stratégie et d'une politique cybernétiques. La CEDEAO a, par exemple, adopté des politiques régionales de lutte contre la cybercriminalité et de protection des infrastructures critiques et a lancé, avec le soutien de la communauté internationale, une initiative régionale de lutte contre la cybercriminalité. La SADC a adopté un cadre juridique et réglementaire harmonisé en matière de cybersécurité, composé de lois types sur la cybercriminalité, la protection des données et le commerce électronique. Les deux CER cherchent à établir ou à approfondir les mécanismes de coopération régionale en matière de cybersécurité.

3) **Réponse aux urgences informatiques.** La croissance rapide des CERT en Afrique a été facilitée par des organisations à but non lucratif telles que le Forum des équipes de réponse aux incidents (en anglais Forum for Incident Response Teams ou FIRST) et l'Équipe d'intervention en cas d'urgence informatique en Afrique (en anglais Africa Computer Emergency Response Team ou AfricaCERT). Ces deux entités ont contribué à faciliter la croissance des CERT dans toute l'Afrique et à leur fournir des forums pour une interaction régulière. Par conséquent, même lorsqu'elles ne sont pas officiellement alignées sur les CER ou l'UA, les CERT du continent ont régulièrement l'occasion d'interagir, de partager les bonnes pratiques et de perfectionner leurs compétences par le biais d'ateliers, de cas pratiques et de hackathons.

Il est nécessaire de renforcer la coordination et l'harmonisation au sein de cette architecture régionale. Comme pour toute architecture émergente, il est nécessaire de renforcer la coordination et la coopération. Dans les grandes lignes, les participants ont estimé que la répartition des tâches et des responsabilités entre les trois composantes était claire : l'UA définit des politiques et des normes à l'échelle du continent, les CER contribuent à la mise en œuvre, au partage des meilleures pratiques et à la facilitation de la coopération en matière de cybersécurité entre leurs États membres, et les CERT s'occupent du renforcement des capacités à un niveau plus technique et opérationnel. Néanmoins, les participants ont souligné la nécessité d'une clarification plus formelle de ces rôles afin d'éviter les risques de double emploi, ainsi que d'une plus grande intégration entre l'UA, les CER et les CERT afin d'assurer une meilleure coordination et de faciliter l'alignement des ressources et des efforts.

Les stratégies et les politiques en matière de cybersécurité sur l'ensemble du continent sont confrontées à d'importantes lacunes en matière de mise en œuvre. Comme beaucoup de politiques élaborées au niveau des CER ou de l'UA, la mise en œuvre peut être un défi. Les participants ont cité le manque de financement et de priorité au niveau du cabinet et du président de leur pays comme des obstacles importants à la mise en œuvre. C'est l'une des principales raisons pour lesquelles la convention de Malabo, bien qu'elle soit récemment entrée en vigueur, a mis une décennie à le faire et n'a pas encore été adoptée par la plupart des États membres.

Les initiatives existantes en matière de renforcement des cybercapacités manquent de coordination et de cohérence. Malgré l'existence de centres d'échange d'informations tels que le Forum mondial sur la cyber-expertise (GFCE), qui cherchent à aligner l'expertise externe sur les besoins en matière de renforcement des cybercapacités, les demandes bilatérales adressées par les États à de multiples partenaires conduisent souvent à des doubles emplois et à un gaspillage d'efforts. Un participant a cité un exemple dans lequel deux partenaires, répondant à une demande d'un État à la recherche d'une capacité, ont organisé sans le savoir deux ateliers sur le même thème à quelques semaines d'intervalle. Le problème est exacerbé lorsque des acteurs extérieurs entreprennent des initiatives de renforcement des cybercapacités sans qu'il y ait un signal de demande fort de la part des pays bénéficiaires, ou lorsque les bénéficiaires du renforcement des cybercapacités formulent des demandes qui ne correspondent pas à leurs niveaux de capacité actuels.

Les infrastructures d'information critiques du continent sont de plus en plus menacées. En raison de menaces telles que les logiciels rançonneurs (ransomwares) et les cyberattaques amplifiées par l'IA, les infrastructures critiques du continent sont de plus en plus menacées. Les

interdépendances au sein des ports, des télécommunications et des secteurs financiers du continent rendent les attaques sur les infrastructures critiques de plus en plus coûteuses et potentiellement déstabilisantes. Les certifications et les formations spécialisées nécessaires pour protéger les logiciels et les systèmes qui gèrent les technologies opérationnelles (OT), les systèmes de commandement en cas d'incident (ICS) et les systèmes de contrôle et d'acquisition de données (SCADA) sont très demandées et l'offre est limitée. Les participants ont souligné que, dans la mesure du possible, l'UA et ses États membres devraient adopter une approche harmonisée pour définir, identifier et protéger les infrastructures critiques, en particulier lorsqu'il existe des dépendances et des vulnérabilités transfrontalières.

RECOMMANDATIONS:

1. ***Cartographier l'architecture de la cybersécurité en Afrique***. Les participants ont recommandé qu'une étude soit entreprise pour cartographier la maturité cybernétique en Afrique aux niveaux national, régional et continental. Des indicateurs communs, tels que ceux utilisés dans l'indice de maturité en matière de cybersécurité de l'Union internationale des télécommunications (UIT), pourraient permettre d'identifier les besoins en matière de renforcement des capacités cybernétiques. L'UA, en partenariat avec un organisme de recherche ou l'UIT elle-même, apparaît comme un candidat naturel pour entreprendre une telle évaluation.

2. ***Améliorer les capacités régionales et nationales de renseignement et d'analyse des menaces.*** Les participants ont recommandé aux pays africains de créer ou de parrainer la création d'outils plus spécifiques au contexte afin d'identifier les cybermenaces auxquelles leurs pays sont confrontés et d'y répondre. Les outils et méthodologies commerciaux largement disponibles peuvent ne pas être bien adaptés pour quantifier les techniques et tactiques les plus courantes des cyberacteurs malveillants opérant en Afrique, qui ont tendance à s'appuyer sur la fraude et l'hameçonnage plutôt que sur des logiciels malveillants sophistiqués, ni les types de systèmes, tels que les téléphones mobiles d'occasion, qui sont le plus souvent pris pour cible. La responsabilité principale de l'élaboration de ces outils varierait probablement d'un pays à l'autre, mais elle pourrait incomber à une CERT ou à une autorité indépendante chargée de la cybersécurité.

3. ***Adopter une stratégie continentale de cybersécurité.*** L'Union africaine devrait publier une stratégie continentale de cybersécurité, tâche qui a déjà été confiée au groupe d'experts en cybersécurité de l'Union africaine (AUCSEG). Cette stratégie devrait attribuer des rôles et des responsabilités clairs en matière de cybersécurité à l'UA, aux CER, aux États membres, à la communauté des CERT et aux partenaires internationaux.

4. ***Organiser des réunions semestrielles ou annuelles de coordination de haut niveau sur le renforcement des capacités, sous l'égide de l'UA-GFCE.*** Afin de remédier à la duplication des efforts des principaux donateurs mondiaux en matière de renforcement des cybercapacités, les participants ont recommandé que l'UA-GFCE organise des conférences de coordination de haut niveau tous les ans ou tous les deux ans. L'objectif de ces conférences serait de permettre aux principaux donateurs internationaux d'aligner les

priorités, les ressources et les domaines d'intervention en matière de renforcement des cybercapacités sur l'ensemble du continent.

5. ***Mettre en place des mécanismes régionaux de coopération en matière de cybersécurité.*** L'Union africaine et les communautés économiques régionales devraient mettre en place des mécanismes régionaux de coopération en matière de cybersécurité afin de permettre une coopération formelle et opérationnelle entre les États africains dans ce domaine. Ces mécanismes peuvent varier d'une région à l'autre, mais pourraient inclure des centres régionaux de partage et d'analyse de l'information (ISAC) pour partager des renseignements sur les menaces, des équipes d'intervention en cas d'urgence informatique (CERT) pour répondre aux menaces et y remédier, ou des centres d'excellence (CoE) pour fournir une formation, publier des programmes modèles et échanger des bonnes pratiques. Ces mécanismes pourraient se concentrer sur les types de menaces pour lesquelles leurs États membres ont un intérêt commun et pour lesquelles une coopération régionale pourrait être utile, comme les cybermenaces émanant d'acteurs extérieurs, les infrastructures d'information critiques transfrontalières, la désinformation ou les groupes transnationaux de cybercriminels. Les participants ont suggéré que les opérations de paix, dans le cadre desquelles certains États membres cultivent certains types de capacités et, le cas échéant, les mettent à disposition au niveau régional, pourraient constituer un modèle utile.

6. ***Faire de la mise en œuvre des politiques de cybersécurité existantes un point central du renforcement des cybercapacités***. Les participants ont souligné les difficultés persistantes auxquelles les États membres sont souvent confrontés dans la mise en œuvre des politiques et stratégies continentales et régionales en matière de cybersécurité. Ils ont recommandé que la mise en œuvre des initiatives existantes, notamment la Convention de Malabo et la Position africaine commune sur l'application du droit international au cyberespace, soit une étape cruciale pour continuer à encourager les États africains à adopter un comportement responsable en matière de cybersécurité. Ils ont recommandé que la mise en œuvre de ces initiatives soit au centre des efforts de renforcement des cybercapacités.

7. ***Donner la priorité au renforcement des cybercapacités Sud-Sud mené par les CER.*** Pour remédier à la duplication, au cloisonnement ou à la mauvaise harmonisation des programmes, les participants ont recommandé que davantage d'efforts de renforcement des cybercapacités soient canalisés par les communautés économiques régionales telles que l'IGAD, la CEDEAO, la CAE, la CEEAC, le COMESA et la SADC. Les CER disposent d'avantages comparatifs par rapport à d'autres acteurs externes en raison de leur connaissance des besoins spécifiques de leurs États membres en matière de renforcement des capacités, de la présence d'infrastructures interdépendantes dans leurs régions et de leur capacité à organiser des initiatives Sud-Sud de renforcement des cybercapacités.

8. ***Harmoniser l'architecture émergente de réponse aux incidents de sécurité informatique du continent.*** Alors que l'architecture d'intervention en cas d'urgence informatique du continent continue de se développer, les participants ont suggéré qu'il était nécessaire de renforcer la coordination et la coopération entre les CERT d'Afrique. Ils ont suggéré que

des plateformes de partage d'informations sur les logiciels malveillants soient adoptées au niveau régional et national, que les CER prennent des mesures pour renforcer la coopération, la coordination et l'harmonisation des capacités et des ressources entre les CERT régionales ou les réseaux de CERT, et que l'Africa-CERT établisse une relation formelle avec l'Union africaine.

9. ***Identifier et prendre des mesures pour protéger les infrastructures critiques transnationales cyberdépendantes.*** L'Union africaine et les CER devraient prendre des mesures pour identifier, coordonner et renforcer la protection des infrastructures d'information critiques dont la compromission aurait des conséquences importantes pour plusieurs États membres. Les institutions multinationales clés, les ports, les câbles sous-marins, les réseaux de télécommunication et les entreprises multinationales des secteurs de la technologie, des télécommunications et de la finance pourraient éventuellement être désignés comme infrastructures critiques régionales ou continentales. Des points de contact cybernétiques fonctionnant 24 heures sur 24 et 7 jours sur 7 devraient être mis en place, en utilisant les CERT nationales comme pôles de coordination.