AFRICA CENTER FOR STRATEGIC STUDIES

25 YEARS

U.S. DEPARTMENT of STATE

Faire progresser la cybersécurité et la stabilité régionales en Afrique

mai 2024

LECTURE EN AMONT

Du 21 au 23 mai 2024

AFRICA CENTER FOR STRATEGIC STUDIES

25 YEARS

U.S. DEPARTMENT of STATE

FAIRE PROGRESSER LA CYBERSÉCURITÉ RÉGIONALE ET LA STABILITÉ EN AFRIQUE

LECTURE EN AMONT

TABLE DES MATIERES

Port Louis, Maurice
Du 21 au 23 mai 2024

Aperçu du programme

Introduction

La région africaine est confrontée à un éventail diversifié et croissant de cybermenaces, allant des acteurs étatiques qui mènent des cyberattaques à des fins géopolitiques aux réseaux cybercriminels qui exploitent l'architecture financière de l'Afrique, de plus en plus dépendante du numérique, à des fins lucratives. Le cadre des Nations unies pour un comportement responsable des États dans le cyberespace ([1]) constitue l'épine dorsale des efforts déployés au niveau mondial pour promouvoir la stabilité et la sécurité dans le cyberespace. Ce cadre comprend l'application du droit international au cyberespace, des normes volontaires et des mesures de confiance. Les normes volontaires non contraignantes comprennent des engagements à protéger les infrastructures critiques, notamment en prenant des mesures réalisables pour atténuer les activités malveillantes survenant dans la juridiction d'un État, et à faciliter la coopération internationale pour prévenir et combattre la cybercriminalité.

En surmontant les différences de capacités et les divergences d'intérêts entre les États membres, les organismes régionaux d'Afrique jouent un rôle crucial dans la coordination des efforts déployés par leurs États membres pour mettre en œuvre le cadre des Nations unies. L'Union africaine (UA) et les Communautés économiques régionales (CER) ont, par exemple, facilité l'adoption de la Convention de Malabo pour permettre à leurs membres de s'entraider dans la détection et la réponse aux menaces transfrontalières en matière de cybersécurité[2] ; rédigé des positions communes et des lois types pour permettre aux pays africains de défendre le cyberespace conformément aux normes juridiques internationales ; et fourni une assistance technique pour développer l'infrastructure d'intervention informatique d'urgence du continent.

Alors que les fondations d'une architecture multilatérale de cybersécurité dans la région africaine sont en train d'être posées, il est nécessaire d'améliorer les mécanismes de coopération et d'affiner d'autres aspects de la manière dont l'UA, les CER, les États individuels et les acteurs extérieurs travaillent pour garantir et promouvoir leurs intérêts communs dans un cyberespace sûr et sécurisé. Lors de cet atelier, les principales parties prenantes de l'UA, des CER et des États africains partageront leurs points de vue et identifieront les possibilités de renforcer les cybercapacités des institutions régionales africaines afin de mettre en œuvre le cadre des Nations unies et de faire progresser la confiance et la coordination dans le cyberespace entre les États membres. Outre l'examen des structures et des initiatives multilatérales africaines, l'atelier permettra également d'identifier les possibilités de coopération efficace et de soutien à ces efforts de la part des États-Unis.

À l'issue de cet atelier de trois jours réunissant des dirigeants et des experts, nous espérons recueillir des idées, des enseignements et des recommandations pour renforcer les mécanismes de coopération régionale en matière de cybersécurité, qui sont de plus en plus nombreux, en fonction des besoins et des intérêts nationaux. À cette fin, des discussions en petits groupes seront organisées tout au long de l'événement, et le programme se terminera par des exposés en séance plénière de chaque groupe de discussion.

---

[1] Assemblée générale des Nations unies (AGNU). *Rapport final de fond du groupe de travail à composition non limitée sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale.* Mars 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[2] Union africaine. « Convention de Malabo sur la cybersécurité et la protection des données personnelles. » Adoptée en juillet 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Objectifs du programme

Les objectifs de l'atelier sont les suivants

1. Convoquer l'UA, les CER et les principaux États africains pour qu'ils échangent des idées, des bonnes pratiques et des enseignements tirés des efforts qu'ils déploient pour renforcer les cybercapacités et améliorer la coopération dans le cyberespace.
2. En s'appuyant sur des exemples d'initiatives régionales réussies visant à renforcer les cybercapacités, formuler des recommandations pour faire progresser les institutions et l'architecture régionales de cybersécurité en Afrique, conformément au cadre des Nations unies.
3. Catalyser les progrès vers la mise en œuvre des recommandations identifiées et discutées par les participants au programme.

Composants de l'atelier et approche

S'appuyant sur les nombreuses décennies d'expertise présentes, cet atelier s'efforcera de tirer des leçons importantes et des pratiques saines par le biais :

- *De sessions plénières* animées par des praticiens et des experts chevronnés, axées sur la collaboration et l'apprentissage réciproque.
- *Un contenu académique* axé sur une analyse fondée sur des données probantes et étayée par des exemples pratiques.
- *Des discussions de groupe* qui offrent aux participants une plateforme de confiance leur permettant de se mettre en réseau et de partager leurs points de vue sur le contenu du programme.
- *Dialogue stratégique* avec des représentants et des participants des États-Unis afin de contribuer à l'élaboration de la politique américaine de soutien aux institutions régionales africaines de cybersécurité.

Le succès de l'atelier repose sur une analyse honnête et un dialogue productif. À cette fin, le Centre d'études stratégiques de l'Afrique (CESA) s'efforce de fournir des données empiriques pour faciliter un échange franc et ouvert sur des questions cruciales, ainsi que pour jeter les bases d'une mise en réseau efficace entre pairs. Pour faciliter l'apprentissage, nous fournissons cet avant-propos et des lectures recommandées. Nous encourageons les participants à se familiariser avec ces documents avant l'atelier afin de pouvoir s'engager activement avec les autres participants. Les lectures sont destinées à favoriser un dialogue sain sur un large éventail de défis africains en matière de cybersécurité et à susciter une discussion sur la manière dont les acteurs régionaux peuvent travailler de concert avec les acteurs nationaux et internationaux pour les relever. ***Afin de permettre une discussion franche sur des questions sensibles, cet atelier se déroulera dans son intégralité dans le cadre d'une politique stricte de non-attribution, qui est contraignante pendant et après le séminaire.***

Préparation de l'atelier

Avant l'atelier, nous demandons aux participants de

1. Parcourir ce document avant de se rendre à l'atelier et prendre le temps de réfléchir aux questions de la discussion et de s'entretenir avec ses collègues, si nécessaire.

2. Passer en revue chaque partie de la lecture anticipée et des lectures recommandées la veille de chaque session et noter pour soi-même les questions, les commentaires ou les expériences que vous souhaitez partager.

Jour 1 : Perspectives sur la promotion de la stabilité et de la sécurité dans le cyberespace

Session 1 : Faire progresser la sécurité et la stabilité internationales dans le cyberespace : Défis et opportunités

Objectifs :

- Fournir une vue d'ensemble des efforts internationaux visant à maintenir la paix et la sécurité mondiales dans le cyberespace en faisant progresser les normes, en appliquant le droit international, en promouvant des mesures de confiance - et une compréhension commune de la nécessité de renforcer les capacités.
- Discuter des défis et des opportunités auxquels ces efforts sont confrontés au niveau international et en Afrique.

Contexte :

À sept reprises depuis 2003, l'Assemblée générale des Nations unies a créé des groupes d'experts gouvernementaux (GGE) chargés d'étudier l'utilisation des TIC par les États. Dans trois rapports de consensus cumulés (2010, 2013, 2015), les groupes d'experts gouvernementaux ont défini un cadre initial pour le comportement responsable des États dans le cyberespace. Dans la résolution 70/237 de l'Assemblée générale, tous les États membres ont accepté d'être guidés par ce cadre. Ce même cadre a été réaffirmé par le groupe de travail à composition non limitée de l'ONU ([3]) en tant que fondement de la poursuite des travaux mondiaux en faveur d'un cyberdomaine pacifique et sûr.

Ce cadre se compose de trois éléments principaux. Premièrement, les États se sont mis d'accord sur l'application du droit international à l'environnement des TIC. Deuxièmement, ils ont convenu de mettre en œuvre des mesures de confiance, y compris des consultations régulières et l'établissement de points de contact pour promouvoir la transparence et le partage d'informations. Troisièmement, le cadre contient 11 normes volontaires et non contraignantes sur le comportement responsable des États dans l'utilisation des TIC :

1) Coopérer pour accroître la sécurité et la stabilité dans l'utilisation des TIC.
2) Prendre en compte toutes les informations pertinentes lors de l'attribution d'un cyberincident.
3) Ne pas permettre sciemment l'utilisation des TIC pour des actes intentionnellement répréhensibles.
4) Coopérer pour lutter contre l'utilisation terroriste et criminelle des TIC.
5) Respecter les droits de l'homme.
6) Ne pas utiliser les TIC pour endommager ou compromettre l'utilisation de l'infrastructure critique d'un autre État pour fournir des services au public.
7) Protéger les infrastructures critiques situées sur leur territoire contre les menaces liées aux TIC.
8) Répondre aux demandes d'assistance des États dont les infrastructures critiques font l'objet d'une cyberactivité malveillante.
9) Assurer la sécurité de la chaîne d'approvisionnement.
10) Encourager le signalement responsable des vulnérabilités liées aux TIC.

11) Ne pas nuire aux équipes d'intervention en cas d'urgence informatique (CERT) et ne pas utiliser les CERT pour se livrer à des activités cybernétiques malveillantes.[3]

La région africaine a joué un rôle important dans la négociation du cadre et dans la sensibilisation à l'importance de renforcer la cybercapacité internationale pour le mettre en œuvre, notamment par la mise en place de stratégies, de programmes et de politiques nationaux de cybersécurité et d'équipes d'intervention en cas d'urgence informatique. En raison de l'augmentation des taux de pénétration de l'internet, de leur influence croissante dans les institutions internationales et des progrès réalisés en matière de sensibilisation et de capacité cybernétique, les pays africains sont susceptibles d'avoir un impact décisif sur la mise en œuvre du cadre. Bien que le cadre ait fait l'objet d'un accord universel, sa mise en œuvre s'est avérée difficile. Cela est dû à toute une série de problèmes, tels que les capacités limitées en matière de cybernétique dans certaines régions du monde, l'ambiguïté quant à la manière d'appliquer les droits de l'homme et les normes juridiques internationales au cyberespace, ainsi qu'un environnement géopolitique mondial de plus en plus conflictuel.

Lectures recommandées :

Assemblée générale des Nations unies (AGNU). *Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale.* Juillet 2021, A/76/135,https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135&Language=E&DeviceType=Desktop&LangRequested=False

Bart Hogeveen, « The UN Norms of Responsible Behavior in Cyberspace », [Les normes des Nations unies sur le comportement responsable dans le cyberespace] Australia Strategic Policy Institute, mars 2022, https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

Louise Marie-Hurl, « The Rocky Road to Cyber Norms at the United Nations » [Le chemin rocailleux vers des normes cybernétiques aux Nations unies], Council on Foreign Relations Net Politics Blog, septembre 2022, https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0.

Conseil de paix et de sécurité de l'Union africaine, « Position africaine commune sur l'application du droit international à l'utilisation des technologies de l'information et de la communication dans le cyberespace », janvier 2024, https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

[3] AGNU, *Rapport de consensus du groupe d'experts gouvernementaux des Nations unies (UN GGE)*, juillet 2015, https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False

Session 2 : Faire progresser la cybersécurité et la stabilité régionales en Afrique

Objectifs :

- Faire le point sur les efforts déployés à l'échelle régionale pour promouvoir la paix, la sécurité et la stabilité dans le cyberespace.
- Discuter des avantages comparatifs, des rôles et des responsabilités des acteurs nationaux et régionaux en Afrique dans la promotion de la cyber stabilité.
- Identifier les lacunes dans l'architecture régionale de cybersécurité de l'Afrique et recenser les possibilités de mettre en place d'autres mesures de renforcement des capacités et de la confiance.

Contexte :

Bien que l'Afrique soit la région la moins numérisée du monde, les capacités cybernétiques varient considérablement d'un pays à l'autre. Selon l'Union internationale des télécommunications, sept pays africains figurent parmi les 50 pays les plus engagés en matière de cybersécurité, dont l'île Maurice, qui occupe la 17ème place à égalité avec la Norvège.[4] Sous l'impulsion de l'Union africaine et des communautés économiques régionales telles que la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), l'architecture régionale de l'Afrique en matière de cybersécurité est sans doute la plus dynamique et la plus avancée de toutes les régions en dehors de l'Europe.

Pour que les institutions régionales africaines maximisent leur rôle croissant dans la promotion de la paix, de la sécurité et de la stabilité dans le cyberespace, il faudra non seulement qu'elles acquièrent des capacités et des aptitudes, mais aussi qu'elles exploitent stratégiquement leurs pouvoirs de rassemblement et de coordination dans l'intérêt des États membres. Il faudra également que l'UA, les CER et d'autres organisations multilatérales tirent stratégiquement parti de leurs pouvoirs de convocation et de coordination dans l'intérêt des États membres. Cela implique une réflexion approfondie sur les intérêts de ces États membres, sur les menaces que les institutions sous-régionales et régionales sont le mieux à même de traiter et sur les possibilités de partenariat qui existent avec des entités bilatérales, multilatérales, du secteur privé et à but non lucratif.

Lectures recommandées :

Nnenna Ifeanyi-Ajufo, « Cyber Governance in Africa : At the Crossroads of Politics, Sovereignty and Cooperation », [La cyber-gouvernance en Afrique : au carrefour de la politique, de la souveraineté et de la coopération]*Policy Design and Practice* 6:2, 146-159, https://www.tandfonline.com /doi/full/10.1080/25741292.2023.2199960

Mailyn Fidler, « Infrastructure, droit et cyber stabilité : An African Case Study » [Infrastructure, droit et cyber stabilité : une étude de cas africaine]. Chesney et al, eds *Cyber Stability and Instability,* 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897108

Nathaniel Allen et Noëlle van der Waag Cowling, « How African States Can Tackle State-backed Cyber Threats » [Comment les États africains peuvent-ils lutter contre les cybermenaces soutenues par l'État ?], 15 juillet 2021, https://www.brookings.edu/articles/how-african-states-can-tackle-state-backed-cyber-threats/.

[4] Union internationale des télécommunications (UIT). Indice mondial de cybersécurité 2020 (GCI). UIT 2024, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E . Les autres pays sont l'Égypte (23), la Tanzanie (37), le Ghana (43), la Tunisie (45), le Nigeria (47) et le Maroc (50). Le Kenya est le numéro 51.

Jour 2 : Faire progresser l'infrastructure de cybersécurité de l'Afrique

Session 3 : Faire le point sur l'architecture régionale de cybersécurité en Afrique

Objectifs :

- Décrire les efforts déployés par l'UA pour promouvoir la cybersécurité et la stabilité régionales en Afrique.
- Identifier les défis et les lacunes.
- Réfléchir et discuter des mesures à prendre par l'UA, la communauté internationale et les États-Unis pour faire progresser les initiatives de l'UA en matière de cybersécurité.

Contexte :
Au cours de la dernière décennie, l'UA a soutenu ou lancé de nombreuses initiatives visant à promouvoir les intérêts de ses États membres dans le cyberespace. Il s'agit notamment des initiatives suivantes

- L'élaboration en 2014 et l'entrée en vigueur en 2023 de la Convention de l'UA sur la cybersécurité et la protection des données personnelles, également appelée convention de « Malabo ».[5] Il s'agit du seul traité régional sur la cybersécurité actuellement en vigueur. Bien qu'il s'agisse d'une réalisation impressionnante, la convention de Malabo n'a été ratifiée que par 15 États membres. La Convention de Budapest sur la cybercriminalité du Conseil de l'Europe, un traité multilatéral conçu pour être mondial et ouvert à tous les pays, complète les dispositions de la Convention de Malabo. Les États-Unis et, à partir de mars 2024, huit pays africains sont partis à la Convention de Budapest.

- L'adoption en 2024 d'une position africaine commune (PAC) sur l'application du droit international à l'utilisation des technologies de l'information et de la communication dans le cyberespace.[6] Il s'agit d'une contribution importante aux discussions mondiales en cours sur la meilleure façon d'appliquer le droit international au cyberespace, un pilier du cadre pour un comportement responsable des États.

- L'adoption de la cybersécurité comme « projet phare » de l'Agenda 2063 de l'Union africaine. La mise en œuvre étant dirigée par l'Agence de développement de l'Union africaine-NEPAD (AUDA-NEPAD), il s'agit d'une reconnaissance du fait que l'avenir économique de l'Afrique dépend d'un cyberespace sûr, sécurisé et fiable.

Ces initiatives, ainsi que d'autres telles que l'adoption de lignes directrices régionales en matière de protection des données et la création de groupes d'experts en cybersécurité de l'UA (AUCSEG), démontrent l'importance croissante et transversale de la cybersécurité pour l'UA et ses États membres. Il s'agit maintenant pour l'UA de renforcer ces initiatives importantes et de

[5] Union africaine. « Convention de Malabo sur la cybersécurité et la protection des données personnelles. » Adoptée en juillet 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[6] Conseil de paix et de sécurité de l'Union africaine, « Position africaine commune sur l'application du droit international à l'utilisation des technologies de l'information et de la communication dans le cyberespace », janvier 2024, https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

s'en inspirer, tout en naviguant entre les points de vue et les intérêts parfois fracturés et divergents de ses États membres et d'autres membres de la communauté mondiale en ce qui concerne le comportement et la coopération entre les États dans le cyberespace.

Lectures recommandées :

Nnenna Ifyeani-Ajufo. « The AU Took Important Action on Cybersecurity at its 2024 Summit – but More is Needed » [L'UA a pris des mesures importantes en matière de cybersécurité lors de son sommet de 2024, mais il faut aller plus loin], Chatham House, 23 février 2024, https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed.

ALT Advisory, « Africa : La Convention de Malabo de l'UA doit entrer en vigueur après neuf ans », 19 mai 2023, https://altadvisory.africa/2023/05/19/malabo-convention-set-to-enter-force/

AUDA-NEPAD, AUDA-NEPAD « Cybersecurity Assessment Report » [Rapport d'évaluation de la cybersécurité], 23 décembre 2020, https://www.au-pida.org/download/cybersecurity-assessment-report/

Nate Allen, Matthew La Lime, et Tomslin Samme-Nlar, *The Downsides of Digital Revolution : Confronting Africa's Evolving Cyber Threats,* [Les inconvénients de la révolution numérique : faire face à l'évolution des cybermenaces en Afrique], Global Initiative Against Transnational Organized Crime, 2 décembre 2022, pp. 52-53, https://globalinitiative.net/analysis/digital-revolution-africa-cyber-threats/

Session 4 : Faire le point sur les initiatives de la Communauté économique régionale (CER) en matière de cybersécurité et de stabilité

Objectifs :

- Décrire les efforts déployés par les CER pour promouvoir la cybersécurité et la stabilité régionales en Afrique.
- Identifier les bonnes pratiques, les défis et les lacunes.
- Réfléchir et discuter des mesures à prendre par les CER, la communauté internationale et les États-Unis pour faire progresser les initiatives des CER en matière de cybersécurité.

Contexte :

Les communautés économiques régionales (CER) d'Afrique ont joué un rôle variable dans la promotion de la politique, de la stratégie et de la coopération en matière de cybersécurité dans leur région. La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) est de loin la CER la plus active en matière de cybersécurité en Afrique. Elle a adopté une stratégie régionale de cybersécurité, rédigé et influencé l'adoption d'une législation modèle sur la cybersécurité dans ses États membres et, en partenariat avec l'Union européenne, a lancé une initiative pour lutter contre la cybercriminalité en Afrique de l'Ouest. D'autres CER, dont la Communauté de développement de l'Afrique australe (SADC) et la Communauté de l'Afrique de l'Est (CAE), ont adopté des lois et des législations types sur des questions telles que la cybercriminalité, la cybersécurité et la protection des données. D'autres encore, comme l'Autorité intergouvernementale pour le développement (IGAD), sont en train d'examiner comment les défis de cybersécurité auxquels sont confrontés leurs États membres pourraient bénéficier d'une approche régionalisée.

En raison de ressources limitées, de la portée et de l'ampleur véritablement mondiales du défi de la cybersécurité et des relations parfois conflictuelles au sein de chaque région, les dirigeants des CER devront peut-être se montrer particulièrement sélectifs quant aux défis de la cybersécurité auxquels ils s'attaquent. Sur certaines questions, telles que les menaces cybernétiques émanant d'acteurs non étatiques qui dépassent les frontières de leur région ou l'adoption de lois types qui reflètent les intérêts et les besoins régionaux, les États africains pourraient tirer profit d'une approche plus régionalisée de la cybersécurité. Sur d'autres questions, il peut être plus prudent pour les États membres de travailler de manière bilatérale ou de s'en remettre à des organismes régionaux ou internationaux.

Lectures recommandées :

Communauté économique des États de l'Afrique de l'Ouest, « Stratégie régionale de la CEDEAO en matière de cybersécurité et de cybercriminalité », février 2021, https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf

Autorité intergouvernementale pour le développement (IGAD), « IGAD SSP Holds IGAD Regional Conference on the Existing Cybersecurity Frameworks of all IGAD Member States » [La SSP de l'IGAD organise une conférence régionale sur les cadres de cybersécurité existants dans tous les États membres de l'IGAD], 8 juillet 2023, https://igad.int/igad-ssp-holds-gad-regional-conference-on-the-existing-cybersecurity-frameworks-of-all-igad-member-states/.

Centre d'excellence en coopération pour la cyberdéfense de l'OTAN, « Communauté de développement de l'Afrique du Sud », https://ccdcoe.org/organisations/sadc/

MISA-Zimbabwe, « Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights » [Cybersécurité et lois sur la cybercriminalité dans la région de la SADC : Implications pour les droits de l'homme], 2021, https://cybilportal.org/publications/cybersecurity-and-cybercrime-laws-in-the-sadc-region-implications-on-human-rights/

Session 5 : Faire progresser les architectures nationales et régionales d'intervention en cas d'urgence informatique en Afrique

Objectifs :

- Faire le point sur les efforts déployés par les acteurs nationaux et régionaux pour développer des capacités de réponse aux urgences informatiques adaptées à la menace et à l'environnement en Afrique.
- Identifier les défis et les lacunes.
- Réfléchir et discuter de la manière dont les acteurs nationaux et régionaux peuvent travailler ensemble pour renforcer les CERT d'Afrique.

Contexte :

Les CERT (Computer Emergency Response Team), parfois appelées CSIRT (Computer Security Incident Response Teams) en français Équipes d'intervention en cas d'urgence ou d'incident de sécurité informatique, sont des nœuds essentiels de l'écosystème de cybersécurité d'un pays. En tant que centres d'excellence technique et d'expertise, les CERT nationales jouent souvent un rôle central dans la sensibilisation à la cybersécurité, la surveillance du trafic Internet pour détecter les menaces, la protection et le rétablissement des infrastructures d'information critiques en cas d'attaque, et la réponse aux demandes de coopération et d'assistance internationales. Les CERT sont si essentielles que l'une des normes des Nations unies stipule que les États ne doivent pas mener ou soutenir sciemment des activités visant à nuire aux systèmes d'information des équipes d'intervention d'urgence autorisées d'un autre État. [17]

Le paysage des CERT en Afrique est diversifié et évolue rapidement. La majorité des pays africains n'ont pas encore mis en place de CERT national, mais le nombre de CERT nationaux en Afrique a augmenté de près de 50 % entre 2018 et 2021, passant de 13 à 19.[8] Certains pays, comme le Ghana, l'Égypte et l'île Maurice, possèdent de solides infrastructures de protection des CERT et des infrastructures d'information critiques (IIC). Des organisations telles que le Forum mondial des équipes de réponse aux incidents et de sécurité et AfricaCERT participent depuis plus de dix ans à la création, au renforcement des capacités et à l'échange de bonnes pratiques entre les CERT basées en Afrique. Le soutien des pays donateurs par l'intermédiaire d'experts partenaires chargés de la mise en œuvre a également joué un rôle essentiel. Pour aller de l'avant, ces entités doivent aller au-delà du simple renforcement des capacités et envisager des possibilités plus larges de collaboration et de partenariat avec des organisations multilatérales, des gouvernements nationaux et des partenaires bilatéraux clés.

Lectures recommandées :

Internet Society et Commission de l'Union africaine (CUA), *Lignes directrices pour la sécurité de l'infrastructure Internet en Afrique*, 24 mai 2017, https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

[7]AGNU, *Rapport de consensus du groupe d'experts gouvernementaux des Nations unies (UN GGE)* juillet 2015, https://undocs.org/Home/Mobile?FinalSymbol=A%2F70%2F174&Language=E&DeviceType=Desktop&LangRequested=False

[8] UIT, *2020 Global Cybersecurity Index* (GCI), https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, p. 7

Jean-Robert Hountomey, Hayretdin Bahsi, Unal Tatar, Sherif Hashem & Elisabeth Dubois, *Cyber Incident Management in Low-Income Countries*, AfricaCERT et le Global Forum on Cyber Expertise (GFCE), 2022, https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/

Nate Allen, Sherif Hashem et Elizabeth Kolade, « 'Leapfrogging' or 'lagging'? : highlighting critical information infrastructure protection challenges and opportunities in Egypt and Nigeria » [Avancer ou reculer : mise en évidence des défis et des opportunités liés à la protection des infrastructures d'information critiques en Égypte et au Nigéria], à paraître, *Journal of Cyber Policy*, https://doi.org/10.1080/23738871.2024.2304560.

Jour 3 : Faire progresser la coopération entre les États-Unis et l'Afrique en matière de cybersécurité

Session 6 : Faire progresser la coopération américano-africaine en matière de cybersécurité

Objectifs :

- Faire le point sur les efforts de coopération en matière de cybersécurité entre les États-Unis et l'Afrique déployés par le Ministère des Affaires Étrangères, le Ministère de la Défense et le Ministère de l'Intérieur.
- Identifier de nouveaux domaines de partenariat, en se concentrant sur les possibilités de coopération régionale et de partenariats multilatéraux.

Contexte :

Depuis près de vingt ans, la pierre angulaire de la politique internationale des États-Unis en matière de cyberespace est le soutien à un internet ouvert, interopérable, fiable et sûr. En Afrique, les États-Unis ont mis l'accent sur la réalisation de ces objectifs en cherchant à mettre en œuvre le cadre des Nations unies et en aidant les pays partenaires à renforcer leur cybersécurité nationale grâce à une approche pangouvernementale et multipartite. La cybersécurité en Afrique présente un intérêt croissant pour la politique étrangère des États-Unis. Lancée en 2022 lors du sommet des dirigeants américains et africains, l'initiative « Digital Transformation with Africa » (DTA) de la Maison Blanche compte parmi ses principaux objectifs la promotion de la gouvernance et de la réglementation afin de garantir un environnement numérique sûr.[9] En 2023, la cybernétique a été abordée pour la première fois lors de l'exercice militaire « Justified Accord » organisé par le commandement américain pour l'Afrique au Kenya.[10] Les États-Unis ont organisé des dialogues bilatéraux sur le cyberespace et le numérique avec le Kenya et l'Afrique du Sud.

Compte tenu de la numérisation rapide de l'Afrique, de son influence croissante sur les affaires mondiales et des capacités cybernétiques de plus en plus importantes dans de nombreux pays, les États-Unis et leurs nombreux partenaires dans toute la région africaine ont tout intérêt à approfondir cette coopération. L'examen des possibilités d'approfondissement de la collaboration ne dépend pas seulement de l'identification des domaines d'intérêt mutuel, mais aussi de l'examen des domaines dans lesquels la coopération avec les États-Unis ou l'assistance technique de ces derniers peuvent présenter des avantages comparatifs pour les États et les organisations régionales d'Afrique.

Lectures recommandées :

Département d'État américain, « Déclaration pour l'avenir de l'Internet », 28 avril 2022, https://www.state.gov/declaration-for-the-future-of-the-internet

Maison Blanche, « FACT SHEET : New Initiative on Digital Transformation with Africa (DTA) » [FICHE D'INFORMATION : Nouvelle initiative sur la transformation numérique avec

[9] Maison Blanche, « FACT SHEET : New Initiative on Digital Transformation with Africa (DTA) » [FICHE D'INFORMATION : Nouvelle initiative sur la transformation numérique avec l'Afrique], 4 décembre 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/.

[10] Colin Demarest, « Cyber to be Featured for First Time at US Military Exercise in Africa », C4ISRNet, 22 décembre 2022, https://www.c4isrnet.com/cyber/2022/12/22/cyber-to-be-featured-for-first-time-at-us-military-exercise-in-africa/.

l'Afrique], 4 décembre 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/.

Colin Demarest, « Cyber to be Featured for First Time at US Military Exercise in Africa » [Le cyberespace à l'honneur pour la première fois lors d'un exercice militaire américain en Afrique], C4ISRNet, 22 décembre 2022, https://www.c4isrnet.com/cyber/2022/12/22/cyber-to-be-featured-for-first-time-at-us-military-exercise-in-africa/.

Orientations du groupe de travail : Recommandations pour faire progresser l'architecture de cybersécurité de l'Afrique

Objectifs :

- Partagez les idées clés et les enseignements tirés de la discussion qui sont pertinents pour l'ensemble du groupe.
- Procéder à une évaluation complète et partagée de l'architecture de la cybersécurité en Afrique, notamment au niveau régional (UA), sous-régional (CER et autres) et national, et de la manière dont ces éléments s'articulent entre eux.
- Formuler des recommandations sur la manière d'étendre, de modifier, de réviser ou d'améliorer l'architecture de cybersécurité régionale et sous-régionale existante de l'Afrique, conformément au cadre.
- Identifier les possibilités de partenariat entre les gouvernements africains, les institutions régionales et les États-Unis pour mettre en œuvre les recommandations proposées.

Contexte :

L'un des éléments clés de cet atelier sera une série de groupes de discussion « de travail » qui formuleront des recommandations visant à faire progresser l'architecture régionale de cybersécurité de l'Afrique conformément au cadre et en partenariat avec les principaux acteurs et institutions présents. Les groupes de travail comprendront environ 10 participants chacun et seront composés d'une combinaison de parties prenantes issues d'institutions multilatérales, de gouvernements africains, d'experts et de participants basés aux États-Unis.

Au cours de trois réunions, les participants à ces groupes de travail vont : 1) identifier ce qu'ils considèrent comme les cybermenaces les plus importantes en Afrique, 2) faire le point sur l'architecture régionale de cybersécurité en Afrique, et 3) élaborer des recommandations spécifiques pour que l'UA, les CER et leurs pays, en partenariat avec les États-Unis et d'autres acteurs, fassent progresser l'architecture régionale de cybersécurité en Afrique conformément au cadre.

Lors de la séance de synthèse du dernier jour, les groupes présenteront leurs conclusions et leurs recommandations à un panel d'experts, qui leur fournira un retour d'information et encouragera la poursuite du débat. Des instructions plus spécifiques concernant la conduite des groupes de travail accompagnent cet avant-propos.