Laboratoire Africain de
Recherches en Cyberstratégie

La cybergouvernance en Afrique : au carrefour de la politique, de la souveraineté et de la coopération

Résumé : L'Afrique s'est récemment concentrée sur l'ambition de réaliser la transformation numérique à travers la poursuite de diverses initiatives phares visant à atteindre les objectifs de son « Agenda 2063 ». La transformation numérique sera mieux réalisée grâce à des politiques et mécanismes de cybergouvernance appropriés. Ainsi, le succès de la stratégie de transformation numérique de l'Afrique 2020-2030 dépend de divers facteurs. Selon cette stratégie, les gouvernements africains ont la responsabilité fondamentale de créer un environnement favorable, avec des politiques et des réglementations qui promeuvent la transformation numérique à travers les piliers fondamentaux, qui incluent la cybersécurité. La stratégie souligne également la nécessité de renforcer les capacités humaines et institutionnelles de la région pour sécuriser le cyberespace en instaurant la confiance dans l'utilisation des cyber-technologies. L'objectif de ce document est d'examiner le programme de cybergouvernance de l'Afrique en relation avec la paix et la sécurité. Bien qu'il existe des dimensions politiques pour déterminer les seuils de ces discours en Afrique, les incertitudes des mécanismes de gouvernance, les fondements politiques et les limites de la capacité numérique peuvent signifier que les normes internationales de cybergouvernance ont été simplement théoriques dans le contexte africain. Ce document examine les stratégies politiques existantes de l'Afrique en matière de cybergouvernance, ainsi que l'interaction de la région avec les processus internationaux de cybergouvernance. Il examine également les perspectives et les défis de la cybergouvernance dans la région, ainsi que les approches permettant de tirer parti de la coopération internationale pour promouvoir la cyber-stabilité dans la région.

Mots clés : Afrique, cybergouvernance, transformation digitale, politiques cyber, souveraineté digitale.

Par

Larc-Publication

31/01/2024

Pour citer la version originale :

Nnenna Ifeanyi-Ajufo (2023), "Cyber governance in Africa: at the crossroads of politics, sovereignty and co-operation", Policy Design and Practice, 6:2, 146–159, DOI: 101,080/25741292.2023.2199960

Introduction

L'Afrique a récemment commencé à explorer un programme sur la transformation numérique. Après l'adoption de la Déclaration de *Charm el-Cheikh* de 2019[1], en février 2020, la Commission de l'Union africaine (CUA) a adopté la Stratégie de transformation numérique pour l'Afrique[2], qui a été suivie par la Feuille de route numérique de l'Union européenne[3] la même année. L'Union européenne a fait de la transformation numérique l'un des piliers de son engagement et de sa coopération avec l'Afrique, s'est attachée à stimuler la transformation numérique du continent et à renforcer l'ordre international fondé sur des règles et le système multilatéral (*European Union Commission* : 2020). Ces dernières années, la cybergouvernance a été au premier plan des agendas diplomatiques et politiques d'importantes réunions bilatérales et multilatérales (*Potter* : 2002). Le discours continue de se développer dans le cadre de consultations formelles et informelles avec des initiatives diplomatiques régionales et internationales. La promotion de la sécurité et de la stabilité dans le cyber-environnement peut être renforcée par l'adoption de politiques appropriées,[4] et la mise en place de mesures de coopération qui peuvent contribuer à une cybergouvernance appropriée.[5]

[1] Troisième session ordinaire du Comité technique spécialisé de l'Union africaine sur les technologies de la communication et de l'information (STC-CICT), 22-26 octobre 2019, Sharm El Sheikh, Égypte 37590-2019_sharm_el_sheikh_declaration_-_stc-cict-3_oct_2019_ver2410-10pm-1rev-2.pdf (au.int)
[2] The African Union Digital Transformation Strategy for Africa (2020–2030)
[3] Communication-shaping-europes-digital-future-feb2020_en_4.pdf (europa.eu)
[4] Le Groupe d'experts gouvernementaux (GGE) des Nations unies a adopté par consensus les Normes relatives au comportement responsable des États dans le cyberespace en 2010, 2013 et 2015. The UN Norms of Responsible State Behaviour in Cyberspace.
[5] Voir la norme 4 des 11 normes non contraignantes relatives au comportement responsable des États dans le cyberespace du Groupe d'experts gouvernementaux des Nations unies.

I. La cybergouvernance en Afrique

Pour une cybergouvernance efficace, la coopération est impérative, car, dans le contexte d'un cyberespace sans frontières, les approches collaboratives engendrent une responsabilité partagée entre les États (*Mueller* : 2020). La septième action clé de la feuille de route des Nations unies pour la coopération numérique est la promotion de la confiance et de la sécurité dans l'environnement numérique. [6]Pour promouvoir la confiance et la sécurité dans l'environnement numérique, il est nécessaire de coopérer (*Meyer* : 2020). Le rapport 2021 du Groupe d'experts gouvernementaux (GGE)[7] réaffirme que « ... un environnement TIC ouvert, sûr, stable, accessible et pacifique est essentiel pour tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationales "[8]. Le rapport final du Groupe de travail à composition non limitée (GTCNL)[9], qui a confirmé les résultats des rapports du Groupe d'experts gouvernementaux[10], exhorte les États à coopérer avec d'autres États pour mettre en œuvre un comportement responsable dans le cyberespace.

Le débat sur la gouvernance et la coopération en Afrique pour la sécurité et la stabilité dans le cyberespace a été largement inexploré (*Microsoft* : 2021). La préparation de l'Afrique à la cybergouvernance soulève de nombreuses questions quant à l'efficacité des mécanismes de gouvernance africains pour assurer la cyber-résilience dans la région (*Schlehahn* : 2020). Les disparités en matière de capacités numériques et de structures politiques semblent également constituer un défi pour la mise en œuvre des principes de comportement responsable des États dans le cyberespace par les États africains. La position et l'approche des dirigeants africains à l'égard de la souveraineté numérique et le fait que la coopération numérique pourrait impliquer une dépendance numérique face à des capacités numériques différentes suscitent également des

[6] Assemblée générale des Nations unies. Rapport du Secrétaire général-Feuille de route pour la coopération numérique A/74/81 Juin 2020. Roadmap_for_Digital_Cooperation_EN.pdf (un.org).
[7] 2021 Report of the Group of Governmental Experts on Advancing Responsible State behaviour in Cyberspace in the Context of International Security. final-report-2019-2021-gge-1-advance-copy.pdf (un-arm.org).
[8] Ibid, voir la note 5 du rapport.
[9] Le groupe de travail à composition non limitée des Nations unies (Open-ended Working Group) sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, créé en vertu de la résolution 73/27 de l'Assemblée générale. Rapport final de fond. UNGA A/AC.290/2021/CRP.2 10 mars 2021
[10] Les rapports de consensus de 2010, 2013 et 2015 des groupes d'experts gouvernementaux des Nations unies sur les menaces, normes, règles et principes existants et émergents relatifs au comportement responsable des États, au droit international, au renforcement de la confiance, à la coopération internationale et au renforcement des capacités, qui constituent ensemble un cadre cumulatif et évolutif pour le comportement responsable des États dans leur utilisation des TIC.

inquiétudes.[11] La transformation numérique offre à l'Afrique d'immenses possibilités, mais une transformation numérique efficace et efficiente en Afrique ne peut se produire que dans un cyberespace fiable, sûr et résilient, d'où l'importance d'examiner la cybergouvernance et le programme de transformation numérique en Afrique en relation avec la paix et la sécurité.

II. Centrer la cybersécurité dans la transformation numérique

La stratégie africaine de transformation numérique[12] a mis en évidence la nécessité d'une plus grande capacité à détecter et à atténuer les cyberattaques dans la région. Selon cette stratégie, il incombe aux gouvernements africains de créer un environnement propice, avec des politiques et des réglementations qui favorisent la transformation numérique à travers les piliers fondamentaux, y compris la cybersécurité.[13] La stratégie affirme également sans équivoque que « les mesures et outils réglementaires collaboratifs en matière de TIC constituent la nouvelle frontière pour les régulateurs et les décideurs politiques qui s'efforcent de maximiser les opportunités offertes par la transformation numérique dans l'ensemble des industries ».[14]

En 2014, la Commission de l'Union africaine a adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (ci-après la Convention de Malabo)[15] afin de fournir des principes fondamentaux et des lignes directrices pour assurer la cybersécurité, la protection efficace des données personnelles et la création d'un environnement numérique sûr (*Ball* : 2017). La Convention de Malabo est une législation régionale importante qui fournit un cadre pour assurer la cybersécurité en Afrique en réglementant les transactions électroniques, en protégeant les données personnelles et en luttant contre la cybercriminalité. La CUA considère la Convention de Malabo comme une stratégie visant à créer un système uniforme de cybergouvernance, à garantir des approches réglementaires unifiées entre les États membres de l'Union africaine et à promouvoir la cyber-résilience dans la région. La Convention encourage les

[11] Par exemple, dans de nombreux cas, la convention de Malabo de l'Union africaine semble faire primer la souveraineté et la discrétion nationales sur le droit international, notamment dans le chapitre 3 sur la promotion de la cybersécurité et la lutte contre la cybercriminalité.
[12] The African Union Digital Transformation Strategy for Africa (2020–2030).
[13] Ibid p. 7
[14] Ibidem. Italics mine for emphasis.
[15] La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, 2014. La Convention a été adoptée lors de la 23e session ordinaire du Sommet de l'Union africaine qui s'est achevée à Malabo, en Guinée équatoriale, le 27 juin 2014.

États membres de l'UA à reconnaître la nécessité de protéger les infrastructures TIC, de lutter contre la cybercriminalité et d'encourager la libre circulation de l'information grâce à un cadre réglementaire unifié en matière de cybersécurité.

Depuis l'adoption de la Convention de Malabo, la CUA s'est concentrée sur le renforcement des capacités en organisant des initiatives de renforcement des capacités en matière de cybergouvernance en collaboration avec des partenaires clés, des communautés économiques régionales (CER) et des États membres, afin de promouvoir une culture de la cybersécurité, de renforcer la confiance dans l'utilisation des TIC et de fournir des orientations sur l'élaboration de politiques en matière de cybersécurité. La CUA, en coopération avec l'Internet Society, a élaboré des lignes directrices sur la sécurité de l'infrastructure de l'Internet en Afrique[16] et des lignes directrices sur la protection des données personnelles pour l'Afrique.[17] En 2018, le Conseil exécutif de l'Union africaine a approuvé la « Déclaration de l'UA sur la gouvernance de l'Internet et le développement de l'économie numérique "[18] et a adopté la cybersécurité comme projet phare de l'Agenda 2063 de l'Union africaine.[19] En étroite collaboration avec l'Union européenne, la CUA a lancé l'« Initiative de politique et de réglementation pour l'Afrique numérique (PRIDA) », dont le mandat essentiel est de renforcer les capacités des groupes d'acteurs africains de l'Internet dans les 55 États membres de l'Union africaine (UA) sur les questions de gouvernance de l'Internet et de cybersécurité.[20]

[16] Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique. Une initiative conjointe de l'Internet Society et de la Commission de l'Union africaine. 30 mai 2017 AfricanInternetInfrastructureSecurityGuidelines_May2017.pdf (internetsociety.org).

[17] Lignes directrices sur la protection des données personnelles pour l'Afrique. Une initiative conjointe de l'Internet Society et de la Commission de l'Union africaine. Personal Data Protection Guidelines for Africa - Internet Society

[18] African Union Declaration on Internet Governance and Development of Africa's Digital Economy Assembly/AU/Decl.3(XXX)

[19] Voir l'Agenda 2063 : L'Afrique que nous voulons. L'Agenda 2063 : L'Afrique que nous voulons. | Selon l'Union africaine (au.int), "l'Agenda 2063 est le cadre stratégique qui permettra à l'Afrique d'atteindre son objectif de développement inclusif et durable et constitue une manifestation concrète de l'élan panafricain pour l'unité, l'autodétermination, la liberté, le progrès et la prospérité collective dans le cadre du panafricanisme et de la renaissance africaine". Pour affirmer leur engagement à soutenir la nouvelle voie de l'Afrique vers une croissance et un développement économiques inclusifs et durables, les chefs d'État et de gouvernement africains ont signé la déclaration solennelle du 50e anniversaire lors des célébrations du jubilé d'or de la formation de l'OUA/UA en mai 2013. L'Agenda 2063 est la manifestation concrète de la manière dont le continent entend réaliser cette vision au cours d'une période de 50 ans, de 2013 à 2063.

[20] L'initiative "Politique et réglementation pour l'Afrique numérique" (PRIDA) est une initiative conjointe de l'Union africaine (UA), de l'Union européenne (UE) et de l'Union internationale des télécommunications (UIT). Elle est soutenue par le programme panafricain financé par l'UE. Voir l'initiative de politique et de réglementation pour l'Afrique numérique (PRIDA) (itu.int)

III. Un carrefour de la politique, de la souveraineté et de la coopération

Alors que les sociétés sont de plus en plus numérisées, la cybergouvernance, en particulier en ce qui concerne la sécurité, continue d'apparaître comme une priorité politique pour de nombreux gouvernements à travers le monde. Cependant, les pays africains continuent d'afficher des niveaux de cyber-maturité faibles (*International Telecommunications Union* : 2021 a). Les États membres de l'UA ont des intérêts divergents, et l'inefficacité des mécanismes de gouvernance ainsi que le manque de capacités en matière de politiques, de stratégies et d'infrastructures ont constitué un défi pour l'Afrique dans le domaine de la cybergouvernance. Les organisations régionales telles que l'Union africaine sont ancrées dans leurs contextes historiques, culturels et politiques respectifs, ce qui a une incidence sur leurs idéologies et leurs capacités dans des domaines tels que la cybergouvernance (*Pawlak, Tikk, Kerttunen* : 2020). La création de cadres juridiques et de relations diplomatiques a des fondements politiques, y compris dans les conversations sur la souveraineté numérique qui résonne avec le contexte historique de l'Afrique en termes de colonisation. Dans ces contextes, la manière dont les stratégies de cybergouvernance en Afrique sont abordées pour promouvoir et garantir la paix, la sécurité et la stabilité dans le cyberespace pose de nombreux défis.

III. I. Défis liés aux lois et aux politiques

Par rapport à des régions comme l'Europe, l'Afrique ne dispose pas d'un programme unifié et coopératif en matière de cybergouvernance. Les points de vue des États membres africains sur la cybergouvernance ne sont pas homogènes, sans normes ni principes communs (*Clifford* : 2022). Certains gouvernements africains sont désireux d'accorder la priorité à la cybergouvernance et de sécuriser les infrastructures critiques,[21] cependant, de nombreux autres gouvernements considèrent toujours la cybergouvernance comme une non-priorité (*Nicholas* : 2018). La réticence des États africains à ratifier les conventions régionales et internationales en est incontestablement la preuve. Depuis 2014, la Convention de Malabo n'est pas encore entrée en vigueur conformément à l'article 36 de la Convention en raison d'une ratification insuffisante de la part des quinze (15)

[21] Par exemple, le Ghana est un pays africain qui a fait d'immenses efforts pour lutter contre la cybercriminalité. Les efforts déployés par le Ghana ces dernières années pour lutter contre la cybercriminalité ont abouti à des initiatives telles que le Centre national de cybersécurité (NCSC) - créé en 2018 - et la loi sur la cybersécurité (*Cybersecurity Act 2020*), qui ont considérablement renforcé le développement de la cybersécurité dans le pays. Le Ghana a en outre ratifié les conventions de Malabo et de Budapest, ce qui témoigne de la ferme déclaration d'intention du pays en matière de cybersécurité.

États africains requis.[22] L'importance de la Convention de Malabo pour diriger la cyber gouvernance dans la région dépend de son adoption par les États africains. L'entrée en vigueur de la Convention de Malabo constituera une étape majeure dans la mise en place d'un cadre juridique régional africain et dans l'élaboration de normes et de principes communs en matière de cybergouvernance.

La participation des États africains aux processus mondiaux de cybergouvernance est limitée. L'importance et l'influence d'un accord ou d'un traité international ou régional dans un pays donné dépendent de la mesure dans laquelle cet instrument a été intégré et mis en œuvre dans la législation et les stratégies nationales (*Finnemore & Sikkink* : 1998). La Convention du Conseil de l'Europe sur la cybercriminalité (la Convention de Budapest)[23] a été rédigée pour se concentrer sur l'harmonisation des lois et le renforcement de la coopération internationale afin de promouvoir la cybersécurité au-delà des frontières et est entrée en vigueur en 2001. Seul un nombre insignifiant de pays africains ont ratifié la Convention, malgré les efforts du Conseil de l'Europe pour promouvoir la coopération avec les États africains par l'intermédiaire de la CUA.

L'Afrique est composée de sous-régions dotées d'organisations sous-régionales bien structurées qui jouissent d'une indépendance exécutive, législative et judiciaire. Il s'agit notamment de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), de la Communauté de l'Afrique de l'Est (CAE), de la Communauté de développement de l'Afrique australe (SADC) et de la Communauté de l'Afrique centrale (CEEAC). Bien qu'il s'agisse d'une évolution positive qui reflète l'intégration et la coopération sous-régionales plus larges en Afrique, ces organisations sous-régionales s'engagent dans des stratégies indépendantes en matière de cybergouvernance et n'ont aucune obligation explicite ou exécutoire envers la CUA en ce qui concerne leurs décisions d'adoption ou de priorisation d'une stratégie de cybergouvernance. Chaque organisation sous-régionale est indépendante. Au niveau sous-régional, la SADC a adopté la loi type de la SADC sur la cybercriminalité en 2012 pour guider et faciliter l'harmonisation des lois nationales sur la cybercriminalité et la CEDEAO a adopté la directive de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) sur la lutte contre la cybercriminalité au

[22] Voir l'article 36 de la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, 2014.
[23] Convention on Cybercrime, 2001. Budapest 23/11/2001

sein de la CEDEAO, 2011, y compris d'autres stratégies indépendantes de cybergouvernance entreprises par la CEDEAO.

Le manque de capacités, d'expertise et de compétences se répercute sur le processus de cyberlégislation. De nombreux États africains n'ont toujours pas de législation ou de stratégie en matière de cybersécurité. Les recherches montrent que seuls dix-sept (17) des cinquante-quatre (54) pays africains disposent d'une stratégie nationale de cybersécurité et que seuls trois (3) de ces pays possèdent les critères minimums essentiels pour une stratégie de cybersécurité adéquate (*Ajijiola & Allen* : 2022). Selon l'Union internationale des télécommunications (UIT), seuls vingt-neuf (29) des cinquante-quatre (54) pays africains ont promulgué une législation sur la cybersécurité (*International Telecommunications Union* : 2021 b).

La maîtrise de la cyberlégislation est un défi pour les législateurs africains. Lorsque les pays africains disposent de lois, ils doivent être en mesure de les mettre en œuvre. Si certains États rédigent des cyberlégislations, la capacité de cyber-légiférer efficacement et de mettre en œuvre de telles lois est toujours en question dans la région. De telles lacunes pour les parlementaires et les décideurs politiques se traduiraient par des stratégies de cybergouvernance irréalistes. Un exemple en est la loi nigériane sur la cybercriminalité que la Cour de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a ensuite jugé nécessaire d'abolir ou de réviser en raison de dispositions susceptibles de porter atteinte aux droits de l'homme des citoyens et de restreindre les droits des utilisateurs du cyberespace à la liberté d'expression et à la protection de la vie privée.[24] La compréhension des réalités de la cybergouvernance est également minimale, ce qui explique que les contradictions dans les textes juridiques soient courantes. La transposition évidente de la législation occidentale en matière de cybergouvernance, qui ignore souvent les réalités culturelles et les capacités nationales, est fréquente dans les juridictions africaines.

III.2. Idéologies sur la souveraineté numérique

La souveraineté numérique est un débat de plus en plus récurrent dans les discours sur la cybergouvernance internationale (*Schmitt* : 2017). Elle est particulièrement interprétée comme une préoccupation majeure pour les gouvernements africains (*Delport* : 2021). La nature sans frontières

[24] La loi nigériane de 2015 sur la cybercriminalité (interdiction et prévention). En 2020, la Cour de la CEDEAO a statué que l'adoption par le Nigeria de l'article 24 de la loi de 2015 sur la cybercriminalité (interdiction et prévention) constituait une violation du droit à la liberté d'expression.

de l'Internet pose des problèmes à de nombreux États africains qui ont l'habitude de contrôler toutes les activités sur leur territoire, ce qui explique la résurgence constante du discours sur la souveraineté numérique dans la région. Il arrive régulièrement que des gouvernements africains restreignent l'accès des citoyens à l'Internet,[25] manifestement en raison d'une mauvaise compréhension de l'agenda de la cybergouvernance (*Lewis* : 2017). Les Normes des Nations Unies sur le comportement responsable des États dans le cyberespace appellent les États à respecter les résolutions du Conseil des droits de l'homme et de l'Assemblée générale des Nations Unies visant à promouvoir et à protéger la jouissance des droits de l'homme sur Internet.[26] Des experts et hauts fonctionnaires des Nations Unies, y compris le Secrétaire général des Nations Unies, ont également affirmé officiellement que « les fermetures générales d'Internet et les blocages et filtrages génériques des services sont considérés par les mécanismes des Nations Unies relatifs aux droits de l'homme comme une violation du droit international relatif aux droits de l'homme ».[27] Cependant, la conception qu'ont les États africains des droits de l'homme et de la sécurité, associée à l'instabilité politique rampante dans la région, se heurte souvent à la réalité et aux attentes des cadres internationaux des droits de l'homme (*Calandro* : 2021). La volonté de contrôler l'Internet est toujours considérée comme une mesure de cybersécurité et de sécurité nationale et comme un rétablissement de la souveraineté numérique par ces États africains (*Ifeanyi-Ajufo* : 2021).

Dans l'ensemble, ces défis signifient que les normes relatives au comportement responsable des États dans le cyberespace[28] sont largement théoriques dans un contexte africain. Si les États

[25] En juin 2021, le gouvernement nigérian a interdit l'utilisation de Twitter dans le pays et a menacé de poursuivre tout Nigérian qui violerait cette interdiction. Le gouvernement éthiopien est devenu célèbre pour ses fermetures d'Internet et a été décrit comme l'un des pires au monde en la matière. La Tanzanie, la Zambie, l'Ouganda, le Zimbabwe, le Togo, le Burundi, le Tchad, le Mali et la Guinée ont également restreint l'accès à l'internet ou aux applications de médias sociaux à différents moments, notamment pendant les élections. Les rapports montrent qu'en un an, au moins dix pays africains ont bloqué ou interdit l'accès à l'internet ou restreint les cyber-activités par diverses mesures.

[26] Voir la norme 5 des Normes des Nations unies relatives au comportement responsable des États dans le cyberespace. ("Les États, en assurant l'utilisation sécurisée des TIC, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et la jouissance des droits de l'homme sur l'internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère numérique, afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression").

[27] Déclaration conjointe sur la liberté d'expression et les réponses aux situations de conflit Déclaration conjointe du rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression, du représentant de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias, du rapporteur spécial de l'Organisation des États américains (OEA) sur la liberté d'expression et du rapporteur spécial de la Commission africaine des droits de l'homme et des peuples (CADHP) sur la liberté d'expression et l'accès à l'information, présentée à l'occasion de la Journée mondiale de la liberté de la presse de l'UNESCO, le 4 mai 2015. Déclaration commune sur la liberté d'expression et les réponses aux situations de conflit - OSCE

[28] G7 Declaration on Responsible States Behavior in Cyberspace, Lucca, 11 April 2017. https://www.mofa.go.jp/files/000246367.pdf

africains ne sont pas les seuls à tenter de contrôler ou de restreindre l'Internet, au-delà de la politisation, le manque de ressources des institutions africaines, qui manquent souvent de compétences, de capacités et de ressources financières pour mettre en œuvre des mesures efficaces de cybergouvernance, peut signifier que suivre de telles approches sera plutôt contre-productif. Compte tenu de la faiblesse de la région en matière de cybergouvernance, il est plus avantageux pour les États africains d'investir dans la coopération et de poursuivre un programme de coopération internationale visant à améliorer la cybergouvernance.

III.3. Stratégies de coopération numérique

La nécessité de combler les lacunes institutionnelles dans les structures de coopération numérique présente des défis politiques (*The United Nations* : 2021). Les États africains ont continué d'explorer la manière dont un programme de coopération numérique peut placer l'Afrique dans une position stratégique pour gouverner efficacement le cyberespace (*Calandro* : 2021), mais le colonialisme reste une question sensible pour l'Afrique et est souvent au centre des interprétations de l'intervention occidentale (*Said* : 1993 ; *Said* : 1978 ; *Hardt & Negri* : 2000 ; *Dunch* : 2002). Par conséquent, la coopération numérique et sa relation avec la cybergouvernance doivent également être considérées en termes de sphères d'influence. L'Afrique craint que diverses initiatives extérieures ne visent l'impérialisme numérique plutôt que la coopération numérique. La tentative constante des gouvernements africains de mettre l'accent sur la souveraineté numérique peut être considérée comme une résistance subtile à toute forme de domination numérique dans la région. Les États africains ont commencé à remettre en question les stratégies de coopération existantes et insistent de plus en plus sur le fait que la coopération numérique devrait plutôt se dérouler selon les conditions de l'Afrique (*Teevan* : 2001). Il n'existe pas de stratégies internationales claires sur la manière de garantir l'égalité numérique. Pour que la coopération prospère, l'égalité numérique, plutôt que le seul renforcement des capacités, devrait être au premier plan du discours. Une mesure de l'égalité des normes en termes de capacité et d'infrastructure numériques devrait être un programme central pour la coopération numérique, plutôt que de se concentrer simplement sur le renforcement des capacités basé sur la charité. Il faut également tenir compte du fait que les technologies numériques ne sont pas principalement construites en Afrique, ce qui peut impliquer que l'idée du mécanisme de conception des technologies émergentes est imprégnée d'intérêts étrangers.

La Chine et la Russie ont été des acteurs clés de la coopération en Afrique (*Bowmans* : 2020). La Chine et la Russie sont également considérées comme des partenaires clés pour le renforcement de la cybersécurité dans de nombreux États africains (*Citation* : 2021). La Chine a joué un rôle clé dans la fourniture d'infrastructures TIC aux États africains, notamment en étant présente dans les locaux du siège de l'Union africaine. L'intérêt de la Chine pour le paysage africain de la cybersécurité ne peut être dissocié du fait que la Chine conçoit et produit des produits et services numériques qui sont principalement utilisés en Afrique (*Solomon* : 2021). Ces dernières années, l'influence de la Russie sur la gouvernance en Afrique[29] a dépassé celle de tout autre acteur extérieur en poursuivant la coopération sur différentes trajectoires telles que l'extension de l'influence militaire et sécuritaire, y compris l'influence cybernétique.[30] La Russie semble prête à créer son propre Internet souverain,[31] et comme les approches de coopération ont tendance à refléter les approches de gouvernance nationales, il est logique d'affirmer que les approches russes et chinoises de la cybergouvernance ont un effet profond sur l'élaboration de l'agenda africain de la cybergouvernance (*Klinwachter* : 2022).

III.4. Les défis de la cyberdiplomatie

Il serait vain de séparer l'agenda de la cyberdiplomatie de l'agenda général de la diplomatie en Afrique. La manière dont les nations africaines ont tendance à voter dans les processus diplomatiques et dont elles soutiennent d'autres États dans les processus diplomatiques internationaux repose sur des fondements politiques. Par exemple, alors que seuls cinq pays africains ont ratifié la Convention de Budapest du Conseil de l'Europe, trente-deux pays africains ont voté en faveur de la résolution de décembre 2018 soutenue par la Russie qui demandait au Secrétaire général des Nations unies de recueillir les points de vue des pays sur la cybercriminalité. Plus de trente (30) pays africains ont également voté en faveur de la résolution de l'Assemblée générale des Nations Unies de décembre 2019, motivée par la Russie, qui vise à créer un nouveau traité sur la cybercriminalité.[32]

[29] Africa Centre for Strategic Studies 'Russia in Africa' September 24, 2021. Russia | Topic in Focus – Africa Center for Strategic Studies
[30] The Geopolitical and Potential Cyber Influence of Russia in Africa October 31, 2019 The geopolitical and potential cyber influence of Russia in Africa (lab52.io)
[31] WIRED 'Russia Inches Towards Its Splinternet Dreams. April 1, 2022 Russia Inches Toward Its Splinternet Dream | WIRED
[32] United Nations General Assembly Resolution A/74/401 'Countering the use of information and communications technologies for criminal purposes' 25 November 2019.

L'Afrique est plus désavantagée en termes de cyber diplomatie et de participation aux divers processus diplomatiques de cyber gouvernance. Les pays africains ont été largement absents des processus de l'ONU sur l'élaboration de normes en matière de cybernétique. Par exemple, bien qu'il ait été dit que les membres du Groupe d'experts gouvernementaux (GGE) des Nations unies sont sélectionnés sur la base d'une répartition géographique équitable, en réalité, l'Afrique n'est pas toujours prise en compte dans ces processus de la même manière que les autres régions. Depuis 2004, seules neuf nations africaines sont membres du Groupe d'experts gouvernementaux des Nations unies (*Calandro* : 2021). Le GGE et l'OEWG ont énormément progressé en termes de discussions sur la cybergouvernance, mais ces discussions n'ont pas suffisamment pris en compte et reflété les intérêts de l'Afrique. Les réalités et les capacités nationales de l'Afrique n'ont pas été prises en compte au premier plan des processus de la même manière que celles d'autres régions (*Schmitt & Vihul* : 2017). L'analyse du Conseil de sécurité de l'ONU lors du premier débat sur les technologies émergentes réaffirme le fait que les inégalités numériques signifient qu'en réalité, il y a peu de pays qui définissent l'agenda numérique pour le reste du monde (*Roberts* : 2021). Une fois encore, comme l'Afrique manque de cyber-diplomates qualifiés, il devient tout aussi difficile de promouvoir les intérêts africains dans les processus cyber-diplomatiques (*Union africaine* : 2018).

III.5. La capacité numérique de l'Afrique

Les normes internationales en matière de cybergouvernance se heurtent souvent aux réalités des pays en développement, en particulier de la région africaine, qui se trouvent à l'extrémité de la fracture numérique et n'ont pas les capacités, les compétences et les infrastructures nécessaires pour assurer efficacement une cybergouvernance conforme aux normes internationales (*Calandro* : 2021). Selon *Castells*, l'infrastructure TIC de l'Afrique est maigre par rapport aux normes mondiales actuelles et, en comparaison, il y a plus de lignes téléphoniques à Manhattan ou à Tokyo que dans l'ensemble de l'Afrique subsaharienne (Castells : 2001). Selon lui, la différenciation entre les nantis et les démunis en matière de TIC « ajoute un clivage fondamental aux sources existantes d'inégalité et d'exclusion sociale dans une interaction complexe qui semble creuser le fossé entre la promesse de l'ère de l'information et sa sombre réalité pour de nombreuses personnes dans le monde » (*Castells* : 2001). Il est donc littéralement impossible pour des régions comme l'Afrique de participer efficacement aux discours sur la cybergouvernance internationale. D'autres problèmes

d'infrastructure se posent dans la région. En plus d'être la région la moins numérisée du monde, de nombreux pays d'Afrique manquent également d'infrastructures minimales, telles que l'électricité, nécessaires pour faire progresser les avantages des technologies numériques, ce qui rend absurdes les efforts internationaux en matière de cybergouvernance dans le contexte de l'Afrique. Associé au manque d'accès aux infrastructures de base et aux conflits politiques incessants, le programme de transformation numérique de l'Afrique n'est pas clair, ce qui rend le débat sur la capacité numérique encore plus difficile à conceptualiser.

IV. Renforcer la cybergouvernance en Afrique par la coopération

Après avoir examiné les stratégies juridiques et politiques existantes en matière de cybergouvernance en Afrique, il est important de se pencher sur la manière dont la coopération peut être mise à profit pour renforcer la cybergouvernance en Afrique. La coopération en tant que stratégie encourage les États à établir des partenariats stratégiques et à s'engager sur le plan multilatéral. Il faut en tenir compte dans la mise en œuvre de la stratégie de transformation numérique de l'Union africaine (*Ayodele* : 2021). La coopération sera de plus en plus une condition préalable à la réalisation de la cyber stabilité. Pour promouvoir la confiance et la sécurité dans l'environnement numérique, il est nécessaire de se concentrer sur la stabilité dans le cyberespace en respectant les Normes de comportement responsable des États,[33] y compris les mesures de coopération qui peuvent contribuer à prévenir la cyber-instabilité.[34] Les normes mettent l'accent sur la coopération internationale.[35] Divers efforts ont été déployés pour assurer la cybergouvernance par la coopération. Pour la région africaine, l'Union européenne et le Conseil de l'Europe ont déployé des efforts de coopération plus transparents.[36] Ces efforts de coopération interrégionale ont notamment porté sur l'amélioration de l'élaboration des cyber-politiques et le

[33] Le groupe d'experts gouvernementaux des Nations unies (GGE) a adopté par consensus en 2010, 2013 et 2015 des normes relatives au comportement responsable des États dans le cyberespace. Les normes des Nations unies relatives au comportement responsable des États dans le cyberespace.

[34] Voir la norme 4 des 11 normes non contraignantes relatives au comportement responsable des États dans le cyberespace du Groupe d'experts gouvernementaux des Nations unies.

[35] Voir les normes 1 et 4 des normes des Nations unies relatives au comportement responsable des États dans le cyberespace.

[36] African Union Commission April 12, 2018 'African Union Commission and Council of Europe Join Forces on Cybersecurity' African Union Commission and Council of Europe Join Forces on Cybersecurity | African Union (au.int)

renforcement des cyber-capacités.[37] L'Europe a déjà commencé à mettre en œuvre une stratégie globale avec l'Afrique qui aidera le continent à concevoir et à mettre en œuvre ses propres solutions aux défis locaux dans les orientations politiques de la Commission européenne pour la période 2019-2024.[38]

Compte tenu de la nature du cyberespace, le multilatéralisme est un impératif pour la cybergouvernance. Il est impossible pour un État africain d'assurer la cyber stabilité et d'endiguer les cybermenaces sans coopération. Les cyber-activités dépassent les frontières nationales et l'Afrique peut assurer la coopération en encourageant des politiques de cybergouvernance appropriées. Selon *Calandro*, « la préservation de la cyber stabilité est un effort de collaboration, et les acteurs étatiques des pays africains doivent concevoir des mécanismes de coopération pour observer et mettre en œuvre des normes et les inclure dans leur politique ou stratégie nationale en matière de cyber » (*Calandro* : 2021).

Si la Convention de Malabo aide les États africains à élaborer des lignes directrices et sert de modèle de législation que les États membres pourront adopter en matière de cybersécurité, elle n'est pas sans poser de problèmes (*Zahid* : 2016). L'anatomie de la convention de Malabo — la fusion de la cybersécurité et de la protection des données — constituera un revers, notamment parce que les dispositions de la convention relatives à la protection des données ne sont pas directement formulées en termes de cybersécurité. Dans le Règlement général sur la protection des données (RGPD) de l'Union européenne, par exemple, ces questions sont séparées. Dans l'ensemble, la plupart des définitions de la Convention de Malabo sont moins complètes que celles que l'on trouve dans des instruments similaires tels que la Convention de Budapest. L'idée que les conventions de Malabo et de Budapest sont concurrentes et présentent donc des intérêts divergents peut également poser problème. Il est important que les États africains comprennent que les lois et conventions modèles telles que les conventions de Budapest complètent la convention de Malabo et ne la remplacent pas. Le champ d'application de la Convention de Malabo est beaucoup plus large que celui de la Convention de Budapest, ce qui est un aspect positif de la Convention, étant

[37] The Africa-EU Partnership 'Policy and Regulation Initiative for Digital Africa (PRIDA)' Policy and Regulation Initiative for Digital Africa (PRIDA) | The Africa-EU Partnership (africa-eu-partnership.org)

[38] European Union Political guidelines for the next Commission (2019-2024) - "A Union that strives for more: My agenda for Europe" 16 July 2019 Political guidelines for the next Commission (2019-2024) - "A Union that strives for more: My agenda for Europe" | European Commission (europa.eu).

donné qu'elle réglemente la cybersécurité, la sécurité des données et la sécurité des transactions électroniques.

Pour garantir une cybergouvernance efficace, les politiques doivent orienter l'engagement de tous les acteurs concernés vers la réalisation d'une cybergouvernance efficace. La Convention de Malabo le souligne dans son article 26.[39] Il est important de noter que la Convention de Malabo est axée sur la protection des droits de l'homme. La Convention contient des dispositions relatives à la protection des données qui couvrent le contrôle des données personnelles. La Convention exige également des gouvernements qu'ils respectent la Charte africaine des droits de l'homme et des peuples,[40] ainsi que d'autres droits fondamentaux tels que la liberté d'expression, le droit à la vie privée et le droit à un procès équitable, entre autres. La Convention enjoint les États partis à adopter des lois sur la cybersécurité qui tiennent compte de leur constitution et des conventions internationales relatives aux droits de l'homme. Elle complète largement les dispositions de la Convention de Budapest.

Il est nécessaire de renforcer l'obligation d'accorder la priorité à la cybergouvernance en Afrique. Lors de l'élaboration et de la conception d'un programme de coopération numérique avec la CUA et les États membres de l'UA, d'autres organisations régionales, États et parties prenantes devraient réexaminer les stratégies de coopération numérique existantes (*Ifeanyi-Ajufo* : 2022). À l'avenir, la réalité de l'Afrique doit être prise en compte de manière stratégique dans les divers programmes de coopération numérique. Les lacunes en matière de capacités ne sont pas nécessairement les mêmes d'une région à l'autre, de sorte que les tentatives de renforcement des cyber-capacités en Afrique doivent être abordées de manière ciblée, et les transferts de capacités et d'expertise doivent faire l'objet d'une stratégie visant à garantir que la coopération numérique ne se traduise pas par une dépendance numérique (*Teevan* : 2001).

Conclusion

Alors que les conversations sur la transformation numérique continuent de prendre de l'importance dans la région, l'Afrique doit créer son propre programme de cybergouvernance.

[39] Voir l'article 26 (1-4) de la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, 2014.
[40] African Charter on Human and Peoples' Rights, 1981.

L'Afrique a besoin d'un cadre clair en matière de cybergouvernance et une approche unifiée pourrait être utile. La ratification de la Convention de Malabo par les États membres africains pourrait être la panacée pour un continent uni avec des normes, des standards et des principes partagés, fournissant une base préalable pour une approche commune de la cyber gouvernance à travers la région. La CUA et les États membres de l'UA devraient fournir les ressources nécessaires pour assurer la ratification de la convention de Malabo et exhorter les États membres de l'UA à faire le point sur les dispositions de la convention de Malabo afin de promouvoir la cybergouvernance dans la région.

L'importance de la coopération dans le domaine de la cybergouvernance se traduira aussi essentiellement par l'adhésion à la convention de Budapest. Cela sera particulièrement important pour la coopération internationale. En ratifiant la Convention de Budapest, les pays africains se donneront de meilleures chances de bénéficier d'un soutien international et d'une assistance juridique et technique pour promouvoir la cyber-résilience dans la région et faire avancer un programme africain sur la cybergouvernance (*Mbuvi* : 2011).

Au-delà de la ratification de ces instruments, les États africains doivent valoriser les partenariats stratégiques internationaux et régionaux et l'adoption des meilleures pratiques mondiales. Les organisations régionales ont un rôle clé à jouer dans la formulation des politiques et l'obtention de résultats en matière de cybergouvernance (*Nicholas* : 2018). Alors que l'Afrique poursuit sa transformation numérique, la CUA doit continuer à créer des dialogues pour réfléchir aux opportunités et aux défis pour assurer la cybersécurité en Afrique. Alors que les États poursuivent l'introduction de principes et de normes de cybergouvernance mondiale (*Xinmin* : 2016), ils doivent également poursuivre un programme multilatéral qui affirme de manière réaliste les normes cybernétiques comme des règles mondiales (*Smith* : 2017) et qui obligerait toutes les régions, y compris l'Afrique, à s'engager et à rendre compte des normes qui exigent une cybergouvernance appropriée pour assurer la paix et la stabilité dans le cyberespace. Selon la stratégie de transformation numérique de l'Union africaine, « à mesure que les États membres de l'Union africaine augmentent leur accès à la connectivité à large bande, ils deviennent plus interconnectés et plus vulnérables… » Il devient essentiel de renforcer nos capacités humaines et

institutionnelles pour sécuriser notre cyberespace en instaurant la confiance dans l'utilisation des cyber-technologies. "[41]

Références

African Union. (2018). 'Cyber Security and Cybercrime Policies for African Diplomats Cyber Security and Cybercrime Policies for African Diplomats.' African Union. [Google Scholar]

Ajijiola, A. & N. Allen. (2022). 'African Lessons in Cyber Strategy.' African Lessons in Cyber Strategy—Africa Centre for Strategic Studies. [Google Scholar]

Ayodele, O. (2021). 'The Digital Transformation of Diplomacy: Implications for the African Union and Continental Diplomacy.' South African Journal of International Affairs 28 (3): 379–401. doi:10.1080/10220461.2021.1968944. [Google Scholar]

Ball, K. (2017). 'African Union Convention on Cyber Security and Personal Data Protection.' International Legal Materials 56 (1): 164–192. doi:10.1017/ilm.2016.3. [Google Scholar]

Ball, K. (2017). 'African Union Convention on Cyber Security and Personal Data Protection.' International Legal Materials, 56 (1): 164–192. [Google Scholar]

Bowmans (2020). 'Russia and China in Africa: Development Allies or Geopolitical Opportunists?' www.bowmanslaw.com [Google Scholar]

Calandro, E. (2021). 'Partnering with Africa on Cyber Diplomacy,' EU Cyber Direct. [Google Scholar]

Castells, M. (2001). The Internet Galaxy: Reflections on the Internet. New York: Business, and Society Oxford University Press. [Google Scholar]

Clifford, C. (2022). 'Russia's efforts to promote cyber norms that serve its interests gain traction in Africa.' www.africaportal.org [Google Scholar]

Delport, J. (2021). 'The State of Cybersecurity in Africa.' The State of Cybersecurity in Africa - IT News Africa - Up to date technology news, IT news, Digital news, Telecom news, Mobile news, Gadgets news, Analysis and Reports. [Google Scholar]

[41] The African Union Digital Transformation Strategy for Africa (2020–2030), 44–45

Dunch, R. (2002). 'Beyond Cultural Imperialism: Cultural Theory, Christian Missions and Global Modernity.' History and Theory 41 (3): 301–325. doi:10.1111/1468-2303.00208. [Web of Science ®], [Google Scholar]

European Union Commission. 2020. 'EU paves the way for a stronger, more ambitious partnership with Africa.' European Union Commission. [Google Scholar]

Finnemore, M., and K. Sikkink. (1998). 'International Norm Dynamics and Political Change.' International Organization 52 (4): 887–917. doi:10.1162/002081898550789. [Web of Science ®], [Google Scholar]

Handler, S. (2021). 'The 5 × 5—Cyber Capacity and Conflict in Africa' The Cyber Statecraft Initiative The 5 × 5—Cyber capacity and conflicts in Africa - Atlantic Council. [Google Scholar]

Hardt, M. & A. Negri. (2000). Empire. Cambridge: Harvard University Press. [Google Scholar]

Ifeanyi-Ajufo, N. (2021). 'Net-Politics in Africa,' EU Cyber Direct. https://directionsblog.eu/net-politics-in-africa/ [Google Scholar]

Ifeanyi-Ajufo, N. (2022). 'International Co-operation and Cybersecurity in Africa,' EU Cyber Direct. [Google Scholar]

International Telecommunications Union 2021. 'Global Cyber Security Index 2020.' Global Cybersecurity Index. [Google Scholar]

International Telecommunications Union 2021 a. Are African countries doing enough to ensure cybersecurity and Internet safety? https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/ [Google Scholar]

International Telecommunications Union 2021b. *Global Cyber Security Index 2020*. [Google Scholar]

Kerttunen, M. & E. Tikk. (2019). 'The Politics of Stability: Cement and Change in Cyber Affairs.' Published by the Norwegian Institute of International Affairs. NUPI_Report_4_2019_KerttunenTikk.pdf (unit.no). [Google Scholar]

Klinwachter, W. (2022). 'Internet Governance Outlook 2021: Digital Cacophony in a Splintering Cyberspace.' www.circleid.com [Google Scholar]

Lewis, J. (2017). 'Fighting the Wrong Enemy: aka the Stalemate in Cybersecurity' The Cipher Brief. https://www.thecipherbrief.com/column/expert-view/fighting-the-wrong-enemy-aka-the-stalemate-in-cybersecurity [Google Scholar]

Meyer, P. (2020). 'Norms of Responsible State Behaviour in Cyberspace.' In The ethics of Cybersecurity. The International Library of Ethics, Law and Technology, edited by Christen M., Gordijn B, Loi M, 347–360. Springer. [Google Scholar]

Microsoft. (2021). 'International Cybersecurity Norms: Reducing conflict in an Internet-dependent world.' www.microsoft.com [Google Scholar]

Mueller, M.L. (2020). 'Against Sovereignty in Cyberspace.' International Studies Review 22 (4): 779–801. [Web of Science ®], [Google Scholar]

Mbuvi, D. (2011). 'African States Urged to Ratify Budapest Cybercrime Convention." African States Urged to Ratify Budapest Cybercrime Convention | CSO Online. [Google Scholar]

Nicholas, P. (2018). 'The role that regions can and should play in critical infrastructure protection.' www.microsoft.com [Google Scholar]

Pawlak, P., and M. Tikk, and E. Kerttunen. 2020. 'Cyber Conflict Uncoded. The EU and Conflict Prevention in Cyberspace.' European Union Institute for Security Studies Conflicts Series Brief. [Google Scholar]

Potter, E. H. ed. (2002). Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century. Montreal, QC: McGill-Queen's University Press. [Google Scholar]

Roberts, M. M. (2021). 'The UN Security Council Tackles Emerging Technologies.' The UN Security Council Tackles Emerging Technologies | Council on Foreign Relations. [Google Scholar]

Said, E. (1978). Orientalism. London: Routledge. [Google Scholar]

Said, E. (1993). Culture and Imperialism. New York: Vintage Books. [Google Scholar]

Schlehahn, E. (2020). 'Cybersecurity and the State.' In The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, edited by M. Christen, B. Gordijn, M. Loi. Switzerland: Springer. [Google Scholar]

Schmitt M. N. (ed. 2017). The Tallinn Manual on the International Law Applicable to Cyber Operations. New York: Cambridge University Press. [Google Scholar]

Schmitt, M. & L. Vihul. (2017). 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms.' https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [Google Scholar]

Smith, B. (2017). 'The Need for a Digital Geneva Convention.' https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [Google Scholar]

Solomon, S. (2021). 'Experts: Report of China Hacking African Union HQ Fits Larger Pattern.' Experts: Report of China Hacking African Union HQ Fits Larger Pattern. www.voanews.com [Google Scholar]

Teevan, C. (2001). 'Building Strategic European Digital Co-operation with Africa.' Briefing Note: No. 134, The European Centre for Development Policy Management (ECDPM). [Google Scholar]

The United Nations (2021). 'The Age of Digital Interdependence.' Report of the UN Secretary General's High-level Panel on Digital Co-operation 2020. [Google Scholar]

Xinmin, M. (2016). 'Key Issues and Future Development of International Cyberspace Law.' China Quarterly of International Strategic Studies 02 (01): 119–133. doi:10.1142/S2377740016500068. [Google Scholar]

Zahid, J. (2016). 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime.' Cybercrime Programme Office of the Council of Europe. [Google Scholar]

À propos de l'Auteur :

NNENNA IFEANYI-AJUFO est professeur de droit et de technologie. Elle est vice-présidente du Groupe d'experts en cybersécurité de l'Union africaine (AUCSEG). Ses recherches portent principalement sur la gouvernance des technologies numériques, les droits numériques et l'État de droit dans le cyberespace.

À propos du LARC :

Le LARC (Laboratoire Africain de Recherches en Cyberstratégie) est un cadre de réflexion, créé par votre serviteur et regroupant des chercheurs pluridisciplinaires, avec pour mission de décrypter, d'analyser et d'anticiper les enjeux de demain dans le cyberespace africain.

Pour soutenir les activités du LARC ou y contribuer par vos propres publications, visitez notre site web : https://www.larc.africa

Pour citer cet article :

Version rééditée de [2023 : Nnenna Ifeanyi-Ajufo], « La cybergouvernance en Afrique : au carrefour de la politique, de la souveraineté et de la coopération », Note N° 11 — LARC, janvier 2024.