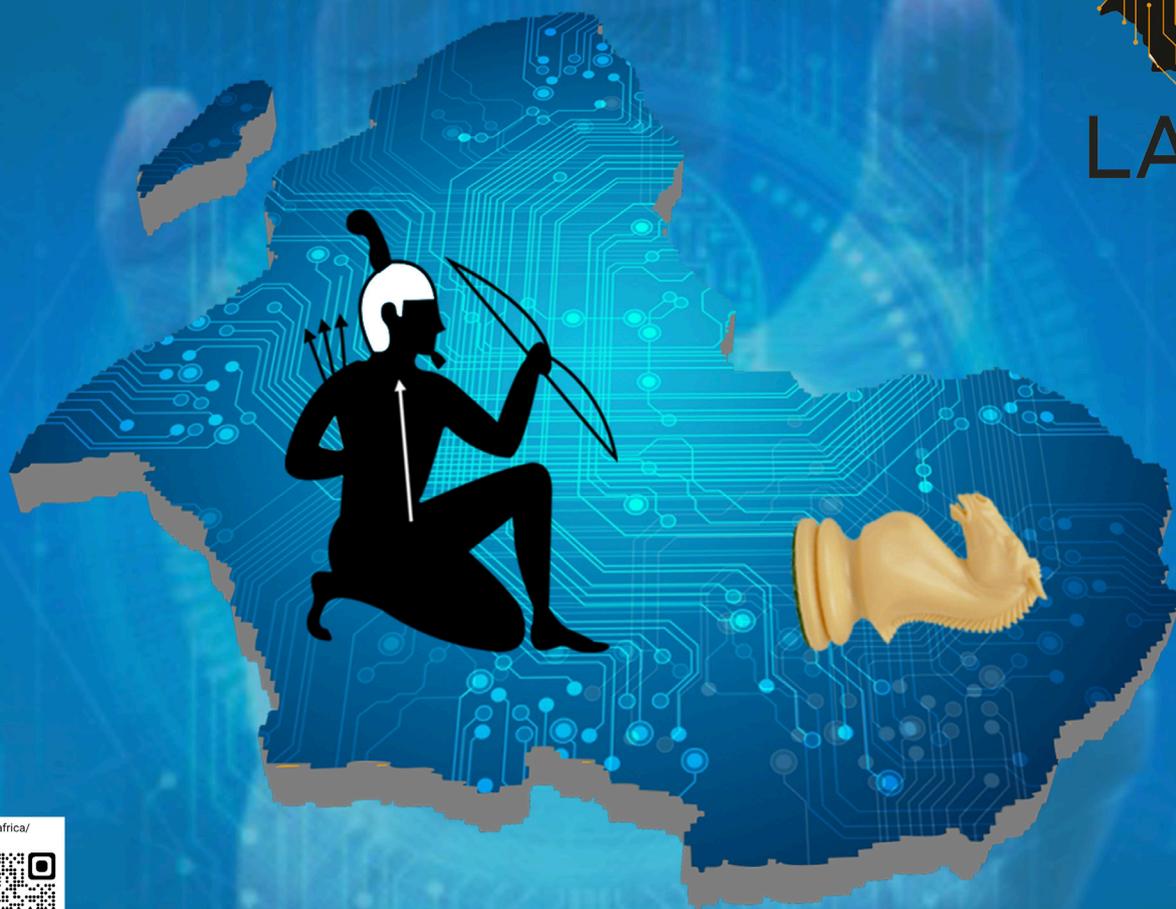


Magazine Africain de Cyberstratégie

Décrypter les enjeux de demain dans le cyberspace africain

MAC / n° 001 / Février 2024



L'INVITÉ P.07

«La plupart des États Africains n'intègrent pas encore la notion de rapports de forces, l'essence même de la stratégie».

DJINGOU NGAMENI

LE QUESTION-MAG P.10

«Comment comprendre les lenteurs et l'instabilité de l'accès à internet en Afrique Subsaharienne ?».

*Avec BAMAHOSSOVI Justin
et Dr ZEKENG NDAJI*

Sommaire

4 La Note de Rédaction

Les articles
Highlights

5

7

L'INVITÉ

9 Aux nouvelles

10

Le Question-Mag

12

L'actualité

16

Le choix de la rédaction

17

Les partenaires

À propos de nous

Derrière l'élaboration de votre rendez-vous semestriel, se trouve une équipe dynamique, passionnée et acharnée qui travaille sans relâche pour produire un magazine à la conquête des enjeux nouveaux du cyberspace africain pour l'Afrique.

Pr Isidore BIKOKO



Notre approche

Les recherches sont menées sous le joug d'un paradigme à la fois critique et descriptif.

Nos valeurs

- Défi
- Engagement
- Créativité
- Coopération
- Réflexion.



Léa Arselle TSAFACK



Leslie MBANGO

L'ÉQUIPE

Directeur de publication

François-Xavier DJIMGOU NGAMENI

Conseiller scientifique

Pr Isidore BIKOKO

Conseillère Technique

Leslie MBANGO

Rédactrice en chef

Léa Arselle TSAFACK NGULEFEM

Rédacteurs

Pr Nnenna IFEANYI-AJUFO

Pr José DO-NASCIMIENTO

Justin Oumar BAMAHOSSOVI

Dr William Maxime ZEKENG NDADJI

Fabiola NGUESSIE

Conception

Bertrand FINI

La note de la rédaction

À propos du magazine

Rendus à l'évidence de ce que le cyberspace continue de faire couler l'encre sur ses usages et risques au détriment de ses potentialités pour l'Afrique, le MAC a été pensé. C'est un éditorial scientifique qui s'intéresse d'une part à toute forme d'actualité relative à la cyberstratégie africaine ; d'autre part aux activités et projets de la structure qui la couvre notamment le LARC. Le MAC bénéficie de la même crédibilité



que le LARC qui l'accueille et se veut compétitif en ce sens où ses intentions sont novatrices pour le numérique africain.

Avis aux auteurs

En intervenant dans le MAC, les rédacteurs ont une vitrine de vulgarisation de leur avis quant au débat stratégique en cours sur le cyberspace africain. Les déclarations des auteurs n'engagent pas la rédaction. Toute responsabilité étant due au propriétaire de la pensée.

Toute contribution d'article doit formellement rejoindre les objectifs du MAC et par ricochet ceux du LARC tels que précisés sur le site www.larc.africa

Note aux lecteurs

Ravis de vous soumettre cette première édition de notre Magazine. Prenez plaisir à parcourir les divers articles et rubriques proposés. N'hésitez pas à nous faire un retour sur vos impressions et suggestions pour les prochains numéros. Soyez également ce relais entre nous et votre entourage passionné des questions cyber.

*Humblement,
la rédaction du MAC*

Les articles Highlights

Rubrique consacrée à la mise en évidence de quelques articles sensibles d'intérêt récemment publiés chez le LARC. Intégrant notre grille de lecture, ces auteurs nous transportent vers un univers où le cyberspace cesse d'être un lieu d'affrontements pour devenir un objet scientifique à saisir. Sous des axes que vous retrouverez certainement, notamment la Gouvernance, la Technologie et la Stratégie, appréciez la quintessence de ces articles qui vous est livrée dans ce numéro de votre magazine.

Dossier n°1 : La cybergouvernance en Afrique : au carrefour de la politique, de la souveraineté et de la coopération

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 des mécanismes de cybergouvernance appropriés, et 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 cyberspace 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 politiques et 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.

Pour lire l'intégralité de ces articles, rendez-vous sur notre site web via les liens mentionnés ci-dessous : <https://larc.africa/category/gouvernance/>

Présentation de l'auteur

NNENNA IFEANYI-AJUFO est professeur de droit et de technologie à la Leeds Law School, Leeds Beckett University, du Royaume-Uni. Ses recherches portent principalement sur la gouvernance des technologies numériques, les droits numériques et l'État de droit dans le cyberspace.

Nnenna est une **experte reconnue dans les domaines du droit et de la technologie**. Elle a contribué à la rédaction d'études académiques sur la gouvernance des technologies numériques. Elle occupe plusieurs postes importants dans des organisations internationales liées à la cybersécurité et à la gouvernance numérique en Afrique. Elle est **vice-présidente du Groupe d'experts en cybersécurité de l'Union africaine (AUCSEG)** et a activement conseillé la Commission de l'Union africaine (CUA) et les États membres africains sur les cadres juridiques internationaux, régionaux et nationaux liés à la cybersécurité et à l'État de droit dans le cyberspace, ainsi que sur la promotion de la cybergouvernance dans la région. Elle a reçu plusieurs prix et bourses.

En 2020, elle a été nommée parmi les **50 personnes à la tête de l'innovation juridique en Afrique** lors des Africa Legal Innovation Awards.

Dossier n°2 : Transhumanisme et Intelligence artificielle face à l'axiologie africaine.

Il est temps de mener une réflexion axée sur les enjeux stratégiques des NTIC plus précisément de deux de ses technologies à savoir le transhumanisme et l'Intelligence Artificielle. L'Afrique a nul besoin de s'accommoder totalement de toutes les avancées numériques qui lui sont offertes sans les passer au crible de la pensée africaine. Déroulant la portée surtout régressive de ces nouveaux apports technologiques, on se rend bien compte que le remplacement de l'Homme ou sa substitution par des outils technologiques indépendants n'entraîne pas uniquement des portées bénéfiques mais aussi et surtout cette évolution provoque la fin de l'humanité. L'objectif de la présente réflexion est bien de relever les risques liés à long et à court terme des Nouvelles Technologies. Plus clairement, il s'agit de mettre en avant les facteurs de durabilité défaillants des technologies innovantes qui nous sont proposées par l'IA et pourtant inhérents à la survie de l'humanité. De là, naît le besoin heuristique d'intégrer la notion de durabilité lors de nos usages courants des Nouvelles Technologies afin que les risques majeurs liés à leur utilisation soient mesurés, voire dominés par leurs potentialités. Ceci dit, comment introduire une logique de durabilité dans notre rapport

aux usages des NT que la Raison et la Science mettent à notre disposition ? La première étape est de réévaluer la nature de nos rapports avec ces NT. La conception africaine doit envisager les NT comme un objet dont il peut disposer, stratégiquement parlant bien évidemment, sans risquer de devenir l'outil de ces technologies innovantes. La deuxième étape est de considérer la pensée africaine, mieux celle bantou pour établir une nouvelle approche (complémentaire plutôt qu'empirique) entre les êtres et les techniques dont ils disposent. Auquel cas, nous risquons un effet boomerang de ces technologies nouvelles sur nous. Par ailleurs, la régulation (veille) doit régir la mise sur pied et l'utilisation publique des Intelligences Artificielles.

Mots clés : Transhumanisme, axiologie africaine, stratégie de gouvernance, intelligence artificielle.

Pour lire l'intégralité de ces articles, rendez-vous sur notre site web via les liens mentionnés ci-dessous : <https://larc.africa/category/strategie/>

Présentation de l'auteur

JOSÉ DO-NASCIMENTO est juriste et politologue. Actuellement chercheur à l'IDEST de l'Université Paris-Saclay en France, il est également président de l'association de recherche sur les perspectives de la modernité en Afrique (ARPEMA) et membre de la Research Team Members du MINDS (Mandela Institute for Development Studies) en charge du programme de recherche, *African Heritage Research Study*. Ses sujets de prédilection sont le panafricanisme, la géopolitique, la renaissance africaine, la politique, la gouvernance, la pensée africaine, l'épistémologie, etc...

José Do-Nascimento est également auteur de plusieurs ouvrages à succès, tous consacrés à l'Afrique, dont le dernier *L'Afrique au risque d'une cybercolonisation* (L'Harmattan, 2017 Hors-série, Collection Études Africaines) est copublié avec DJIMGOU NGAMENI. Fortement influencé par la pensée de Cheikh Anta Diop, il lui consacre un ouvrage intitulé *La pensée politique de Cheikh Anta Diop* (L'Harmattan : 2021)

Pour lui, l'Afrique n'accuse pas de retard quelconque, elle a plutôt subi une régression due à la doctrine du développement. Il déclare à cet effet lors d'un entretien autour de son livre *Les chemins de la modernité en Afrique* (L'Harmattan : 2017) accordé à *Thinking Africa* en 2018 :

« Il faut abandonner le développement comme perspective de modernité (...) la renaissance africaine est réellement une alternative comme perspective de modernité. »

L'invité

Ce semestre, le MAC est allé à la rencontre d'un expert en cyberstratégie, entrepreneur acharné et entièrement dévoué à la promotion d'une idée, le LARC. Vous l'aurez compris, l'auteur de Souveraineté numérique et cyberdéfense : un enjeu de taille pour l'Afrique s'est prêté à notre exercice d'interview. Suivons ensemble cet entretien de la rédaction afin de cerner le parcours instructif d'un chercheur.

Rédaction MAC : D'où part L'expert en cyberstratégie ?

Invité : J'ai toujours été passionné par les mécanismes de sécurité des systèmes d'information, surtout par le lien entre cybersécurité et Intelligence Économique... À ce titre, j'ai nourri mon intérêt pour ces thématiques en m'informant sur les impacts liés aux entreprises et aux États. En tant qu'ingénieur réseau et cybersécurité, puis analyste des renseignements sur les cybermenaces, j'ai exploré ces problématiques pour le compte de diverses entreprises aussi bien au Cameroun qu'à l'étranger. Mon passage à l'École de Guerre Économique de Paris (MBA option cybersécurité) m'a également permis d'assimiler les notions de grille de lecture, rapport de forces, rivalités de pouvoir. J'ai pu mieux cerner comment ces notions s'appliquent aussi au cyberspace. L'expert en cyberstratégie est le produit de ce parcours et de ma curiosité naturelle pour le domaine de la stratégie.

R : Quels moments clés ont été décisifs dans votre choix de carrière ?

I : Au-delà de mes formations, ce sont mes observations et expérience à l'étranger qui consti-



tuent le fondement de mon dévouement à la cyberstratégie. Tout au long de mon parcours, en tant qu'analyste des menaces cybers entre autres, j'ai vu à quel point les problématiques de protection des systèmes d'information pouvaient déstabiliser les différentes organisations pour lesquelles j'ai travaillé, et ne pouvais m'empêcher une comparaison avec la situation des organisations africaines dont le niveau de maturité cyber demeure des plus faibles au monde. J'ai dès lors commencé à intervenir pour certaines organisations comme consultant en cybersécurité notamment sur les aspects stratégie et gouvernance.

Qu'est-ce qui pousse un Ingénieur et consultant en œuvre à mettre sur pied un laboratoire sous couvert d'une entreprise à but non lucratif ? Y avait-t-il un manque derrière cette initiative ?

Professionnellement parlant non, mon parcours me prédisposait à des perspectives intéressantes. C'est plus une question de conviction. Avec mon premier ouvrage, j'ai pu émettre un constat sur la guerre cybernétique en cours dans le monde sans manquer de décrypter les concepts de souveraineté numérique et de cyberdéfense. J'insistais sur l'angle mort que tout ceci représente pour l'Afrique surtout en ce qui concerne la réflexion sur la protection du cyberspace. Après quoi je me suis dit, si les décideurs que tu interpellés te demandaient comment faire pour élaborer une stratégie pour leur État dans le cyberspace tel que tu le leur suggères, à partir de quels éléments travailleraient-ils ? Le deuxième constat alarmant a été qu'il n'y avait pas de réponse. L'idée du laboratoire naît de la nécessité de créer un espace de réflexion pour contribuer à combler ces manquements.

Quelles étaient vos motivations en fondant le LARC ?

I : Tandis qu'ailleurs le cyberespace est entériné comme milieu stratégique c'est-à-dire comme théâtre d'opérations militaires, la plupart des États africains dans leur stratégie de transformation numérique n'intègrent pas encore de dialectique de volonté entre États. La notion de rapport de forces étant l'essence même de la stratégie. L'idée du LARC était et demeure de proposer un corpus de connaissances traitant de ces problématiques, afin de permettre aux cibles africaines d'avoir de la matière pour concevoir leur stratégie propre, partant de l'Afrique comme épicentre de la réflexion.

En quoi ce laboratoire participe-t-il de votre ascension ? êtes-vous à présent comblé ?

En tant qu'individu je ne recherche pas d'ascension particulière avec cette initiative. C'est une vision d'intérêt public, c'est pourquoi les articles sont gratuits. L'objectif est de diffuser au maximum ce contenu afin d'ouvrir le débat sur des thématiques récentes relatives au cyberspace, et encore absentes de nos grilles d'analyse habituelles. C'est parce que j'ai essayé de répondre à une question pour laquelle je n'ai pas trouvé de réponse existante que j'ai décidé d'en proposer. Mon vœu est de poser les jalons pour que d'autres chercheurs puissent poursuivre la réflexion.

D'où part la nécessité d'une vitrine médiatique telle que le MAC ? Intègre-t-il vos notions ?

Oui, le MAC rejoint la vision du LARC en ce sens où il est question de diffuser d'une nouvelle façon les idées du laboratoire en donnant la parole à divers acteurs pertinents pour notre problématique, notamment une grille de lecture axée sur les enjeux dans le cyberespace. La nécessité du MAC part du fait que malgré les cinq ans d'ancienneté du laboratoire, il y a toujours très peu d'acteurs de l'écosystème de la cybersécurité qui traitent des problématiques de cyberstratégie. Alors le MAC se veut ce média qui

La cyberstratégie est un domaine à fort potentiel

s'appuie sur la vision du LARC pour diffuser toutes les productions centrées sur les notions d'enjeux, de conflictualité et de rivalité dans le cyberspace qui manquent aux autres supports existants. Par ailleurs, c'est un signe d'évolution du laboratoire dans son processus d'autonomie d'édition de ce qui s'avère spécifique à l'Afrique.

À quoi devons-nous nous attendre ? Des projets pour 2024 ?

Oui, la parution du Tome II de l'ouvrage Cyberstratégie Africaine est prévue. Celui-ci sera axé sur une proposition de modèle d'innovation technologique endogène mais aussi sur l'idée d'un Programme Africain d'Industrialisation Numé-

rique sur lequel le laboratoire se penche actuellement. En plus bien sûr de relever la contre-histoire de l'évolution de la science informatique que nous développons également. Nous aurons l'occasion d'y revenir après la parution. Je suis aussi porteur d'un projet d'Académie, pour faciliter la diffusion de ce corpus que nous créons autour de la cyberstratégie africaine. Notre plus-value sera de ne pas se limiter à former des Ingénieurs en Technologies numériques mais de produire des cyber-stratèges/cyber-stratégistes capables d'alimenter la grille de lecture stratégique sur les problématiques de transformation numérique en Afrique.

Quel message pour le public jeune qui a du mal à envisager une carrière similaire en contexte camerounais ?

Premièrement ils doivent croire que c'est possible, il suffit de travailler ardemment. Deuxièmement ils doivent se rendre à l'évidence que l'avenir du cyberspace ne peut plus faire fi des problématiques de protection, donc de cybersécurité voire de cyberdéfense. Ainsi, un profil bien formé sur des questions relevant de stratégie appliquée au cyber a plus de chances de construire une carrière. C'est un domaine ayant de belles perspectives car l'impact de la cybersécurité se fait de plus en plus important pour le fonctionnement de nos entreprises et même de nos États.

Propos recueillis par la rédaction du MAC

Aux nouvelles

POINT I : Académie

Ce point permet de vous faire le débrief sur les écoles et/ou formations à venir. Ce sont majoritairement des services offerts par les partenaires du Laboratoire et le LARC lui-même.



Pour ce numéro, nous avons choisi de vous parler d'un projet encore embryonnaire certes, mais qui a bien l'intention de ravir votre attention. Le LARC

envisage pour le deuxième semestre de l'année en cours, de proposer au public africain des formations certifiantes de qualité en Cyberstratégie. Ces formations pour un début se feront entièrement en ligne, et suivront deux cursus sous différents profils. Un parcours dit de formation initiale où le niveau Licence en sciences informatiques ou équivalent est exigé. Cette formation se déroulera en deux ans. Un deuxième niveau dit expert sera adressé pour sa part, aux professionnels de domaines connexes, désireux

de diversifier leur expertise quant aux stratégies applicables au cyberspace en général et celui africain en particulier.

Projet en cours de maturation, mais très prisé. Rapprochez-vous dès maintenant de notre équipe si vous vous sentez stimulé par les offres de formation afin de réserver votre place. Ne manquez pas de suivre notre actualité récente sur nos sites agréés afin d'être les premiers informés dès le lancement.

La rédaction

Point II : À venir...

Sous le haut patronage de la Présidence de la République et du ministère des transports du Sénégal, l'African Critical Infrastructure Forum annonce pour très bientôt l'ACIS Forum Dakar 2024 qui se déroulera du 24 au 26 juin prochain. Le thème retenu pour cette année est « La cybersécurité et la sûreté des infrastructures portuaires, aéroportuaires, plateformes Offshore. »

Pourquoi participer à l'ACIS Forum Dakar 2024 ? En plus d'être reconnu comme le seul forum spécialisé dans ce domaine, les organisateurs (Kubuk Conseil principalement) offrent aux participants des opportunités d'échanges et de réseautage exceptionnelles, un accès privilégié

à des solutions avant-gardistes, sans oublier un impact positif sur leur image et leurs affaires.

Au programme ? Échanges, Formations, Exercices de gestion, Démonstrations d'attaques en live, conférences avec des

intervenants extrêmement qualifiés... etc.

Pour vous inscrire ou recueillir d'amples informations, rendez-vous sur le site officiel : <https://www.acisforumdakar.com/fr/>



Le Question-mag

Dans l'optique d'agrémenter la lecture stratégique du cyberspace africain, la rédaction du MAC a adressé son questionnaire à deux chercheurs _que vous aurez l'occasion d'apprécier en biographies succinctes_, qui, ont tenté chacun de contribuer au débat en cours sur le difficile accès au réseau Internet en Afrique subsaharienne. Avant de donner la parole à nos avis, déroulons ensemble la problématique mise en question.

1. Comment comprendre et expliquer les lenteurs permanentes et l'instabilité de l'accès à Internet dans la plupart des pays d'Afrique subsaharienne ?
2. Quelles sont les causes techniques profondes de cette accessibilité instable et limitée ? Quels impacts et leçons stratégiques peut-on en tirer ?
3. Quelles actions techniques, stratégiques ou politiques urgentes peuvent améliorer cet état de fait ?

M. BAMAHOSSOVI JUSTIN OUMAR, JURISTE CHARGÉ DE LA COOPÉRATION, COMMISSION DE PROTECTION DES DONNÉES PERSONNELLES DU SENEGAL (CDP)

Je m'intéresse à la protection des données personnelles en m'assurant que leur traitement ne porte pas atteinte aux droits et libertés fondamentaux. À travers la coopération, un des leviers du multilatéralisme, les enjeux portant sur l'accès à internet sont des questions préjudicielles à résoudre avant toute avancée majeure relative à la régulation des ressources immatérielles et leur exploitation grâce aux NTIC. C'est la raison pour laquelle, avant tout accord de partenariat ou de convention internationale, un accent particulier sur la sécurité et le respect des droits des données via des dispositifs technologiques fonctionnant grâce à Internet sont rigoureusement encadrées.



justin.oumar@cdp.sn
justinoumar@gmail.com

1. Ces lenteurs et instabilité sont parfois dues à la timidité des politiques publiques dans le secteur technologique. Les investissements du secteur numérique voués à l'amélioration des infrastructures d'internet ne sont pas toujours prioritaires. L'inadaptabilité des infrastructures existantes qui supportent l'internet facilitent leur instrumentalisation sans précédent de la part des autorités publiques. La recherche d'un équilibre entre la nécessité de maintenir l'ordre public en ligne et la sécurité de l'État dans sa globalité d'une part, et d'autre part l'obligation de respecter les droits et libertés fondamentaux soulèvent beaucoup de complexi-

tés. Or, dans plusieurs États, Internet est perçu comme un outil de développement pour opérer des changements structurels profonds. C'est un baromètre du respect des droits fondamentaux, du niveau de l'État de droit et de la démocratie sur tous ses angles. Conscients de ces atouts remarquables qui pourraient être profitables, certaines autorités publiques font d'internet un moyen de censure médiatique et de répression numérique via des coupures...

2. En premier lieu, l'insuffisance d'infrastructure technologique dédiées aux TIC, plus particulièrement les dispositifs numériques

pour le déploiement de l'internet (réseaux de câbles et systèmes d'interconnexion entre autres...) ainsi que les services offerts sont d'une carence évidente. Des facteurs connexes comme la faiblesse de la fourniture d'électricité ou la porosité des points de jonction des câbles sous-marins peuvent impacter significativement la capacité de résilience des parcs technologiques parfois peu performants.

En second lieu, les impacts sont nombreux. En plus d'élargir le fossé de la fracture urique entre le Nord et le Sud, ces causes affaiblissent fondamentalement nos tissus éco-

nomiques fortement dépendants aujourd'hui des technologies et d'internet. Sans parler du recul démocratique qui entraîne souvent une série de violations des droits fondamentaux notamment la liberté d'expression. L'accès à l'information et la liberté de réunion surtout en ligne, devenus quasi systématiques en période électorale ou lors des mouvements de contestation citoyenne.

3. Malgré les nombreux efforts consentis par certains gouvernements conscients des avantages liés aux investissements colossaux sur les NTIC, notamment sur l'accessibilité à l'internet, nos dépendances technologiques exogènes restent un facteur fragilisant. De notre point de vue, les États devraient mettre l'accent sur la formation et le transfert de technologies susceptibles de favoriser l'autonomisation de nos ressources humaines, industrielles et plus tard notre pensée stratégique. Tout en gardant à l'esprit que les

principales ressources naturelles qui gravitent autour des technologies proviennent d'Afrique.

Aussi, il urge une coopération technologique harmonisée autour de nos différentes organisations continentales et/ou régionales. La plupart des États ayant en commun les mêmes défis et enjeux politiques en matière de technologie, ils devraient formuler le plaidoyer d'une seule voie, définir les partenariats bilatéraux/multilatéraux avec les acteurs majeurs (surtout du secteur privé), tout en favorisant la promotion locale. Par ailleurs, l'évolution du taux de connectivité, les performances sur la couverture d'internet, les efforts sur l'inclusion numérique et le dynamique mobile Banking de la zone saharienne, s'apprécient comme des agrégats selon les Objectifs de développement initiés par les Nations Unies en Afrique. Toutefois, ces résultats doivent légitimer une meilleure présence de la région Afrique dans la gouvernance mondiale d'In-

ternet, car la polarisation des initiatives innovantes portées par la prolifération des Start up dynamiques ont montré que la jeunesse africaine entretient une relation fusionnelle avec les outils technologiques.

Retenons en perspective, que les technologies d'avenir seront africaines dans la mesure où elles continueront d'inspirer la richesse créatrice de homos africanis. Encore est-il plus utile de valoriser une identité technologique africaine au détriment d'une souveraineté technologique utopique. Tous les acteurs de la pensée constructrice africaine ont pour responsabilité la promotion d'une « Afrique » innovante et numérisée, bâtie sur des valeurs propres. Sa concrétisation serait aisée si les chercheurs ne se recroquevillent plus dans leurs labos souterrains mais s'affranchissent de la pesanteur des dogmes académiques/universitaires. Leur contribution ne peut être que bénéfique pour le progrès de la société.

**Dr. ZEKENG NDADJI MILLIAM MAXIME,
ENSEIGNANT-CHERCHEUR, UNIVERSITÉ DE DSCHANG /
INFORMATIQUE – GÉNIE LOGICIEL**

Actuellement, je mène des travaux de recherche dans un domaine à l'intersection entre le Génie Logiciel et l'Intelligence Artificielle. L'idée étant de proposer des modèles et outils facilitant la création d'intelligences artificielles et de logiciels dont le but est souvent de résoudre des problèmes de divers domaines d'applications tels que : la e-gouvernance, le e-learning, l'agroécologie, etc.

ndadjimaxime@yahoo.fr 674 96 53 70



1. Les lenteurs permanentes et l'instabilité de l'accès à Internet dans la plupart des pays d'Afrique subsaharienne peuvent être attribuées à divers facteurs complexes et interconnectés. Voici quelques explications possibles. Tout d'abord,

bon nombre de ces pays abritent des infrastructures sous-développées vieillissantes voire obsolètes. Très souvent, l'infrastructure de télécommunication, y compris les câbles sous-marins, les réseaux de fibres optiques (lorsqu'ils

existent), et les infrastructures locales, sont souvent dépassés ou abimés. Cela peut entraîner des pertes de signal, des retards de transmission et une capacité limitée, contribuant aux lenteurs. Les coûts élevés associés à la mise en

place d'infrastructures de télécommunication modernes rendent difficile l'investissement massif dans ces domaines. Les opérateurs de télécommunication semblent être réticents à investir dans des infrastructures onéreuses, ce qui limite la qualité et la couverture des services Internet. De plus, le marché des télécommunications est dominé par un petit nombre d'opérateurs. Le manque de concurrence peut être une explication à la tarification élevée pour des services de moindre qualité, les opérateurs n'ayant pas assez de pression concurrentielle pour améliorer leurs services. Sans oublier que l'instabilité politique et économique de certains pays décourage les investissements étrangers et nationaux. Comme pour d'autres secteurs d'activités, les conflits, la corruption et l'insécurité perturbent la croissance et le développement des réseaux de communication.

2. Soulevons à présent quelques causes techniques profondes. La première raison est le faible taux d'alphabétisation numérique. Dans certaines régions, le manque de connaissances digitales affecte la demande de services Internet. La demande est réduite car les utilisateurs n'ont pas conscience de l'utilité d'Internet ; ce qui contribue à réduire la pression sur les fournisseurs dans l'amélioration de leurs services. Il ne faut pas oublier que ces derniers sont souvent limités par leur insuffisance de capacités. Deuxièmement, la géographie de certaines régions peut rendre difficile l'extension des réseaux de communication. Les zones rurales, généralement moins peuplées, sont moins bien

desservies sûrement en raison des coûts élevés liés à l'extension du réseau sur de longues distances. Surtout le petit nombre de liaisons Internet dont disposent les États les laisse dévastés en cas de catastrophe naturelle ou d'accident. La troisième raison est le faible niveau de veille informatique. Les attaques cybernétiques sont légion et sont aussi à l'origine des perturbations du service Internet. Il existe un manque criard de mesures de sécurité adéquates. Stratégiquement parlant, ces défaillances techniques sont à l'origine de bon nombre de conséquences accablantes pour les pays africains. Nous soulignerons surtout la fragilisation de la sécurité informatique, le lourd retard technologique pour ce qui est des avancées et le problème d'interopérabilité qui affecte la qualité des services Internet.

3. Pour améliorer l'accessibilité à Internet en Afrique subsaharienne, plusieurs actions techniques, stratégiques et politiques peuvent être considérées comme urgentes. Voici quelques recommandations.

- Investir dans l'infrastructure : en allouant des ressources financières significatives pour moderniser et étendre les infrastructures de télécommunication (câbles sous-marins, réseaux de fibres optiques, infrastructures locales) et en encourageant les partenaires à mobiliser des fonds et compétences dans le développement des infrastructures.
- Favoriser la concurrence et encourager la diversité des fournisseurs : Les États doivent promouvoir un environnement concurrentiel et mettre en œuvre des politiques

visant à empêcher la monopolisation du marché des télécommunications. Soutenir la diversification des fournisseurs de services Internet pour stimuler la concurrence et offrir des options aux consommateurs. Favoriser la coopération régionale pour partager les infrastructures et faciliter l'accès à Internet à travers les frontières.

- Renforcer la sécurité informatique et investir dans l'éducation numérique : Ceci passe par la mise en place des politiques et des réglementations qui obligent les fournisseurs de services à renforcer la sécurité de leurs réseaux. La formation en cybersécurité pour sensibiliser les acteurs à la protection contre les menaces en ligne et susciter l'intérêt pour la discipline auprès de la population.
- Faciliter l'accès à Internet dans les zones rurales et développer des politiques gouvernementales favorables : Pour ce faire, les pouvoirs publics doivent encourager les investissements dans les infrastructures de télécommunication et attirer des investisseurs. Il faut engager des procédures pour connecter les zones rurales (surtout les écoles, centres de santé entre autres) avec des technologies saines pour leur environnement
- Enfin, il faut impliquer les acteurs internationaux et faire un suivi-évaluation constant. Des ateliers régionaux doivent impérativement être au programme pour un meilleur partage des pratiques. Il faudrait régulièrement mesurer les progrès et ajuster les stratégies en fonction des besoins changeants.

L'Actualité

Cette rubrique reprend quelques actualités récentes et marquantes du point de vue du LARC, avec un court commentaire basé sur notre grille d'analyse (logique des enjeux)

Fin octobre 2023 : les Forces Armées Ghanéennes (GAF) ont annoncé la création d'une Direction des Opérations de Cybersécurité et de Guerre Électronique.

À travers cette annonce, le Ghana entre dans le cercle très restreint des États africains qui ont pleinement pris conscience du phénomène de conflictualité et de rapports de forces dans le cyberspace, et qui tirent les conséquences qui en découlent en traitant ce phénomène à un niveau stratégique pertinent. Comme l'affirme le Vice-Amiral Seth Amoama, Chef d'État-major de la défense des Forces Armées du Ghana : « La sécurité dans le cyberspace est aussi cruciale que sur terre, en mer, dans les airs et dans l'espace (...) la protection des données et des infrastructures de communication est essentielle pour garantir la sécurité nationale. »

Les devanciers du pays de Nkrumah dans cette démarche sont l'Égypte, le Nigeria, le Rwanda, l'Afrique du Sud, l'Algérie et dans une certaine mesure l'Éthiopie, pour ne citer que ceux-là. Cette initiative ghanéenne confirme la pertinence de nos travaux qui attirent l'attention des États sur la nécessité de considé-



rer le cyberspace comme milieu stratégique et espace d'affrontements (militaire, économique, politique, culturel, etc.) dans lequel s'opposent différents acteurs à objectifs et intentions parfois antagonistes. Vivement que les États encore dans l'insouciance s'inspirent de cette démarche, préalable pour la souveraineté numérique de l'Afrique.

Dans un élan panafricaniste, nous

suggererions une réforme profonde de la PACSD (Politique Africaine Commune de Sécurité et de Défense) portée par l'Union Africaine, en consacrant le cyberspace à l'échelle continentale comme milieu stratégique. Ce n'est qu'ainsi que nous serons capables de tirer toutes les implications tactiques et opérationnelles pour les forces africaines de sécurité et de défense concernées par cette politique.

L'Actualité

Le 10 Janvier 2024, le groupe Anonymous Sudan dans son canal Telegram annonce avoir mené une cyberattaque massive contre l'infrastructure de SUDACHAD le plus grand fournisseur de télécommunications au TCHAD.

Anonymous Sudan est un groupe d'hacktivistes (pirates informatiques motivés par des convictions religieuses et/ou politiques) issu du Soudan. En 2023 il initie maintes attaques par déni de service en représailles des actes posés par leur cible (souvent occidentale) qui irait à l'encontre de leurs convictions. On se souvient qu'en Août 2023, ce même groupe menaçait la France en cas d'intervention militaire au Niger. Cette attaque contre SUDACHAD provoquait une interruption d'Internet sur la quasi-totalité du territoire, avec des conséquences socio-économiques qui restent encore à évaluer. L'opérateur télécom serait la

victime de prétendus liens entre l'État du Tchad et le groupe paramilitaire RSF au Soudan.

Au regard de la cible (infrastructure critique), du type d'attaque (sabotage), de la motivation (conviction politique revendiquée), et de l'impact (perturbation de la vie sociale et économique du pays), cette cyberattaque prouve à suffisance qu'un groupe d'hacktivistes peut dans le cyberspace tenter de contraindre un État. Vu ainsi, la cyber opération d'Anonymous Sudan peut être considérée comme une action stratégique (forcer l'État tchadien à remettre en question un éventuel partenariat de défense). Cette

action bien que malveillante, fait de ce groupe un acteur stratégique du cyberspace africain.

À la lumière de cette actualité, soulignons l'urgence pour les forces de défense, centres de recherche et décideurs africains de s'intéresser de prêt à cette nouvelle branche de la stratégie qu'est la Cyberstratégie. On découvre une nouvelle définition des notions de facteurs, principes et acteurs stratégiques propres au cyberspace en tant que milieu spécifique. L'ouvrage Cyberstratégie Africaine, Tome I à paraître très bientôt aux éditions Ifrikiya & LARC abordera largement ces néologismes.



L'Actualité

2023 : Le Cameroun réaffirme son intérêt pour la Cybersécurité

Le gouvernement camerounais œuvre de plus en plus pour que la cybersécurité soit un domaine de portée majeure. Il n'est plus question de partir de paradigmes étrangers, les étudiants chercheurs ont de nouvelles voies à suivre dans leur choix de carrière. L'implémentation du Master en Cybersécurité et cybergouvernance de l'Université de Bamenda emboîte le pas aux deux annexes (Bandjoun et Nkolbisson) de l'Université de Dschang qui offrent cette option depuis quelques années déjà. À côté du secteur public, de nombreuses offres de formation sont proposées par des entités d'enseignement supérieur privé à titre professionnel. Soulignons ici le cas de RHOpenLabs Acad qui se distingue par ses de formations certifiantes (lesdites certifications sont internationalement reconnues) aux métiers notamment d'Analyste SOC entre autres. Ils plongent les apprenants dans un environnement de travail purement pratique avec simulations d'attaques. En bonus, le « Projet Fil rouge », l'une des surprises de la formation, consiste à accompagner les apprenants dans un projet personnel innovant inhérent à son domaine ; l'objectif étant de se démarquer de ses camarades car les meilleurs académiciens sont aussitôt retenus par la filiale du groupe RHOpenLabs.

Dans le même sillage, l'Agence Nationale des Technologies de



l'Information et de la Communication (ANTIC) n'a de cesse de multiplier les séminaires et sensibilisations sur la cyber-résilience et la protection des données sensibles des citoyens. Au-delà de ses certifications et actions engagées avec divers partenaires internationaux, l'association publique a établi la Journée Nationale de la Cybersécurité au Cameroun. Pour le compte de l'année 2023, elle s'est tenue au mois d'octobre. Il a été question pendant environ une semaine riche en activité, de descentes dans plusieurs établissements primaires et

secondaires du pays pour initier les plus jeunes à l'utilisation responsable d'Internet.

Ces différentes actions déplorables tardives, engagées par l'État du Cameroun font montre d'une prise de conscience sur les dangers liés à l'utilisation naïve d'Internet quand on sait bien que le cyberspace est en proie aux vices de cyber-malfaiteurs multiples. Nous sommes encore loin d'une stratégie propre, bien que ces actions constituent un pas dans la démarche.

La rédaction



Le choix de la rédaction

La rédaction du MAC consulte pour vous les nouvelles parutions intimement liées aux problématiques du cyberspace africain, notamment de cyberstratégie africaine.

Procurez-vous dès maintenant ces ouvrages disponibles aux sites mentionnés.

Souveraineté numérique et cyberdéfense : Un enjeu de taille pour l'Afrique

Auteur : Djimgou Ngameni

Editeur : LARC

Date de parution : Janvier 2021

Format : Papier

Nombre de pages : 204 pages

Prix : 17€ soit 11.000Frs CFA

Pour commander : info@larc.africa



L'Afrique au risque d'une cybercolonisation

Auteurs : José Do Nascimento & Djimgou Ngameni

Editeur : L'Harmattan

Date de parution : Avril 2023

Format : Papier, PDF et Epub

Nombre de pages : 238 pages

Prix : 25€ (16.500Frs CFA) papier ; 18.99£ (12.500) Epub & PDF

Pour commander : https://editions-harmattan.fr/catalogue/commande/commande_add.asp?no=76859&cdo=0&cdf=0&cds=0



Cyberstratégie Africaine-Tome I

Auteur : Djimgou Ngameni

Editeurs : Ifrikiya & LARC

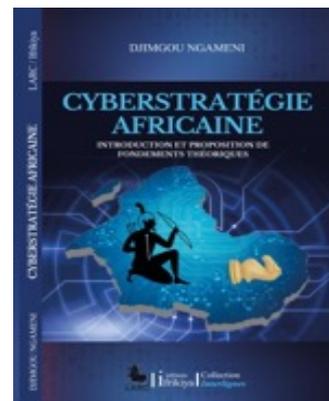
Date de parution : Février 2024

Format : Papier

Nombre de pages : 290 pages

Prix : 23€ soit 15.000Frs CFA

Pour commander : info@larc.africa



Africa
Cybersecurity
Magazine

Les partenaires

Ecole Politique Africaine (EPA)



Site officiel : <https://ecole-politique-africaine.fr/>

Fonction : Académie

Contact : +33 745 325 987 contact@ecole-politique-africaine.fr

Pages : Facebook, Instagram, LinkedIn

Académie Camerounaise de Lutte contre la Cybercriminalité / Cameroon Academy for Cybercrime Control (ACLC-CACC)



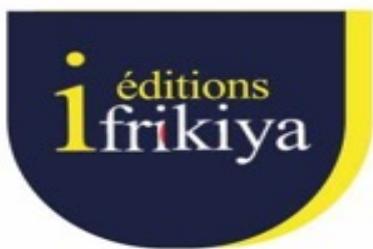
Site officiel : <https://aclc-cacc.org/fr/>

Fonctions : Formation, Recherche

Contact : +237 691-710-690 [info\[at\]aclc-cacc.org](mailto:info[at]aclc-cacc.org)

Pages : Facebook, Twitter, LinkedIn, YouTube

Ifrikiya, une maison d'édition ouverte sur le Continent



Site officiel : <https://www.facebook.com/ifrikiya.editions/>

Fonction : Édition

Contact : 6 99 77 10 99 editionsifrikiya@yahoo.fr

Pages : Facebook, <http://plumencre.e-monsite.com/news/annuaire-editeurs/editeurs-cameroun/editions-ifrikiya.html>

Africa Cybersecurity mag, magazine spécialisé sur la Cybersécurité, la CyberDéfense, la CyberJuridiction et la Protection Numérique en Afrique ; édité par la société CyberSpector.

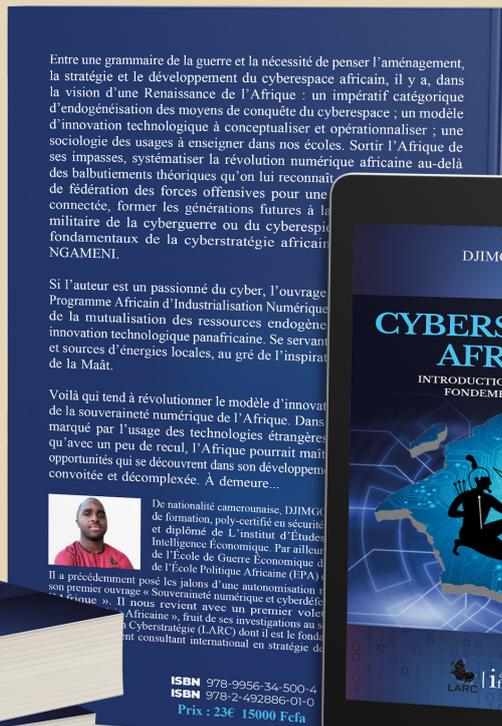
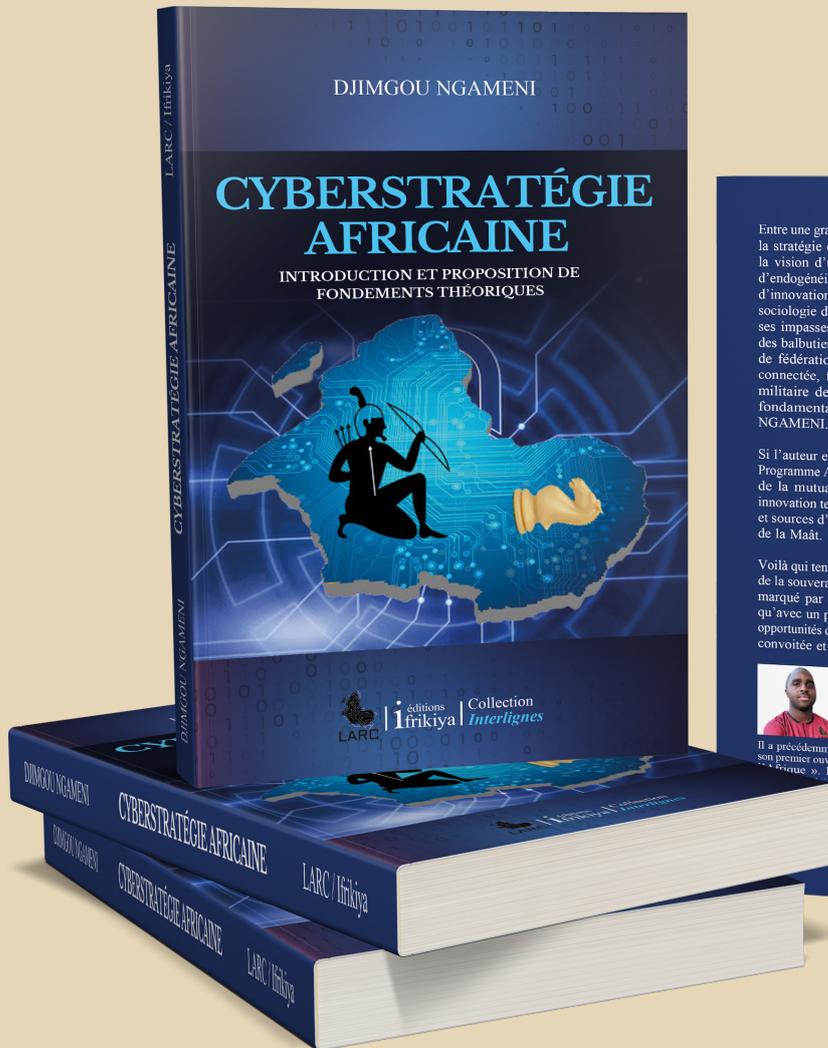


Site officiel : <https://cybersecuritymag.africa/index.php/>

Fonction : Magazine d'actualité cybernétique

Contact : contact@cybersecuritymag.africa

Pages : Facebook, Twitter, YouTube, LinkedIn



Décrypter les enjeux de demain dans le cyberspace africain

Nous contacter

 info@larc.africa

 696 683 515

 www.larc.africa

LARC



<https://larc.africa/>

