Magazine Africain de Cyberstratégie

Décrypter les enjeux de demain dans le cyberespace africain

MAC / n° 002 / Novembre 2024

LARC

« Au-delà de la mise en place de réglementations claires et adaptées aux réalités, les décideurs africains devraient adopter une approche encore plus stratégique et intégrée.»

Nathalie KIENGA P.10

Souveraineté numérique Vs autonomie stratégique de l'Afrique dans le cyberespace :

QUEL CHOIX POUR LES ETATS AFRICAINS ?

SOMMAIRE

Dans un monde où le cyberespace redéfinit les rapports de force, l'Afrique se retrouve à un carrefour crucial. Rendus à l'évidence de ce que le cyberespace continue de faire couler l'encre sur ses usages et risques au détriment de ses potentialités pour l'Afrique, le MAC a été pensé. Le semestriel s'intéresse à toute forme d'actualité relative à la cyberstratégie africaine ainsi qu'aux activités et projets de la structure qui l'héberge, notamment le LARC. Le MAC se veut compétitif dans le sens où son approche est prolifique pour le numérique africain. La thématique de ce numéro « Souveraineté numérique Vs Autonomie stratégique dans le cyberespace : Quel choix pour les Etats africains » pose une problématique complexe : Comment les Etats africains devraient-ils se comporter face à cette double finalité ? La souveraineté numérique en tant qu'idéal, ne pourrait-elle pas se faire précéder d'une volonté d'autonomie stratégique dans le cyberespace ? Ne serait-ce pas une alternative intéressante ?

La notion de souveraineté numérique que nous évoquons implique un contrôle accru sur les infrastructures et données, tout en soulevant des interrogations sur les enjeux géopolitiques de cette dépendance technologique. Cette notion est-elle encore pertinente? Face à l'émergence de puissances technologiques et à la domination des géants du numérique, il est impératif pour l'Afrique de réexaminer son approche stratégique. Au-delà de la simple protection de données, la souveraineté numérique implique la capacité à définir nos propres normes, à mieux maîtriser nos infrastructures d'hébergement et de communication, ainsi qu'à encourager l'innovation locale. A ce propos, des experts en cybersécurité et en stratégie appliquée au cyberespace vous guident à travers les défis actuels, des cyberattaques aux menaces géopolitiques, tout en proposant des solutions concrètes et adaptées. Nos chercheurs apportent également des perspectives critiques sur la manière dont les Etats africains peuvent non seulement se défendre, mais aussi s'imposer sur la scène mondiale. Ils examinent les enjeux liés à la coopération régionale, à la gouvernance numérique, éléments clés pour bâtir un avenir numérique résilient. Grâce à notre clin d'œil de lecture, nous vous suggérons les fondamentaux tandis que la rubrique Tendances, identifie des pistes de sortie. Retrouvez aussi en exclusivité, les dernières actualités relatives au LARC. L'enjeu est de taille et mérite une réflexion collective, raison pour laquelle ce numéro se veut un appel à l'action. Par la mise en lumière de ces problématiques, nous souhaitons engager les ressources africaines pour la construction d'un futur dans lequel l'Afrique passe de spectateur à ACTEUR.

[Avis aux auteurs et lecteurs]

En intervenant dans le MAC, les rédacteurs ont une vitrine de vulgarisation de leur avis quant au débat stratégique en cours sur le cyberespace 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.

Humblement, **la rédaction du MAC**

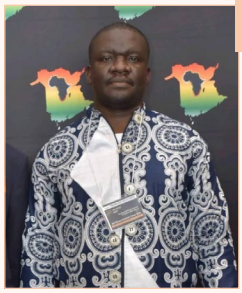
PROFIL DES INTERVENANTS

DJIMGOU NGAMENI

François-Xavier DJIMGOU NGAMENI et le promoteur de RHOPEN LABS et fondateur du LARC (Laboratoire Africain de Recherches en Cyberstratégie) Auteur de plusieurs ouvrages, il est passionné par la problématique de souveraineté numérique de l'Afrique. Conférencier et consultant en cybersécurité/cyberdéfense, il conduit des travaux sur la cyberstratégie en Afrique.

Nathalie KIENGA

Formée à l'Ecole de Guerre Economique de Paris où elle obtient un MBA en Cybersécurité, Sécurité Internationale et Risque, Nathalie KIENGA, Ambassadrice ID4AFRICA, est une influence notoire du cyberespace africain depuis plus de dix ans. Fondatrice de l'Institut Africain de la Cybersécurité et de la sécurité des infrastructures (I-CSSI), elle occupe actuellement le poste Chef adjoint du Conseil National de Cyberdéfense de la République Démocratique du Congo.



François HEUTHOU

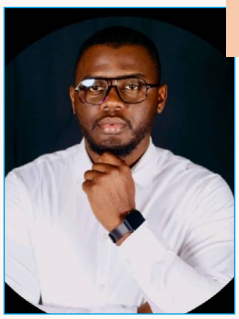
Expert cybersécurité certifie CAPTE et CISEH, François HEUTCHOU est un chercheur dévoué a la formation et a la sensibilisation aux pratiques de sécurité cyber. Analyste cyber fort de plusieurs années d'expériences, il fonde l'ACLCCACC (Association Camerounaise de Lutte contre la Cybercriminalité - Cameroon Association for Cybercrime Control) en 2018 avec pour but de répondre efficacement aux besoins en formation de son pays. Il est actuellement chercheur au Centre de Recherche et de Développement en Education (CDRE) de l'Université de Moncton au Canada, il continue d'œuvrer activement .

Haris FOTSO

Haris FOTSO est titulaire d'un doctorat, développeur Full stack et ingénieur en intelligence artificielle et logiciel. Directeur général de Victoire informatiques basé en Ontario, il est également le webmestre informatique de la Fondation Muna Kalati et du Groupe Kabod. Webmestre et développeur complet, il a développé un système de gestion de l'apprentissage (LMS), un système de gestion de bibliothèque et un système de gestion scolaire

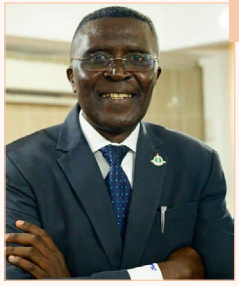
Bara FALL

Consultant et Architecte Sécurité, Bara FALL, le promoteur de la culture #cyberpour tous est doté d'une dizaine d'années d'expériences. Parti d'ingénieur informatique, il s'est spécialisé en cybersécurité et occupe depuis plus de dix ans le poste de Référent sécurité informationnelle chez Bank Of Africa. Il fonde ABC Cyber Community, afin de sensibiliser le public aux enjeux de la cybersécurité.



Kévin W.

Kevin est un spécialiste de l'assistance informatique. Directeur technique et cofondateur de SUNITER, il travaille actuellement comme responsable de la sécurité de l'information pour EUROCLEAR. Consultant en cybersécurité, il possède une expérience notoire.



Rtd Roger KUITCHE

Le retraité Colonel Roger KUITCHE, fort de ses 36ans d'expérience professionnelle, détient une exposition nationale et internationale significative, notamment en mati7re de stratégie militaire auprès des Nations Unies et d'autres organisations internationales. Désormais CEO de Best Practice Sarl, il s'active dans le conseil stratégique et le coaching des entreprises et organismes sur la sécurité et la paix. Son objectif, démystifier la stratégie militaire pour l'appliquer dans les organisations.

Oumar DIALLO

Expert en renseignement cyber et consultant Cybersécurité, Oumar Diallo est le promoteur de la DIALLO Team Intelligence.

Penser le cyberespace africain au-delà de ses usages : Cas de l'IA

La révolution numérique en cours dans le monde est rythmée par une succession d'innovations technologiques [telles que l'IA, la Blockchain, les NBIC, l'impression 3D, etc.] qui de plus en plus transforment en profondeur nos modes de vie, de pensée, de travail, d'action, etc. Ces technologies, qui véhiculent des visions du monde et des enjeux significatifs, sont la plupart du temps adoptées dans les pays africains sans questionnement préalable. Bien souvent, on considère uniquement leur capacité à favoriser ou à soutenir l'idéal de développement que nous recherchons. C'est ce conditionnement de la perception africaine des technologies numériques que l'on désigne par la logique des usages.

Le présent article se propose d'explorer le cas de l'intelligence artificielle en examinant la manière dont son arrivée récente en Afrique est traitée. L'objectif est de présenter une grille de lecture alternative sur la perception des technologies, celle qui sous-tend les travaux menés par le LARC Cette autre perspective vise à dépasser les simples usages pour recentrer la réflexion de façon constante sur les véritables enjeux du cyberespace africain. C'est ce que l'on désigne par la logique des enjeux.

Du contexte et enjeux actuels du cyberespace

L'essor des technologies numériques, en particulier de l'intelligence artificielle, transforme les industries et les sociétés à une vitesse fulgurante, posant ainsi des défis en matière de gouvernance et de sécurité. Alors que de nombreuses voix se concentrent sur l'intégration de l'IA dans divers domaines, peu d'analyses sur le continent se penchent sur les mécanismes qui la régissent. Ce manque de réflexion sur la finalité et les implications des technologies numériques crée un vide que nous devons combler.

Comme le montre l'actualité récente, nous assistons aujourd'hui encore à une narration dominée par l'usage (apport de l'IA dans la cybersécurité en Afrique, pour améliorer les performances des armées ou encore le rendement des agriculteurs africains, etc). La plupart des acteurs se concentrent sur les techniques d'intégration de ces technologies dans divers secteurs, négligeant les enjeux stratégiques qui en découlent, créant ainsi un retard analytique que le LARC se propose de combler.

La logique du LARC : enjeux et risques au cœur de nos préoccupations

Le Laboratoire Africain de Recherches en Cyberstratégie se positionne en pionnier en ce sens où nous mettons en lumière les défis que pose le cyberespace pour notre continent. Plutôt que de se limiter à une approche utilitaire, nous explorons les dimensions juridiques, géopolitiques et stratégiques de la transformation numérique. L'identification des menaces potentielles sur le cyberespace africain constitue notre mot d'ordre. Nous allons au-delà de ces technologies afin de voir comment celles-ci peuvent être utilisées de façon autonome et maîtrisée.

Revenons au cas de l'intelligence artificielle. Notre approche consiste particulièrement pour ce cas de figure à questionner les impli-

cations de son intégration. Rassurez-vous, l'IA n'est pas qu'un outil : elle cristallise une vision du monde, redéfinit les rapports de forces et soulève l'épineuse question de la souveraineté. C'est un nouveau vecteur de puissance. Lors d'une rencontre avec des étudiants en Septembre 2017, le président russe s'est exprimé au sujet de l'intelligence artificielle. Selon lui, « Celui qui dominera l'intelligence artificielle dominera le monde car l'IA sera l'un des grands enjeux du 21ème siècle. » « La lutte entre nations pour la supériorité en matière d'IA causera probablement la troisième guerre mondiale. », renchérit Elon MUSK trois ans plus tard. Comment les pays africains peuvent-ils s'assurer que ces technologies servent leurs intérêts au lieu de renforcer des dynamiques de dépendance ? Comment dominer l'IA ? Quels sont les leviers pour y parvenir ?

Des points imminents pour analyse profonde

La stratégie cyber, en tant que dynamique des intentions dans le cyberespace, doit être établie avant toute action opérationnelle. Plutôt que d'adopter ces technologies sans réserve, nous suggérons de les passer au crible d'une grille de lecture centrée sur les enjeux, afin d'en dégager des usages plus conformes à notre vision du monde. Dans cette perspective, il devient évident que des leviers de dépendance émergent, qu'il est essentiel de considérer pour envisager une utilisation plus contrôlée de l'IA. Par exemple :

- La guerre des semi-conducteurs, processeurs et puces, qui bat son plein entre les grandes puissances, avec un avantage américain à travers Taiwan, talonné par la Chine qui vise sa souveraineté effective en la matière ;
- La question de supercalculateur (HCP), qui fournit la puissance de calcul nécessaire pour faire tourner les algorithmes d'IA très gourmand en ressources ;
- La question de l'accès à l'énergie stable et à bas coût, pour faire tourner les data centers qui hébergent ces supercalculateurs ;
- La question de l'accès aux matières premières, nécessaires pour construire toute cette couche de base, et la technologie pour les transformer;
- La question des biais algorithmiques, qui reflète la vision de monde et les perceptions biaisées des concepteurs de modèles et d'algorithmes d'IA que nous adoptons sans questionnement.

Aujourd'hui, au regard de leur large avance sur ces différents leviers, les États-Unis et la Chine forment une sorte de duopole qui domine l'IA et en font un outil d'accroissement de leur puissance. Malgré le centre de recherche pour l'IA lancé à Accra par Google il y a quelques années, le continent africain est pratiquement vierge en termes d'infrastructures numériques de base pour soutenir durablement et de façon indépendante ses usages de l'IA.

Pour une réinvention de la narration du cyberespace en Afrique

Il devient urgent de passer d'une logique d'intégration à une réflexion profonde sur les implications stratégiques. Le LARC se veut initiateur d'un dialogue autour de la gouvernance numérique, prenant en compte les réalités africaines. Il est essentiel pour les chercheurs de s'impliquer pour la construction d'une vision épurée du cyberespace africain. En redéfinissant notre rapport au cyberespace, nous avons l'opportunité de façonner un avenir numérique qui soit à la fois sécurisé et conforme à nos aspirations. Il est temps de prendre un engagement stratégique envers un avenir plus proche de la souveraineté.

Léa Arselle TSAFACK *et DJIMGOU NGAMENI*

La stratégie militaire appliquée au cyberespace africain : NOTES SUR BEST PRACTICE

Le ®Colonel Roger KUITCHE retraité des Forces Armées est reconnu pour son expertise en stratégie militaire, mais aussi pour son exposition internationale significative, notamment en lien avec les mécanismes des Nations Unies et d'autres organisations internationales. Il est également le CEO de la société Best Practice, où il se concentre sur le coaching et le conseil stratégique aux décideurs, notamment dans le domaine de la sécurité et de la paix. En plus de son rôle dans le secteur privé, il est impliqué dans des initiatives visant à démystifier la stratégie militaire appliquée aux entreprises et aux administrations, ce qui montre son engagement à partager ses connaissances et son expertise.

Explorons ensemble ce projet bien ficelé de notre expert stratège.

La rédaction :
Comment s'est façonnée votre vision stratégique ?

® Colonel : Plusieurs expériences jumelées ont façonné ma vision stratégique. La première expérience a été la diplomatie militaire. Principalement en tant que membre de l'Union Africaine au Soudan (MUAS) de 2005 à 2007 avec la fonction d'Officier Mouvement au sein du Darfur Integrated Task force, et plus tard commandant du détachement camerounais à la MICOPAX en RCA de 2010 à 2012. De 2016 à 2019 j'étais attaché de défense auprès du Haut-Commissariat du Cameroun au Nigeria et accrédité dans dix pays d'Afrique de l'Ouest. Ces missions m'ont permis d'acquérir une compréhension approfondie de la coopération internationale et de la diplomatie militaire. J'ai ainsi pu développer des compétences en négociation et en gestion des relations complexes.

Aussi, la participation active au conflit de Bakassi a été la pierre angulaire de ma formation stratégique. Plus tard, en tant que commandant de la 41e infanterie motorisée (2014-2016), je crois avoir joué un rôle crucial dans les opérations contre Boko Haram. Cette expérience m'a appris l'importance de la résilience, de la coordination et de la stratégie à long terme.

De plus, pendant la pandémie de Covid 19, j'ai suggéré d'appliquer des principes militaires pour proposer des solutions économico-stratégiques, en comparant la lutte contre le virus a une guerre, nécessitant une stratégie rigoureuse et une adaptation rapide aux nouvelles menaces, permettant de tirer profit de la crise qui est à la fois risque et opportunité de relance de l'économie.

R : Comment envisagez-vous l'évolution de la stratégie militaire face aux nouvelles menaces dans le cyberespace ?

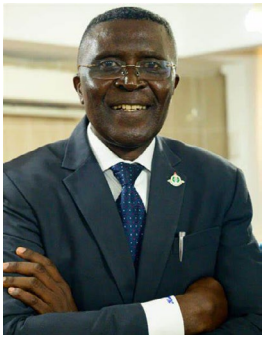
C : La stratégie militaire aujourd'hui ne peut plus être opérationnelle sans l'intégration des défis et risques du cyberespace, lui aussi terrain d'affrontements. A cet effet, plusieurs aspects importants sont à relever notamment l'intégration de ce nouvel espace cyber et de ses innovations et corollaires dans la doctrine militaire ; ainsi que le développement de capacités offensives et défensives.

De plus en plus, les armées intègrent le cyberespace dans leurs doctrines et stratégies globales. C'est pourquoi l'OTAN considère désormais le cyberespace comme le cinquième territoire de guerre. Ceci en raison du constat que la plupart des opérations militaires comportent désormais une dimension cybernétique. Par ailleurs, les nations investissent dans le développement de capacités cybernétiques offensives et défensives. Les capacités offensives incluant les cyberattaques visant à perturber les réseaux ennemis, tandis que les capacités défensives sont axées sur la protection des infrastructures critiques et la résilience face aux attaques. La résilience est devenue un élément central des stratégies de cybersécurité. Les militaires travaillent à renforcer la résilience de leurs réseaux et systèmes pour assurer la continuité des opérations en cas d'offense. Des exercices de simulation d'attaques se font d'ores et déjà réguliers sous d'autres cieux.

Parlez-nous des missions et objectifs de votre structure Best Practice.

Le cabinet Best Practice, que j'ai fondé après ma retraite, a pour mission principale d'appliquer là où c'est possible, les principes et les stratégies militaires au monde des affaires et des organisations. Nos missions peuvent être segmentées en deux groupes. La principale est de fournir des conseils stratégiques efficaces aux entreprises et organisations en vue de les aider à naviguer au mieux dans des environnements complexes et incertains. Nous procédons par l'élaboration de plans stratégiques, la gestion de crises et l'optimisation des opérations.

Nos missions secondaires incluent formation et développement, sécurité et résilience, sans oublier la gestion du changement. Nos programmes adaptés aux besoins spécifiques des clients sont basés sur les principes militaires. Nous aidons par ailleurs les organisations à renforcer leur résilience face aux menaces et aux crises ainsi qu'à mieux gérer les transitions et changements (nouvelles technologies par exemple)



Nos objectifs sont tout autant multiples. Par l'utilisation des techniques éprouvées de gestion militaire, nous visons pour nos clients l'amélioration de l'efficacité opérationnelle ; le renforcement du leadership ; la promotion de l'innovation ainsi que l'assurance d'une stratégie durable.

Best Practice vise à transformer les défis en opportunités en appliquant des stratégies militaires éprouvées au monde des affaires, tout en développant des leaders capables de naviguer dans des environnements complexes et en constante évolution que l'on appelle le monde VUCA.

Quelle est la plus-value de Best practice ?

Notre cabinet apporte modestement une approche intégrée et multidimensionnelle combinant stratégie, innovation, leadership, sécurité et coopération pour aider les organisations et les gouvernements à atteindre leurs objectifs et à surmonter les défis complexes. Nous incluons méthodiquement l'analyse de la situation, la planification stratégique ainsi que la gestion des risques.

En matière de sécurité, Best Practice offre des solutions complètes pour protéger les actifs et informations sensibles. En collaboration avec le Laboratoire Africain de Recherches en Cyberstratégie, nous assurons : la mise en place de mesures de protection contre les cybermenaces, y compris la formation du personnel et l'implémentation de technologies de pointe ; l'évaluation et l'amélioration des mesures de sécurité physique pour protéger les infrastructures critiques ; et enfin la réponse aux incidents.

Best Practice favorise la coopération entre les secteurs public et privé pour renforcer la sécurité et la résilience. Nous estimons que la collaboration entre entités gouvernementales et entreprises favorise le partage de ressources et des informations. Par ailleurs, l'implication des communautés locales dans les initiatives de sécurité renforce la vigilance et la coopération. Je vous invite à suivre nos activités de près via notre site officiel et nos canaux de diffusion.

Lire la communication relative à cet entretien…

Propos recueillis **par la rédaction**

Dossier n° 1 Inscrire la cyberstratégie au cœur des priorités des Etats africains

Le potentiel de l'Afrique est immense, mais il ne se réalisera que si ses dirigeants osent rêver grand et s'engagent activement à transformer ces rêves en réalité. L'engagement et la détermination des dirigeants africains à réussir ce pari ! Sans volonté de leur part, rien de concret n'est possible au-delà des discours.

Mots clés : Souveraineté, cyber, Afrique, gouvernance, puissance, cyberpuissance, évaluation cyber, émergence, hégémonie, démarche africaine.

Résumé

Dans un contexte mondial où la technologie joue un rôle crucial dans la puissance et la compétition, l'Afrique se trouve à un moment charnière dans son développement numérique. Alors que des acteurs majeurs comme les États-Unis, la Chine, la Russie et l'Union européenne dominent les politiques technologiques, le continent doit surmonter des défis spécifiques liés à la cybersécurité et à la souveraineté numérique. Pour cela, une Cyberstratégie complète et cohérente est essentielle pour assurer une transformation numérique efficace. L'engagement des dirigeants africains, l'intégration régionale et la coopération internationale sont cruciaux pour établir une gouvernance solide, dépassant les tensions historiques. Il est également impératif de développer des infrastructures locales et d'adopter des réglementations adaptées, tout en investissant dans l'éducation pour préparer les générations futures aux enjeux numériques. Cette étude vise à mettre en lumière l'importance d'une approche stratégique pour les pays africains, au-delà du cadre de transformation numérique proposé pour 2020-2030. Face à un environnement technologique en rapide évolution, l'Afrique doit s'affirmer comme un acteur compétitif en élaborant des politiques adaptées qui répondent à ses besoins spécifiques et s'assurer que le continent ne soit pas laissé pour compte dans la dynamique technologique mondiale.

Bara FALL

Pour citer cet article : Bara FALL,
Inscrire la Cyberstratégie au cœur des priorités des États africains , Note N° 13 - LARC, Novembre 2024.

Dossier n° 2 L'Afrique est un théâtre techno-géopolitique stratégique. Les dirigeants du continent sauront-ils en tirer parti ?

Les décideurs africains doivent veiller à ce que l'économie numérique de l'Afrique ne soit pas réduite à un pion sur l'échiquier géopolitique et à un simple champ de bataille pour la résurgence de la concurrence des grandes puissances entre les blocs géopolitiques.

Mots clés : géopolitique, transformation numérique, cyberguerre, gouvernance, technologie, réglementation, cyberespace, économie.

Résumé

Bien qu'elle soit la région la moins connectée à l'internet, la transformation numérique de l'Afrique est une frontière pour la géopolitique des technologies numériques. Le potentiel numérique de l'Afrique suscite un vif intérêt au niveau mondial, de même que la possibilité d'en accélérer le rythme et d'exploiter le marché du continent, qui compte plus d'un milliard d'habitants. Une multitude d'initiatives internationales ont été lancées et des investissements ont été réalisés pour connecter les Africains à l'internet. Entretemps, la guerre en Ukraine a montré que les fournisseurs de services « neutres » de technologies numériques peuvent devenir et sont devenus de puissants acteurs de la gouvernance, capables de prendre des décisions unilatérales ayant des répercussions considérables sur les flux d'informations. Bon nombre de ces fournisseurs de services cherchent à répondre aux besoins de l'Afrique en matière d'infrastructures de connectivité, au-delà de l'offre de plates-formes de communication numérique. Les décideurs africains doivent veiller à ce que l'économie numérique de l'Afrique ne soit pas réduite à un pion sur l'échiquier géopolitique et à un simple champ de bataille pour la résurgence de la concurrence des grandes puissances entre les blocs géopolitiques. Les décideurs africains doivent également s'assurer que les lois et réglementations régissant les technologies numériques et le cyberespace sur le continent permettront de faire progresser les objectifs de développement politique et socio-économique de l'Afrique à l'ère du numérique, et doivent éviter d'utiliser ces réglementations pour exercer un « contrôle » sur l'activité en ligne des citoyens.

Nanjira SAMBULI

Pour citer cet article : Nanjira SAMBULI, «L'Afrique est un théâtre techno-géopolitique stratégique. Les dirigeants du continent sauront-ils en tirer parti ? », Note N° 14 - LARC, Novembre 2024.

PAROLE À NATHALIE KIENGA

NAVIGUER ENTRE SOUVERAINETE NUMERIQUE ETAUTONOMIE STRATEGIQUE : LES DEFIS DANS LE CYBERESPACE AFRICAIN. PAROLE A NATHALIE KIENGA

Nathalie KIENGA, experte en cybersécurité se positionne en première ligne des enjeux numériques en Afrique. Dans cette interview accordée au MAC, elle abordera les défis liés à la souveraineté numérique et à l'autonomie stratégique du continent dans le cyberespace. Elle partagera son expérience et sa vision pour renforcer la résilience numérique des nations africaines face aux cybermenaces croissantes. Nous aborderons les choix cruciaux auxquels font face les États africains dans la quête d'une souveraineté numérique tout en préservant leur autonomie stratégique. Quels sont les enjeux actuels et comment les acteurs du continent peuvent-ils se positionner pour un avenir numérique résilient et indépendant ? Explorons ensemble ces questions cruciales qui façonnent l'avenir du numérique en Afrique.

I-CSSI
Institut de Cybersecurité et Sécurité des Infrastructures

La rédaction : Quels ont été les moments clés de votre parcours qui vous ont conduit à votre expertise actuelle ?

Nathalie KIENGA : Bonjour et merci pour votre considération. Je dirais que les moments clés de mon parcours sont mes moments de mentorat.

En effet, avoir eu la chance de travailler avec des mentors experts du secteur a été déterminant pour mon développement professionnel. Ces mentors m'ont non seulement offert des conseils stratégiques, mais ils ont également partagé leurs expériences et leurs défis, ce qui m'a permis d'apprendre de manière concrète et surtout d'éviter quelques erreurs.

R : Comment évaluez-vous l'évolution des menaces dans le cyberespace africain ?

N.K. : L'évolution des menaces dans le cyberespace africain est toujours aussi préoccupante, marquée par une augmentation significative des cyberattaques, notamment des ransomwares et des attaques par déni de service, ciblant principalement les entreprises et les institutions gouvernementales. Ces attaques révèlent une vulnérabilité croissante, posant ainsi des risques majeurs pour la sécurité nationale et le bien-être des citoyens.

De plus, les cybercriminels adoptent des tactiques de plus en plus sophistiquées, utilisant des outils avancés et des méthodes d'ingénierie sociale, rendant la détection et la prévention des attaques plus difficiles.

Sans oublier que dans le contexte actuel de cyberguerre, la cybercriminalité évolue très rapidement, donnant naissance à de nouvelles formes de menaces qui vont au-delà des attaques traditionnelles.

Selon vous, quelle est la meilleure approche pour les États africains ? La souveraineté numérique est-elle la meilleure option ou serait-il bénéfique de se pencher vers une autonomie stratégique du Cyberespace africain ?

C'est une question complexe, mais je pense qu'une approche hybride pourrait être la plus bénéfique. La souveraineté numérique est essentielle pour protéger les données des citoyens et des entreprises, permettant aux États d'exercer un contrôle sur leurs ressources numériques et d'établir des réglementations adaptées à leurs réalités.

D'un autre côté, l'autonomie stratégique permet aux États de gérer leurs systèmes numériques de manière indépendante tout en restant ouverts à la coopération régionale et/ou internationale. Cela renforce leur résilience face aux cyberattaques et favorise des initiatives communes entre pays africains, tout en offrant un meilleur accès aux innovations mondiales. Néanmoins, il est important de reconnaître que les pays africains peuvent encore dépendre des technologies étrangères, notamment de grandes puissances, limitant ainsi leur autonomie aussi bien stratégique que technologique.

Auriez-vous des exemples concrets de réussite ou d'échec de cette approche en Afrique à partager avec nous ?

Il existe plusieurs exemples intéressants.

Concernant la souveraineté numérique : Le Kenya a développé des politiques robustes en matière de cybersécurité, notamment avec la création de l'Autorité nationale de la cybersécurité. Cela a permis de renforcer la sécurité des données, de protéger les infrastructures critiques et de surtout promouvoir l'innovation locale dans le secteur technologique. Le Kenya est également devenu un hub pour les start-ups technologiques, ce qui témoigne de l'impact positif de ces efforts sur l'économie numérique.

Concernant l'autonomie stratégique : L'Afrique du Sud est un bon exemple. Le pays a établi des partenariats régionaux notamment pour partager des informations sur les menaces. Cela a renforcé la coopération entre les États et a permis une réponse collective aux cyberattaques.

Quels conseils donneriez-vous aux décideurs africains pour naviguer ces défis ?

Au-delà de la mise en place de réglementations claires et adaptées aux réalités, les décideurs africains devraient adopter une approche encore plus stratégique et intégrée. Il est crucial d'investir dans des infrastructures numériques robustes et sécurisées, y compris le développement de centres de données locaux. La formation demeure également essentielle ; il faut s'assurer que les équipes soient bien formées tout en favorisant la formation continue.

Enfin la sensibilisation du public ne doit pas être négligée. Promouvoir des campagnes d'éducation à grande échelle pour informer les citoyens sur les risques en ligne et les bonnes pratiques en matière de cybersécurité aidera à créer une culture de sécurité au sein de la société.

Dans quelle logique s'inscrit l'Institut Africain de Cybersécurité et Sécurité des infrastructures ?

L'Institut Africain de Cybersécurité et Sécurité des infrastructures s'inscrit dans une logique de renforcement des capacités et de collaboration régionale face aux défis croissants de la cybersécurité en Afrique. Notre objectif principal est de créer un cadre institutionnel solide pour former des experts en cybersécurité et donc de répondre à un besoin immédiat, promouvoir des recherches innovantes et développer des politiques adaptées aux réalités locales. En favorisant l'échange d'expertise entre les pays africains, nous visons à créer un réseau de soutien qui permet de partager des informations sur les menaces et les meilleures pratiques. Nous continuons à nous développer en République Démocratique du Congo tout en gardant l'ambition de s'ouvrir à d'autres pays dans les années à venir.

Des perspectives d'avenir pour l'état sécuritaire de l'Afrique ?

Les perspectives d'avenir pour l'état sécuritaire de l'Afrique sont à la fois prometteuses et complexes. Il y a une belle prise de conscience des enjeux de la cybersécurité, ce qui pousse les gouvernements à élaborer des politiques plus robustes et à investir dans des infrastructures numériques. En revanche, les challenges restent significatifs, notamment en raison de la diversité des contextes politiques et économiques, des ressources humaines et financières limitées dans certains pays et de la dépendance aux technologies étrangères.

Malgré ces obstacles, nous restons optimistes quant aux années à venir. Avec un engagement accru en matière de collaboration régionale et d'innovation locale, l'Afrique a le potentiel de renforcer sa cyber résilience et d'assurer un avenir plus sûr pour ses citoyens.

Propos recueillis par **Léa Arselle TSAFACK**

Interruption quasi générale de la fibre optique en Afrique : CE QU'IL FAUT COMPRENDRE

Le 14 mars 2024, treize pays de la côte Ouest et du Sud de l'Afrique ont connu une dégradation significative de la qualité du service Internet, avec des interruptions presque totales dans certains cas. Cette panne serait due à un glissement de terrain au large de la Côte d'Ivoire, provoquant la déconnexion de plusieurs câbles sous-marins à fibre optique qui desservent cette région. Parmi ces câbles figurent l'ACE (Africa Coast to Europe), le SAT-3 (Submarine Atlantic), le WACS (West Africa Cable System) et le MainOne. Il est important de souligner que les pannes de câbles sous-marins ne sont pas inédites. Environ 100 coupures de fibre se produisent chaque année, généralement affectant des câbles isolés. Cependant, le fait que plusieurs câbles aient été endommagés simultanément rend cet incident particulièrement marquant en raison de son ampleur.

Bien que cet événement soit d'origine naturelle, il soulève des questions cruciales sur la stratégie des pays africains concernant leurs connexions avec le reste du monde. Dans un contexte où Internet joue un rôle central dans nos vies économiques, sociales et politiques, et où 90 % du contenu consommé est hébergé hors d'Afrique, la quasi-totalité des communications Internet repose encore sur la fibre optique, les communications par satellite ne représentant qu'environ 1%, malgré l'émergence progressive de la technologie Starlink sur le continent. Au-delà de la panne elle-même, cet incident met en lumière l'impuissance des pays africains concernés à résoudre le problème de manière autonome et à rétablir la connectivité rapidement. Cette situation soulève plusieurs enjeux qui témoignent de la dépendance de l'Afrique vis-à-vis de ses canaux de communication, comme le souligne l'ouvrage L'Afrique au risque d'une cybercolonisation. Concernant les câbles à fibre optique, deux principaux leviers de cette dépendance peuvent être identifiés.

Propriété des câbles

Les premiers câbles reliant le continent appartiennent à des consortiums où les pays africains sont généralement représentés par leurs opérateurs télécoms qui gèrent les points d'atterrissage. Cependant, ces consortiums sont souvent dominés par des entreprises étrangères disposant des ressources technologiques avancées. Pire encore, les câbles les plus récents, jugés essentiels pour l'avenir numérique du continent en raison de leur capacité et de leur maillage amélioré, sont presque exclusivement contrôlés par des sociétés privées telles que Google (Cable Equiano), Facebook (2Africa) et Orange (projet Djoliba incluant également un segment terrestre).

Maîtrise technologique

La conception, la fabrication, l'installation et la maintenance des câbles sous-marins nécessitent une expertise avancée qui passe par la recherche et le développement pour concevoir de nouveau type de câble toujours plus performant, l'identification, l'extraction et la transformation des matière première permettant de les fabriquer, la construction des navires spécialisés pour la pose ou la maintenance (Exemple du célèbre navire Léon Thévenin, câblier français appartenant à Orange Marine et spécialisé dans la maintenance des câbles sous-marins, très actif sur les côtes africaines). Il est à noter qu'un petit nombre d'acteurs mondiaux dominent ce secteur. Il s'agit notamment des opérateurs Alcatel Submarine Networks (France), TE Subcom (États-Unis) et NEC (Japon), qui détiennent ensemble environ 75 % du marché mondial, formant ainsi un oligopole. Cette dépendance ne concerne donc pas uniquement les pays africains.

Cette panne a agi comme un électrochoc, soulignant brutalement notre dépendance technologique en la matière. Cela a naturellement fait surgir la question de la "souveraineté numérique" dans le débat public, incitant divers acteurs de la société africaine (journalistes, hommes politiques, influenceurs, etc.) à s'en emparer et à exprimer leurs opinions, parfois peu structurées, mais révélatrices d'une prise de conscience que le LARC tente de mettre en lumière depuis plusieurs années.

Cependant, compte tenu du niveau de dépendance évoqué précédemment, il est légitime de se poser la question suivante : la souveraineté numérique est-elle toujours un objectif réalisable et opérationnel, ou ce concept est-il devenu inopérant et inapplicable dans notre contexte actuel et au regard de nos capacités effectives à pouvoir le mettre en œuvre ? Étant désormais conscients des enjeux sous-jacents et des contraintes qui nous lient, ne serait-il pas plus pertinent d'aspirer à une " autonomie stratégique " qui pourrait être plus accessible et plus immédiate pour les Etats africains ? En analysant la situation, on constate qu'à l'exception de quelques cyberpuissances (comme les États-Unis, la Chine, ou la Russie), la plupart des puissances intermédiaires (comme la Turquie ou Israël) semblent privilégier l'autonomie en s'appuyant sur une logique d'interdépendance avec des partenaires partageant des intérêts stratégiques ou idéologiques communs. Au-delà de la théorie politique et d'une rhétorique ambiante sur la souveraineté numérique qui commence à ressembler à une tendance dépassée, cette approche plus pragmatique mérite d'être explorée par les décideurs africains.

DJIMGOU NGAMENI

Les Etats-Unis interdisent Kaspersky pour cyberespionnage : ECLAIRAGE

Nous sommes en 1987. Peter Pasko (prononcez Pashko) et Miroslav Trnka, bidouillent sur les rares ordinateurs disponibles en Tchécoslovaquie quand ils tombent sur un programme étrange qui s'attaque au système d'exploitation. Ils décident alors de répliquer en mettant au point des lignes de code qui détruisent ce qui est le premier Malware de l'Histoire. Kaspersky découvre les outils sur les ordinateurs au Moyen-Orient en 2014, et son logiciel antivirus les détecte sur une machine aux États-Unis. Kaspersky croyait que la machine avait été infectée par le logiciel de surveillance Equation Group, mais en fait, c'était l'ordinateur personnel d'un employé de la NSA nommé Nghia Hoang Pho, qui avait mal pris à la maison des documents classifiés et du code NSA qu'il aidait à développer qui étaient liés à l'ensemble d'outils Equation Group. En février 2015, le service d'espionnage international de la Stasi du département de la science et des technologies du HVA, annonçait la découverte d'une suite de programmes d'espionnage sophistiqués il a surnommé les outils du Groupe d'équations bien avant que les Shadow Brokers ne commencent à fuir les outils du même groupe en 2016. Le logiciel Kaspersky a téléchargé le contenu de l'ordinateur de Pho sur les serveurs de la société, dans le cadre d'une procédure standard que les programmes antivirus utilisent pour analyser le code malveillant précédemment non découvert. Le PDG Eugene Kaspersky avait ordonné à ses chercheurs de détruire les fichiers.

Mais la collecte de fichiers a contribué à alimenter les allégations des États-Unis selon lesquelles Kaspersky lui-même constitue une menace pour la sécurité. Car, inconnu de Kaspersky à l'époque, Israël avait piraté le réseau de la compagnie en 2014, et en 2015 avait discrètement alerté le renseignement des États-Unis qu'il a vu des agents de renseignement russes siphonner les outils de la machine Pho avec la coopération ou les connaissances de Kaspersky, en utilisant son logiciel antivirus.

Le public n'a appris cette allégation qu'en février 2017 lorsque des sources anonymes l'ont divulguée aux journalistes. Mais aucune preuve étayant cette affirmation n'a jamais été rendue publique, et personne n'a expliqué comment les Israéliens savaient que l'extraction ne faisait pas seulement partie de l'analyse standard des infections et du nettoyage. En 2015, le FBI a commencé à enquêter sur les relations de Kaspersky avec le gouvernement russe, et en 2016, le bureau avait exhorté les entreprises américaines privées de couper les liens commerciaux avec l'entreprise. Puis, en février 2017, le mois où Martin a été inculpé, le Department of Homeland Security a envoyé un rapport secret aux agences gouvernementales disant que le logiciel Kaspersky posait un risque pour la sécurité nationale.

Le compte @hal_999999999 avait été utilisé pour adresser cinq messages privés à deux chercheurs de Kaspersky. Le premier envoyé le 13 août 2016, somait l'un des chercheurs d'organiser une conversation avec Yevgeny, probablement le PDG de Kaspersky Lab, Eugène Yevgeny Kaspersky. Le message n'indiquait pas la raison de la conversation ou le sujet. Mais immédiatement après avoir répondu, les deux chercheurs ont été bloqués par le compte en question. Les deux messages sont arrivés juste 30 minutes avant qu'un groupe anonyme connu sous le nom de Shadow Brokers commence à déverser des outils classifiés de la NSA en ligne et annonce une vente aux enchères pour des code volés de l'agence au prix de $1 million en Bitcoin. Comme Snowden, Martin avait une autorisation de sécurité nationale top secret pour avoir travaillé pour la défense et le renseignement. C'est par ailleurs là où certains de ses vols ont eu lieu.

Kaspersky est la société la plus signalée pour opérations d'espionnage aux USA ces six dernières années. L'Allemagne avait recommandé, quelques semaines après l'invasion russe de l'Ukraine, d'éviter d'utiliser ses services. L'Italie avait dans la foulée ouvert une enquête. «Attribuer des cyberattaques à tel ou tel pays ou tel ou tel groupe est éminemment compliqué». Les Africains vérifient-ils l'origine de leur antivirus ? Un groupe, qu'il soit russe ou privé, peut-il vraiment être indépendant du Kremlin ?

OUMAR DIALLO

Polémique autour de STARLINK

Le réseau Starlink de SpaceX, avéré comme une solution pour les instabilités liées au réseau Internet en Afrique, fait l'objet de controverses depuis son arrivée sur le continent. Afin d'alimenter le débat, quelques spécialistes ont été abordés pour se prononcer sur les implications stratégiques d'une telle technologie.

Kevin W.

Information Security Officer, Cybersecurity Consultant

Il est légitime que des préoccupations de sécurité nationale poussent certains gouvernements africains à évaluer avec prudence l'adoption de Starlink. Toutefois, cette réticence paraît contradictoire lorsqu'on considère la forte dépendance du continent aux technologies étrangères, qu'il s'agisse des appareils électroniques, des services fournis par les GAFAM, ou de l'intelligence artificielle. Malgré des infrastructures numériques limitées, l'Afrique a vu émerger des talents remarquables dans des domaines tels que la mécanique et l'informatique, innovant avec des ressources limitées et un accès restreint à des informations actualisées. L'arrivée de Starlink pourrait représenter un catalyseur majeur, en particulier dans les zones rurales, en offrant une connectivité fiable, ouvrant la voie à un essor accéléré de l'innovation, de l'éducation, et des opportunités économiques. Plutôt que de l'écarter, une approche réfléchie consisterait à encadrer cette technologie par des régulations adaptées, afin de tirer parti de ses immenses bénéfices tout en assurant la protection des intérêts nationaux.

Kevin W.

Haris FOTSO

IA, Sofware ING, Dev Full Stack

En tant qu'expert IT, je reconnais que l'introduction de technologies comme Starlink en Afrique présente à la fois des avantages et des défis. Le potentiel de Starlink pour améliorer la connectivité, en particulier dans les zones reculées, est indéniable. Cependant, les préoccupations soulevées par certains Etats africains, comme le Mali, sont légitimes dans un contexte où la cybersécurité est une priorité cruciale. L'absence d'un contrôle strict sur l'introduction de nouvelles technologies pourrait créer des vulnérabilités, notamment en matière de sécurité nationale, si ces réseaux sont exploités sans régulation adéquate.

Cela étant dit, les préoccupations liées à la dépendance à des infrastructures extérieures (câbles sous-marins, serveurs hors du continent etc.) sont également un point de réflexion critique. Starlink ne devrait pas être isolé comme un cas à part ; il s'inscrit dans un écosystème technologique global où l'Afrique est déjà dépendante d'infrastructures et d'algorithmes contrôlés par des entités extérieures.

En revanche, il est important de noter que certains pays comme le Ghana ont validé et accueilli favorablement la technologie Starlink. Le Ghana a pris en compte les avantages économiques et sociaux liés à l'amélioration de la connectivité, tout en mettant en place des régulations pour assurer que la technologie soit exploitée de manière sécurisée et légale.

En fin de compte, l'implémentation de Starlink nécessite un équilibre entre les avantages de la connectivité et la protection des intérêts nationaux. Un cadre législatif robuste, avec des partenariats entre gouvernements et entreprises technologiques, pourrait atténuer les risques tout en maximisant les bénéfices pour les populations africaines.

Haris FOTSO

Le point avec François HEUTCHOU

Comment l'Afrique peut-elle renforcer sa résilience numérique tout en développant une indépendance technologique

Mots clés : Souveraineté numérique, Afrique, Autonomie stratégique, Résilience numérique, Cybersécurité en Afrique, Protection des données, Infrastructures numériques

A l'ère de la mondialisation numérique, la question de la souveraineté numérique s'impose avec force dans les débats stratégiques en Afrique. Ce concept, souvent lié au contrôle des données et des infrastructures numériques, renvoie à la capacité d'un État à garantir sa sécurité et son indépendance dans le cyberespace. Parallèlement, la notion d'autonomie stratégique apparaît comme une voie pragmatique pour les nations africaines cherchant à se positionner face aux puissances technologiques mondiales comme les États-Unis et la Chine. Le défi est double : développer des infrastructures numériques robustes tout en préservant la maîtrise sur les données et les ressources technologiques.

La Souveraineté Numérique : Maîtriser les Données et les Infrastructures

La souveraineté numérique implique le développement de centres de données locaux, la création de réseaux sécurisés et la mise en place de réglementations sur la protection des données. Cela inclut le stockage de données sur des serveurs nationaux, le développement de plateformes locales pour les services cloud et l'élaboration de normes de cybersécurité. Les pays africains cherchent à limiter leur dépendance envers les géants technologiques étrangers pour mieux contrôler la cyber-souveraineté. Cependant, cette souveraineté reste un défi de taille. La plupart des infrastructures de données sont sous-développées, et les solutions de cybersécurité sont souvent importées de l'extérieur, ce qui expose les États à des risques de surveillance et de cyberespionnage. Les pays africains sont confrontés à la dépendance technologique envers des acteurs étrangers, ce qui les rend vulnérables face à des pratiques telles que la surveillance de masse.

L'Autonomie Stratégique : Une Approche Pragmatique

Face aux difficultés d'atteindre une souveraineté numérique complète, l'autonomie stratégique offre une solution plus réaliste. Il s'agit de diversifier les partenariats technologiques et de renforcer les compétences locales, tout en maintenant un certain contrôle sur les données critiques. Cette approche permet de limiter la dépendance vis-à-vis d'un seul acteur tout en favorisant l'innovation locale. Les partenariats public-privé peuvent aider à développer des centres de données tout en collaborant avec des acteurs internationaux pour le transfert de compétences. Des initiatives comme Smart Africa Alliance favorisent la mutualisation des infrastructures à l'échelle régionale, ce qui permettrait de bâtir une ré-

silience numérique tout en offrant une marge de manœuvre pour définir leurs propres standards de cybersécurité.

Cybersécurité et Gouvernance des Données : Des Priorités

Que ce soit pour la souveraineté numérique ou l'autonomie stratégique, la cybersécurité est une condition essentielle pour protéger les systèmes d'information. Les cyberattaques, ransomwares, et cyberespionnage sont des menaces qui pèsent sur les infrastructures des États africains. Pour y faire face, il est crucial de développer des architectures de cybersécurité résilientes et de promouvoir une culture de la sécurité numérique. La gouvernance des données est également au cœur de la souveraineté numérique. Les pays africains doivent mettre en place des cadres juridiques robustes pour la protection des données personnelles, inspirés du RGPD européen mais adaptés aux contextes locaux. Cela permet de renforcer la confiance des citoyens et d'attirer les investissements étrangers tout en garantissant la sécurité des informations sensibles.

Renforcer les Capacités Régionales et l'Innovation Locale

La mutualisation des ressources régionales, encouragée par l'Union Africaine et la Convention de Malabo, permet de construire des centres de réponse aux incidents et d'améliorer la cybersécurité. L'investissement dans les start-ups locales et les incubateurs numériques est également crucial pour créer des solutions adaptées aux besoins africains. Des pays comme le Rwanda, le Kenya, et le Ghana montrent qu'il est possible de concilier développement technologique et maîtrise des données à travers des stratégies de partenariat équilibrées.

Vers une Convergence entre Souveraineté Numérique et Autonomie Stratégique

Plutôt que de choisir entre souveraineté numérique et autonomie stratégique, les pays africains pourraient adopter une approche hybride, combinant les deux concepts. Par exemple, l'investissement dans des centres de données nationaux peut être réalisé tout en collaborant avec des partenaires internationaux pour le transfert de compétences. Cette approche permet de bâtir une résilience numérique tout en se préparant à une maîtrise accrue de leurs infrastructures. Des initiatives telles que l'African Continental Free Trade Area (AfCFTA) encouragent la coopération régionale dans le secteur numérique et offrent une opportunité de renforcer l'autonomie technologique de l'Afrique. En soutenant les technologies locales et en améliorant les compétences numériques, le continent peut progresser vers un cyberespace plus sécurisé et autonome.

Une Afrique Numérique Résiliente et Ambitieuse

Le développement d'une Afrique plus autonome dans le domaine numérique est un enjeu majeur pour le continent. Cependant, une approche uniquement basée sur la souveraineté numérique pourrait être coûteuse et complexe. L'autonomie stratégique offre une voie plus pragmatique pour renforcer la résilience numérique tout en préparant le terrain pour une plus grande indépendance. En investissant dans la formation des talents locaux, en diversifiant les alliances internationales et en soutenant l'innovation africaine, l'Afrique peut tracer son propre chemin dans le cyberespace. L'objectif est de bâtir une économie numérique inclusive et de garantir la sécurité des données de ses citoyens, tout en se positionnant comme un acteur incontournable sur la scène numérique mondiale.

François HEUTCHOU

NOS PARTENARIATS

L'établissement de partenariats stratégiques nous a permis de renforcer notre impact en cyberstratégie dans le cyberespace africain. Avec **Africa Cybersecurity Mag,** le LARC a signé une convention qui lui permet d'accroître sa visibilité sur les réseaux sociaux, tout en agissant en symbiose quant à ses différents projets d'implication régionale. Parallèlement, notre accord de principe avec **Best Practice** cabinet du Rtd Colonel Roger KUITCHE favorise notre participation à des événements clés du secteur, facilitant ainsi le partage d'expertise et le réseautage. Nous avons par ailleurs l'opportunité de faire intervenir nos chercheurs dans des situations où leur expertise est chère. Enfin, notre collaboration avec l'**IFP RHOPEN LABS** pour la labellisation de nos formations garantit la qualité et la pertinence de nos programmes d'enseignement, offrant ainsi un gage de confiance à nos apprenants.

ÉVÉNEMENTS

Le LARC se prépare à plusieurs événements marquants dans les mois à venir. Tout d'abord, la publication de notre tout premier Rapport biennal est prévue pour le premier trimestre de l'année 2025. Ce bulletin qui se positionne surtout en analyste stratégique et critique, portera sur l'évolution de la cyberstratégie en contexte africain, passant ainsi par une analyse approfondie des tendances et défis actuels. De plus, nous co-organisons le Salon National de la Cyberstratégie en collaboration avec le cabinet ORIN Consulting Group et le Cameroon Digital Think Tank, qui se tiendra à Yaoundé du 30 janvier au 1er février 2025 (date provisoire). Cet événement est placé sous le thème : "Cyberstratégie et Cyberdéfense : Défis et Intégration dans la doctrine sécuritaire et défensive du Cameroun" Nous rassemblerons les experts et acteurs clés du cyberespace pour discuter de ses enjeux cruciaux pour l'Afrique sans manquer de soumettre des solutions cyber innovantes et inédites.

PROJETS EN COURS

Plusieurs projets passionnants sont en préparation chez le LARC. Le Tome 2 de la série «Cyberstratégie Africaine» de DJIMGOU NGAMENI est notamment en cours d'édition. Ce deuxième volume tentera d'approfondir les piliers précédemment amorcés suivant une volonté praticable sur le continent. Parallèlement, notre programme LARC ACADEMIA sera mis à jour d'ici mars, avec des certifications en cyberstratégie de niveau 1 et 2, afin de garantir une formation de qualité adaptée aux défis de notre époque. Enfin, nous organisons également des Masterclass sur la cyberstratégie, visant à partager des connaissances théoriques et pratiques pour le renforcement de compétences des professionnels du secteur.

Leslie MBANGO Epse B.N.

Mise sur pied d'une politique de cryptographie souveraine et d'un algorithme de chiffrement propriétaire : Point de départ de l'autonomisation stratégique de l'Afrique !
Suivant cet idéal de matérialisation de la pensée stratégique du cyberespace africain, par où commencer concrètement ?

L'ouvrage Cyberstratégie africaine Tome I _ que je vous recommande vivement_, suggère une démarche de mise en œuvre effective du concept de « cyberstratégie africaine », articulée autour de cinq piliers : Un traité africain de cyberstratégie, une finalité claire et une ambition assumée, un modèle d'innovation technologique propre à l'Afrique, un discours nouveau sur le numérique en Afrique, ainsi qu'un Programme Africain d'Industrialisation Numérique. Si les 4 premiers piliers relèvent de la dimension théorique de cette démarche et trouvent des débuts de réponse dans les publications du LARC, le dernier pilier relève quant à lui de la dimension technologique de notre approche. Conçu comme un guide pratique, le Programme Africain d'Industrialisation Numérique doit reposer sur l'ensemble de la chaîne de valeur d'une industrie technologique partant de l'inventaire des matières premières utiles à cette industrie, l'inventaire et l'usage des sources d'énergie, la stratégie de transformation des matières premières, le choix des technologies à développer à chaque couche du cyberespace sur la base d'une analyse approfondie, jusqu'à la mise en place de nos propres normes et standards, etc.

Ainsi, pour initier ce programme en l'inscrivant dans une logique d'autonomie stratégique dans le cyberespace, il convient d'identifier des projets à fort impact sur cette finalité. L'un des premiers projets qu'il nous semble urgent de réaliser est le développement d'une politique cryptographique souveraine et d'un algorithme de chiffrement propriétaire à l'échelle africaine.

De quoi s'agit-il concrètement ?

La cryptographie a pour but de protéger la confidentialité des informations, stockées localement ou transmises à un partenaire via des liaisons non maîtrisées, en s'appuyant sur des secrets, dits clés. Pratiquée dès l'Antiquité, c'est une pratique multimillénaire dont on peut retrouver les racines en Afrique. C'est en tout cas ce que nous révèle le Dr J.P MBELEK dans un article intitulé «Le déchiffrement de l'os d'Ishango » paru dans la revue ANKH n° 10/11 2001-2002. Pour lui, plus encore qu'un jeu mathématique, cet os de babouin daté à environ 25.000 ans se présente aussi comme un document crypté, basé sur un codage rudimentaire avec signature à clé publique et clé secrète. Le Dr Cécile Bernal dans ses travaux explore également « L'art de la cryptographie dans l'Égypte ancienne».

Si pendant des siècles, les mécanismes utilisés (code de César, chiffre de Vigenère, Os d'Ishango, Hieroglyphes, etc.) sont restés rudimentaires, les techniques utilisées se sont depuis largement complexifiées. La cryptographie a d'abord connu des usages militaires et diplomatiques, avec une dimension stratégique évidente qu'on a pu observer lors des deux guerres mondiales (le Radiogramme de la Victoire lors de la Première Guerre mondiale, la célèbre machine Enigma lors de la seconde). De nos jours, la discipline s'est considérablement modernisée, s'adaptant au monde numérique. Par leur smartphone, leur carte bancaire, ou même leur passeport, les africains utilisent quotidiennement des moyens cryptographiques la plupart du temps sans en avoir réellement conscience. C'est le cas quand vous utilisez l'application Whatsapp par exemple. La cryptographie, souvent invisible, est ainsi au cœur de la sécurité des données des citoyens comme des États, en assurant leur confidentialité et leur intégrité.

Le chiffrement, l'une de ses applications les plus répandues, est considérée comme la seule garantie de protection (confidentialité) des communications et données sensibles des Etats. Prenons le chiffrement de bout en bout par exemple. Reconnu par les experts comme la meilleure pratique en la matière, c'est un procédé de transmission des données (vidéo, audio, texte, image, etc.) qui permet uniquement à l'émetteur et au récepteur de les déchiffrer sans aucune autre phase de déchiffrement entre les correspondants. Ce qui permet d'empêcher toute écoute électronique y compris par les fournisseurs de télécommunications, d'accès Internet et même

par l'éditeur de la solution qu'on utilise (logiciel d'envoi de mail ou de visioconférence).

Ainsi, en théorie, en utilisant le chiffrement de bout en bout, personne ne devrait être en mesure d'accéder aux clés de chiffrement nécessaires pour déchiffrer la conversation. Cependant, en pratique, les acteurs de l'industrie cryptographique (ceux qui développent les algorithmes ou encore ceux qui proposent des solutions indépendantes de gestion des clefs de chiffrement) et les agences de renseignement (qui insèrent les portes dérobées dans les solutions (matérielles comme logicielles) les plus répandues sur le marché, peuvent dans certaines conditions, s'autoriser l'accès au secret (clés de chiffrement). C'est une pratique qui est désormais de notoriété publique, confirmée par nombres d'actualités (écoute des dirigeants Européens par l'allié américain), de révélations (cf. Edward Snowden), et de rapports d'experts et autres ONG.

Fort de ce qui précède, mettant en évidence une forme de fragilité des Etats et leur dépendance technologique aux algorithmes (pourtant admis comme standard international), la cryptographie (chiffrement, intégrité) s'impose comme une question de sécurité nationale et un enjeu majeur d'autonomie stratégique dans le cyberespace !

Les Etats-Unis utilisent les algorithmes AES et RSA sur lesquels ils ont le total contrôle à travers leurs entreprises du secteur et leurs agences de renseignement. Ces algorithmes sont pourtant considérés comme standard mondial en matière de chiffrement (utilisé dans une grande partie du monde), ce qui donne un avantage stratégique aux USA que ses rivaux perçoivent très mal. C'est d'ailleurs la raison pour laquelle certains d'entre eux ont développé leurs algorithmes de chiffrement propres, conçus pour répondre à leurs besoins spécifiques en matière de sécurité nationale (communications gouvernementales, militaires, diplomatiques, etc.), réduisant ainsi le risque d'espionnage ou d'interception par des acteurs malveillants. Citons par exemple les cas des algorithmes Japonais (Camelia), Nord-Coréen (SEED), Russe (Kuznyechik), Chinois (ZUC), etc.

Afin de contourner cette dépendance aux algorithmes, certaines entreprises développent avec l'aide de leurs États des modules matériels de sécurité (Hardware Security Module ou HSM). Il s'agit d'un équipement électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clefs cryptographiques ainsi qu'effectuer des opérations cryptographiques sensibles. Cependant, pour pouvoir commercialiser facilement leur équipement dans le monde, ils sont obligés de le faire fonctionner avec les algorithmes qui dominent le marché : AES et RSA.

Ainsi donc, les solutions cryptographiques utilisées dans la plupart des pays africains, qui tournent autour des algorithmes reconnus comme stratard, sont conçues et mises en place par des opérateurs étrangers. Or dans ce domaine le principe est très simple : Celui qui détient la clé détient le secret ! La sécurité des communications et données sensibles de nos Etats est donc proportionnelle au niveau de confiance que ces derniers accordent aux opérateurs étrangers qui maîtrisent et contrôlent les technologies matérielles et logicielles utilisées (gestions des clés, algorithmes de chiffrement). D'où l'impérieuse nécessité de développer nos propres solutions en la matière, en commençant par un algorithme de chiffrement propre, basé sur les avancées les plus récentes dans le domaine.

Quelles implications immédiates pour l'Afrique ?

Le développement d'un algorithme de chiffrement propre constituerait un levier stratégique majeur pour renforcer l'autonomie des pays africains dans le cyberespace. Cela permettra par exemple de limiter leur dépendance à l'égard des technologies de chiffrement développées par des entreprises ou des États étrangers, qui bien souvent comportent des portes dérobées, de mieux protéger les données sensibles des gouvernements, des entreprises critiques et des citoyens contre le cyberespionnage, de stimuler la recherche et le développement dans le domaine de la cybersécurité en général, et de la cryptographie en particulier.

Puisqu'on parle de tendance, l'avènement prochain des ordinateurs quantiques menace fortement l'efficacité des algorithmes de chiffrement existants aujourd'hui. Ce qui pousse la recherche mondiale vers les algorithmes dit "post-quantique ". Tout en concentrant les efforts initiaux sur le développement d'un algorithme "classique" en s'appuyant sur les trouvailles scientifiques récentes en la matière, le post-quantique est une voie que nos Etats et chercheurs ne devraient pas trop tarder à explorer, les autres ayant déjà pas mal d'avance sur le sujet. Le chiffrement homomorphique, qui rompt avec l'approche classique en permettant de manipuler des données sans avoir à les déchiffrer, est une piste qui nous semble prometteuse pour notre contexte immédiat. Comptant parmi les meilleurs mathématiciens au monde, l'Afrique ne manque certainement pas d'atouts pour relever ces défis de la recherche avancée en cryptologie.

DJIMGOU NGAMENI

Innovation et renforcement des capacités

- Le Nigeria a procédé en octobre dernier au lancement d'un Centre National de Cybersécurité pour coordonner les efforts de lutte contre la cybercriminalité et fournir une assistance technique aux agences gouvernementales. Un Cybersecurity Council a été initié en mai pour coordonner les efforts entre les secteurs public et privé. Le même mois, la société nigériane Softrite a lancé un logiciel utilisant l'IA pour détecter les menaces en temps réel et contribuer à la sécurisation des infrastructures critiques.
- En juin, le gouvernement Kenyan a annoncé le renforcement de la loi sur la cybersécurité avec des pénalités plus sévères pour les violations de données. Le National Cyber Security Strategy a été mis à jour, incluant des mesures de protection pour les infrastructures critiques. Plus tôt en Mars, le déploiement du câble sous-marin 2Africa a été achevé, améliorant considérablement la connectivité Internet dans plusieurs pays africains, notamment l'Égypte, le Kenya et l'Afrique du Sud.
- Le gouvernement senegalais re-élabore sa stratégie cyber à travers l'établissement d'un Cloud Souverain sur le territoire. En effet, le New Deal Technologique du Sénégal envisage une conservation locale des données personnelles de ses habitants. Le 27 septembre, la signature d'un protocole d'accord entre l'Etat du Sénégal et le géant Google est annoncée. Par cette initiative, le pays entend répondre aux besoins croissants des entreprises et administrateurs de la Sous-Région.

Législation et politiques stratégiques

- En Mars, le gouvernement ivoirien a lancé un Plan National visant à renforcer la cybersécurité des infrastructures critiques. Ce plan inclut la création d'un cadre réglementaire et des formations pour les agents publics.
- Le mois de Mai a été marqué par la suspension et la saisie des kits de connexion. Les raisons ? STARLINK opererait de façon illégale, sans aucune licence. Ce type de technologie sophistiquée est un concurrent non négligeable de la Cameroun Télécommunications et un risque de sécurité nationale du moment où ses services sont hors de contrôle de l'État camerounais. On se souvient qu'un mois plus tôt, la ministre des postes et Télécommunications avait recommandé à Space X de se soumettre aux conformités de l'Agence de Régulation des Télécommunications. Sans réaction prompte, le service s'est tout simplement vu interdit en territoire camerounais.
- Le Mali adoptait tout récemment en Juin la Loi sur la Protection des Données Personnelles, visant à sécuriser le traitement des informations personnelles et à aligner le pays sur les normes internationales. Ils ont réuni ce même mois d'octobre
- Le gouvernement Kenyan a lancé une mise à jour de sa Stratégie Nationale de Cybersécurité depuis Mai. Axée sur la protection des infrastructures critiques et le renforcement de la résilience face aux cybermenaces.
- Le Gouvernement sud-africain adoptait en Juin un Règlement sur la protection des données qui renforce les droits des consommateurs et impose des obligations strictes aux entreprises concernant la gestion des données personnelles.

Léa Arselle TSAFACK

(2024)

Le cyberespionnage : Une arme de guerre entre les Etats par Diamond Security Agency

Publié en Avril dernier par Diamond Security Agency sous la direction de Laïcana Coulibaly, ce livre blanc initie une étude inédite en Afrique. Entre défis, enjeux et solutions en matière de cyberespionnage et cyberattaques en Afrique, les préoccupations de ses auteurs sont clairement énoncées. Si vous êtes intéressés par les enjeux contemporains du cyberespionnage en Afrique ou par les stratégies de cybersécurité régionales, alors ce texte est à lire absolument. Il s'inscrit par ailleurs, en droite ligne d'une volonté de souveraineté numérique.

(2022)

Leçons d'Afrique en matière de cyber-stratégie

Publié le 18 mars 2022 par le Centre d'Études Stratégiques de l'Afrique, cet éclairage de cyber-stratégie postule que face à la recrudescence de la cybercriminalité et des cyberattaques, les Etats africains devraient tous se munir d'une Stratégie Nationale de cybersécurité. Cette dernière valable pour au plus cinq ans constitue selon les auteurs de la publication Nate D.F. Allen et Abdul Ajijola, l'un des impératifs en matière d'autonomie stratégique dans le cyberespace africain. Cette analyse est à découvrir absolument.

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 cyberespace africain pour l'Afrique.

Pr Isidore BIKOKO

Nos valeurs

- Défi
- Engagement
- Créativité
- Coopération
- Réflexion.

Notre approche

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

L' Equipe

Directeur de publication
François-Xavier DJIMGOU NGAMENI

Conseiller scientifique
Pr Isidore BIKOKO

Rédactrice en chef
Léa Arselle TSAFACK NGULEFEM

Responsable des partenariats et formations
Leslie MBANGO Epse B.N.

Rédacteurs
- FALL BARA
- Rtd Colonel KUITCHE Roger
- Nathalie KIENGA
- Haris FOTSO
- Kévin W.
- Oumar DIALLO
- François HEUTCHOU

Conception
Bertrand FINI

Nos Partenaires

EPA
Ecole Politique Africaine

Africa Cybersecurity Magazine

EDIFI

RHOPEN LABS Academy

éditions ifrikiya

BEST PRACTICE SARL
"LA STRATEGIE MILITAIRE APPLIQUEE AUX ENTREPRISES"
CONSULTING STRATEGIQUE - PRESTATION DE SERVICES

Nous contacter

info@larc.africa

696 683 515

www.larc.africa

LARC

https://larc.africa/