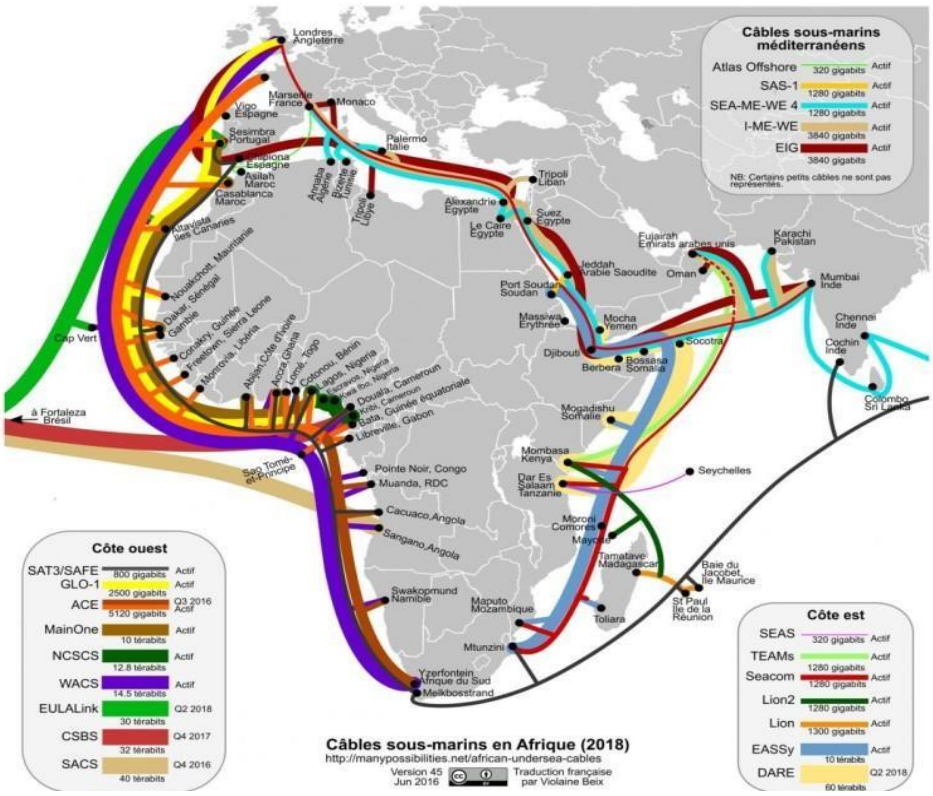
Laboratoire Africain de
Recherches en Cyberstratégie

Inscrire la Cyberstratégie au Cœur des Priorités des États Africains !



Bara FALL

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. 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 en s'assurant que le continent ne soit pas laissé pour compte dans la dynamique technologique mondiale.

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

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.

Introduction

Dans un monde de plus en plus interconnecté, où la technologie est un levier de puissance et de compétitivité, l'Afrique se trouve à un tournant décisif de son développement numérique. Alors que des pays comme les États-Unis, la Chine et l'Union européenne façonnent les normes technologiques mondiales, le continent africain doit relever des défis spécifiques liés à la cybersécurité et à la souveraineté numérique. L'Indice mondial de cybersécurité 2024, publié par l'Union internationale des télécommunications, met en lumière les disparités au sein des nations africaines en matière de préparation et de maturité face aux menaces numériques. Des pays comme le Maroc, le Ghana et le Rwanda se distinguent par des initiatives solides, tandis que d'autres, comme le Nigeria et le Sénégal, doivent encore renforcer leurs capacités. Ce constat souligne l'urgence d'une cyberstratégie cohérente et intégrée qui ne se limite pas à des actions isolées, mais qui encourage l'engagement des dirigeants africains et favorise la coopération régionale et internationale. Il est essentiel de développer des infrastructures locales, d'adopter des réglementations adaptées, et d'investir dans l'éducation afin de préparer les générations futures aux défis numériques. En adoptant une vision audacieuse et proactive, l'Afrique peut non seulement surmonter sa dépendance technologique, mais aussi émerger comme un acteur compétitif sur la scène mondiale. Cette étude vise à explorer les voies stratégiques qui permettront au continent de renforcer sa souveraineté numérique et de s'affirmer dans la dynamique technologique mondiale.

Contexte

L'Indice mondial de cybersécurité 2024, publié par l'Union internationale des télécommunications (UIT), a évalué les engagements en matière de cybersécurité de 194 pays, offrant des insights significatifs sur la situation en Afrique. Ce rapport révèle une large gamme de maturité en matière de cybersécurité parmi les pays africains. Des leaders tels que le Ghana, le Kenya, Maurice, le Rwanda et la Tanzanie se distinguent par des cadres solides et des initiatives avancées.

L'Afrique du Sud, le Bénin, le Togo et la Zambie progressent également, mais des efforts supplémentaires sont nécessaires pour renforcer leurs capacités techniques. En revanche, de nombreux pays, comme le Nigeria, le Sénégal, l'Éthiopie et le Cameroun, font face à des lacunes significatives dans la mise en œuvre de leurs stratégies de cybersécurité. Les principaux domaines d'amélioration incluent le développement des capacités, l'établissement d'équipes d'intervention en cas d'incident, et une coopération régionale et internationale accrue pour renforcer la résilience collective.

Selon cet indice, le Maroc a été placé dans la catégorie la plus élevée, Tier 1, comprenant les pays considérés comme un modèle à suivre en matière de cybersécurité.

À titre de comparaison, les autres pays de la même catégorie que le Maroc, sont l'Allemagne, la France, l'Italie, le Royaume-Uni, le Danemark, le Japon, les États-Unis et l'Espagne, ce qui confirme l'engagement du Maroc à respecter les normes les plus élevées en matière de cybersécurité.

L'indice classe les pays en fonction de cinq indicateurs clés : juridique, technique, organisationnel, renforcement des capacités et coopération.

Imaginons un avenir où l'Afrique devient un leader mondial en technologie en développant des solutions locales innovantes et en renforçant sa souveraineté numérique.

La question de savoir si l'Afrique est prête pour le « **grand combat** » de la souveraineté numérique est complexe et multidimensionnelle, néanmoins avec une approche déterminée et coordonnée, nous avons le potentiel de transformer notre paysage technologique. Pour inverser la tendance de dépendance technologique face aux grandes puissances, nous devons adopter une vision audacieuse et proactive.

I. La souveraineté numérique : dix ans de débats, et après ?

L'ambition qui ressort clairement aussi bien de la stratégie de l'Union Africaine que de l'initiative « Smart Africa », c'est l'utilisation des technologies de l'information et de la communication pour booster le développement socioéconomique du continent.

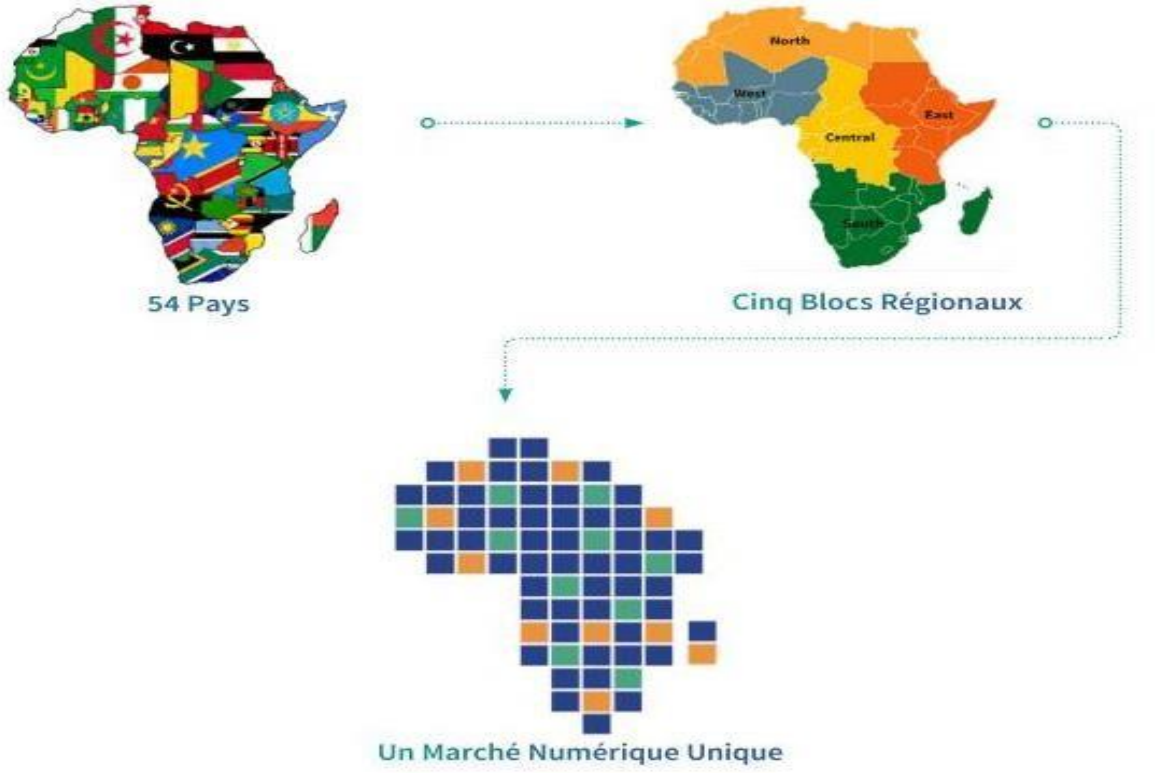


Figure 1 : Schématisation de la vision « Smart Africa »

Smart Africa joue un rôle unique et significatif dans l'écosystème africain de la transformation numérique, bien que sa position soit complexe et soulève plusieurs questions. Cette organisation, soutenue par plusieurs gouvernements et dirigée par le président rwandais, opère de manière quelque peu indépendante de l'Union africaine, en se concentrant sur la cybersécurité et la gouvernance numérique. La création du plan directeur continental pour la cybersécurité par Smart Africa est remarquable. Toutefois, elle soulève des questions quant au chevauchement et à la distinction entre les initiatives de Smart Africa et celles de l'Union africaine. L'implication de Smart Africa auprès de plusieurs gouvernements africains et son alignement sur des chefs d'État tels que le président du Rwanda est intrigant, surtout si l'on considère que ces efforts pourraient être plus efficacement canalisés par l'Union africaine. » Nnenna Ifeanyi-Ajufo

Selon la Professeure de droit et de technologie, l'émergence de Smart Africa et son influence croissante soulèvent des questions sur le rôle de l'Union africaine dans la promotion de la transformation numérique. Est-ce une question de volonté politique, de financement, de capacité ou de leadership qui a conduit à la montée en puissance de Smart Africa en tant qu'acteur clé des initiatives numériques ? Il est essentiel de se poser ces questions au moment où l'Afrique s'engage sur la voie de la transformation numérique, en cherchant à trouver un équilibre entre les capacités, le leadership et la priorité accordée aux objectifs numériques.

L'avenir de la transformation numérique en Afrique pourrait dépendre de la manière dont les organismes régionaux comme l'Union africaine et les plateformes comme Smart Africa peuvent

collaborer et aligner leurs efforts pour le plus grand bien du paysage numérique du continent. Une initiative panafricaine visant à s'appuyer sur les innovations technologiques pour améliorer la prospérité socio-économique des africains. Néanmoins, « Avec la Cyberstratégie Africaine, on aboutit à la prise en compte des notions telles que la cyberdéfense, la cyber-résilience, la cyber-diplomatie, l'actualisation de nos doctrines militaires et de renseignement, etc. Toutes ces notions sont complètement absentes de la réflexion en cours sur le continent, et ce du fait d'un impensé du cyberespace à partir de notre propre référentiel. **»** DJIMGOU NGAMENI

- Une approche sans frontières est essentielle pour surmonter les méfiances historiques entre États africains. En effet les menaces naissantes en matière de cybersécurité exigent une approche « sans frontières », qui faciliterait la vision séculaire de l'intégration régionale et, par extension, de la stabilité/du développement du continent.
- Une démarche qui permet de considérer le cyberespace dans toute sa complexité et sous toutes ses formes (politique, idéologique, économique, stratégique, etc.), de tenir compte de sa dimension conflictuelle et les affrontements de toutes sortes qui s'y déroulent, de mieux apprécier les cyber-risques et les cybermenaces, etc.

Un projet continental d'une « Afrique sans frontières », est visiblement empreint de suspicion mutuelle, de préjugés et de conflits de « supériorité » injustifiés, entre autres, ce qui entraîne des querelles diplomatiques entre les États africains. L'exploration cybernétique de l'Afrique et les initiatives diplomatiques au niveau (sous-) régional dans le cadre de la « Convention de Malabo » dirigée par l'UA, entre autres, pour relever les défis émergents en matière de cybersécurité et exploiter les potentiels du cyberespace africain, constituent une substance pour la vision continentale séculaire d'une « Afrique unique ». L'Afrique a récemment mis l'accent sur l'ambition de réaliser sa transformation numérique en poursuivant diverses initiatives phares visant à atteindre les objectifs de son **« Agenda 2063 ».**

La transformation numérique sera mieux réalisée grâce à des politiques et mécanismes de cybergouvernance appropriés, et le succès de la Stratégie de transformation numérique de l'Afrique 2020-2030 dépend de divers facteurs. Afin de tirer parti de ses atouts et de remédier à l'absence actuelle d'un cadre de coordination numérique commun, la Commission de l'UA coordonne l'élaboration et la formulation de la Stratégie de transformation numérique pour l'Afrique afin d'orienter un programme commun et coordonné de numérisation, de renforcer les synergies et d'éviter la duplication des efforts.

Cependant, les africains n'ont pas encore pris le temps de réfléchir et d'étudier en profondeur ce que c'est que le cyberespace, en le considérant comme un objet d'étude scientifique.

« Dans les stratégies africaines de cybersécurité, les notions de cyberdéfense, de lutte informatique offensive et défensive ne font pas parties des stratégies mise en place par les organisations

y compris dans la convention de Malabo qui est proposée par l'Union Africaine. » DJIMGOU NGAMENI

Qui des politiques et stratégies politiques en vigueur en Afrique en matière de cybergouvernance, l'interaction de la région avec les processus internationaux de cybergouvernance ? Le véritable défi juridique consiste à déterminer quand et comment les droits et régimes juridiques susmentionnés s'appliquent dans le contexte cybernétique unique, questions que la Russie, la Chine et les autres États récalcitrants ont habilement éludées.

On ne sait pas très bien pourquoi ces États ont adopté une approche régressive sur ces questions spécifiques, mais continuent d'accepter l'applicabilité du droit international de manière plus générale. Peut-être considèrent-ils le processus comme un jeu à somme nulle et veulent-ils éviter de donner l'impression que « l'Occident » a le pouvoir de dicter les règles du jeu dans le cyberespace. Ou peut-être la réponse est-elle juridique et opérationnelle dans le sens où ils veulent priver l'Occident d'une justification légale pour répondre aux opérations cybernétiques hostiles qu'il lance lui-même. Bien que cette privation leur soit également applicable, les États concernés sont moins souvent la cible par d'autres États et les avantages d'opérations cybernétiques illégales menées qui en découlent l'emportent sans doute sur les coûts. Enfin, l'opposition à la reconnaissance de notions juridiques élémentaires et irréfutables peut refléter l'état lamentable actuel des relations en dehors du cyberespace. Il s'agit peut-être de questions juridiques « faciles », mais pour l'instant tout le monde joue « dur ».

Sur le plan réglementaire, l'Afrique se trouve à un moment conséquent. Le traité régional sur la cybersécurité est entré en vigueur le 8 juin 2023. Issue de la déclaration d'Oliver Tambo de 2009, cette convention est ambitieuse, englobant les transactions électroniques, la cybersécurité et la protection des données personnelles dans un seul traité - une approche unique par rapport à d'autres régions.

Cependant, les pays africains se sont montrés réticents à ratifier cette convention, avec seulement 15 ratifications à ce jour, aucune, provenant des principales puissances du continent comme le Nigeria, le Kenya, l'Égypte ou l'Afrique du Sud. Même l'Éthiopie, siège de l'Union africaine (UA), n'a pas encore ratifié le traité. Cela démontre le manque de capacité à mettre en œuvre une réglementation pourtant puissante. Cela représente le fossé entre l'existence de cadres réglementaires et leur mise en œuvre. Au niveau sous-régional, les communautés économiques régionales comme la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) et la Communauté de développement de l'Afrique australe (SADC) ont leurs directives en matière de cybercriminalité, ce qui témoigne d'une approche sous-régionale plus dynamique de la cybersécurité.

Toutefois, l'influence de l'Union africaine sur ces initiatives régionales est limitée. En effet, contrairement à d'autres régions du monde, les communautés économiques régionales sont relativement fortes. En outre, les approches législatives varient d'un pays africain à l'autre, certains se concentrant sur

les délits informatiques, tandis que d'autres ont un champ d'application plus large, comme le montrent la loi sur la cybersécurité 2020 du Ghana et la loi sur la cybercriminalité du Nigéria.

Un aspect clé de l'état actuel de la cybersécurité en Afrique est la tendance à la cyber-militarisation de la cybergouvernance. Cela a contribué à une tendance au cyber-autoritarisme, car de nombreux pays africains considèrent la cybersécurité sous l'angle de la sécurité nationale, ce qui conduit à des pratiques telles que les coupures d'Internet, le blocage de services spécifiques (par exemple, l'interdiction de Twitter par le Nigeria entre 2021 et 2022) en réponse à des crises plutôt que de se concentrer sur les vulnérabilités des citoyens dans le cyberespace. Cette approche contraste avec la stratégie de transformation numérique de l'Union africaine (2020-2030), qui préconise une approche de la cybersécurité davantage axée sur les personnes et les parties prenantes que sur les gouvernements.

Bien loin du pacifique village global rêvé par les utopistes au tout début de l'Internet, le cyberespace est désormais perçu à la fois comme une menace et une ressource dans la plupart des conflits géopolitiques contemporains. Pour les armées de nombreuses nations, il est même devenu un enjeu stratégique majeur et un champ de confrontation à part entière. Cette représentation laisse peu de place à la vulnérabilité, pourtant intrinsèque au cyberespace, et encourage le renforcement des capacités défensives et le développement d'un véritable arsenal offensif et de commandements militaires spécialisés.

Or le cyberespace représente un véritable défi stratégique. Contrairement aux autres domaines militaires que sont la terre, la mer, l'air et l'espace, ce milieu, né de l'interconnexion globale des systèmes d'information et de communication, n'est pas un milieu naturel. Il est entièrement façonné par l'homme et surtout en reconfiguration rapide et permanente.

C'est donc un domaine difficile à appréhender et encore plus à représenter, en raison de sa géographie complexe et changeante, et pour part intangible. On ne sait pas encore très bien ce qu'est un terrain militaire dans le cyberespace, et il n'existe pas vraiment de cartes d'état-major du cyberespace. C'est aussi un milieu dans lequel les paradigmes stratégiques classiques comme la dissuasion, la riposte, l'anticipation ou encore le contrôle des armes ne sont pas directement transposables, en raison de ses spécificités propres.

II. Les normes internationales de cybergouvernance n'ont été que théoriques dans le contexte africain !

Dès 1997, dans un article intitulé « Internet géopolitise le monde », Hérodote annonçait la couleur : « À défaut de temporiser les conflits géopolitiques, l'Internet semble au contraire les multiplier et les compliquer » [Douzet, 1997]. À contrecourant des voix optimistes qui annonçaient ni plus ni moins que

la fin de la géographie, nous pointions déjà les enjeux géopolitiques de l'expansion irrésistible des systèmes d'information et de communication à travers le monde :

Le réseau [Internet] est lui-même l'enjeu de nombreux conflits géopolitiques qui donnent lieu à des stratégies de domination de la part des nations aux intérêts divergents qui cherchent à en contrôler le contenu, le fonctionnement et le développement économique. Il est une arme hautement stratégique pour la sécurité des nations [...] et surtout un instrument extrêmement puissant dans les rivalités de pouvoir entre groupes, minorités, forces politiques, religieuses, économiques, au niveau local comme au niveau mondial.

Le paysage actuel des cybermenaces est de plus en plus influencé par les avancées technologiques et la dynamique géopolitique. Avec les défis en 2024 et les conflits militaires en cours, le cyberespace est devenu un champ de bataille pour le contrôle de l'information, l'espionnage et la perturbation. Les normes internationales de cybergouvernance, souvent théoriques en Afrique, doivent maintenant s'adapter à un paysage de cybermenaces où les avancées technologiques et les tensions géopolitiques transforment le cyberespace en un champ de bataille pour le contrôle de l'information et l'espionnage, les cyberactivités sponsorisées par les États brouillant les frontières entre gouvernance traditionnelle et guerre numérique. La cybersécurité fait désormais partie de l'arsenal des conflits géopolitiques, et les attaques peuvent être sophistiquées et persistantes.

- Les cyberopérations soutenues par les États sont généralement motivées par des événements géopolitiques et des conflits militaires. Ces acteurs sont financés et coordonnés par des entités gouvernementales et sont impliqués dans toute une série d'activités, notamment le cyberespionnage, le sabotage, l'utilisation de logiciels malveillants destructeurs contre des cibles à fort impact et des infrastructures critiques, ainsi que la coordination de campagnes de propagande et de désinformation. Ils bénéficient souvent du soutien de leur gouvernement, ce qui signifie généralement qu'ils n'ont pas à se soucier de l'application de la loi.
- Ayant accès à des ressources « illimitées », ces cyberacteurs favorisent généralement le développement et les progrès en matière de cybersécurité, qui finissent par déborder sur le marché des logiciels malveillants pour être utilisés contre les infrastructures civiles.

Le partage des meilleures pratiques entre les États membres est une étape vers le renforcement réussi de la gestion des crises informatiques. Les cyberactivités sponsorisées par les États se sont intensifiées, les pays tirant parti des cyberopérations pour obtenir des avantages politiques, économiques et militaires, ce qui brouille les frontières entre l'art de gouverner traditionnel et les cyberactivités. Les meilleures pratiques proposées sont regroupées dans les quatre phases du cycle de gestion des cybercrises (prévention, préparation, réponse et rétablissement) et font référence aux problèmes survenant à chaque étape avec une approche tous risques.

L'efficacité des stratégies mises en œuvre par les gouvernements africains pour parvenir à un consensus et prendre des mesures dans le domaine numérique est influencée par une série de facteurs, dont certains sont d'origine humaine, tandis que d'autres sont inhérents aux réalités de la région, comme l'instabilité politique et les conflits. Ces facteurs détournent souvent la priorité des objectifs numériques.

Par exemple, l'Union africaine a subi une cyberattaque importante, mais la réponse n'a pas été claire, ce qui reflète la question primordiale de la priorité accordée aux conflits physiques par rapport aux menaces numériques. L'Union africaine, contrairement à l'UE, n'exerce pas la même influence régionale et est reléguée au statut d'observateur dans les négociations sur la cybercriminalité. Cette limitation empêche l'UA de parler au nom de ses États membres ou de leur demander des comptes sur les questions numériques.

> L'approche individualisée de la gouvernance dans les pays africains, a un impact sur la cybergouvernance. Bien que l'Union africaine ait commencé à rechercher une position africaine unifiée sur la cybersécurité, un simple document d'orientation n'équivaut pas nécessairement à un consensus, comme le montre l'impact limité de la convention de Malabo[1].

- Une autre stratégie pourrait impliquer des pays africains "champions" comme le Maroc, l'Égypte, le Ghana et l'île Maurice, qui montreraient la voie et guideraient les autres.
- La convention de Malabo, désormais en vigueur, pourrait servir de plateforme pour créer une approche harmonisée et modifier certaines parties de la convention afin de mieux répondre aux besoins régionaux.
- L'engagement avec les entités privées est un domaine dans lequel Smart Africa se distingue d'une plateforme régionale qui bénéficie non seulement de l'attention de nombreux pays africains, mais qui collabore également de manière intensive avec des entreprises technologiques et des sociétés de télécommunications.

Cette approche inclusive est cruciale car il n'existe aucune autre plateforme ayant une telle perspective régionale qui implique activement les entreprises privées dans l'élaboration du paysage numérique en Afrique. À Nnenna IFEANYI-AJUFO de marteler :

> La stratégie de transformation numérique de l'Afrique, si elle est mise en œuvre de manière transparente et responsable, pourrait fournir un cadre solide pour l'évolution numérique du continent. Cependant, il y a un manque de clarté concernant sa mise en œuvre et sa pertinence pour les différents pays africains. Garantir la transparence et la responsabilité dans la mise en œuvre de cette stratégie permettrait de mieux définir le paysage de la gouvernance numérique en Afrique.

L'Union Internationale des Télécommunications (UIT) a reconnu la performance du Royaume du Maroc qui a obtenu un score global de 97.5/100. Par rapport à l'édition de 2020, le Maroc a réalisé des avancées notables sur les cinq dimensions de l'étude : juridique, technique, organisationnelle,

[1] Nnenna IFEANYI-AJUFO - L'état actuel de la cybersécurité en Afrique est la tendance à la cyber-militarisation de la cybergouvernance

renforcement des capacités et coopération. Le Maroc a obtenu 20 points en termes de mesures juridiques, organisationnelles et de coopération, puis 19,38 points en mesures liées au renforcement des capacités, et 18,12 points dans l'indice relatif aux mesures techniques. Le rapport met en avant un certain nombre de points forts qui ont permis le Royaume du Maroc de réaliser cette performance et renforcer sa position sur l'échiquier mondial. Il s'agit notamment de l'élaboration d'un cadre juridique complet composé de plusieurs textes législatifs et réglementaires couvrant la cybersécurité, la lutte contre la cybercriminalité, la protection des données à caractère personnel, l'identité numérique et les services de confiance et du lancement récent de la stratégie nationale de cybersécurité à l'horizon 2030.

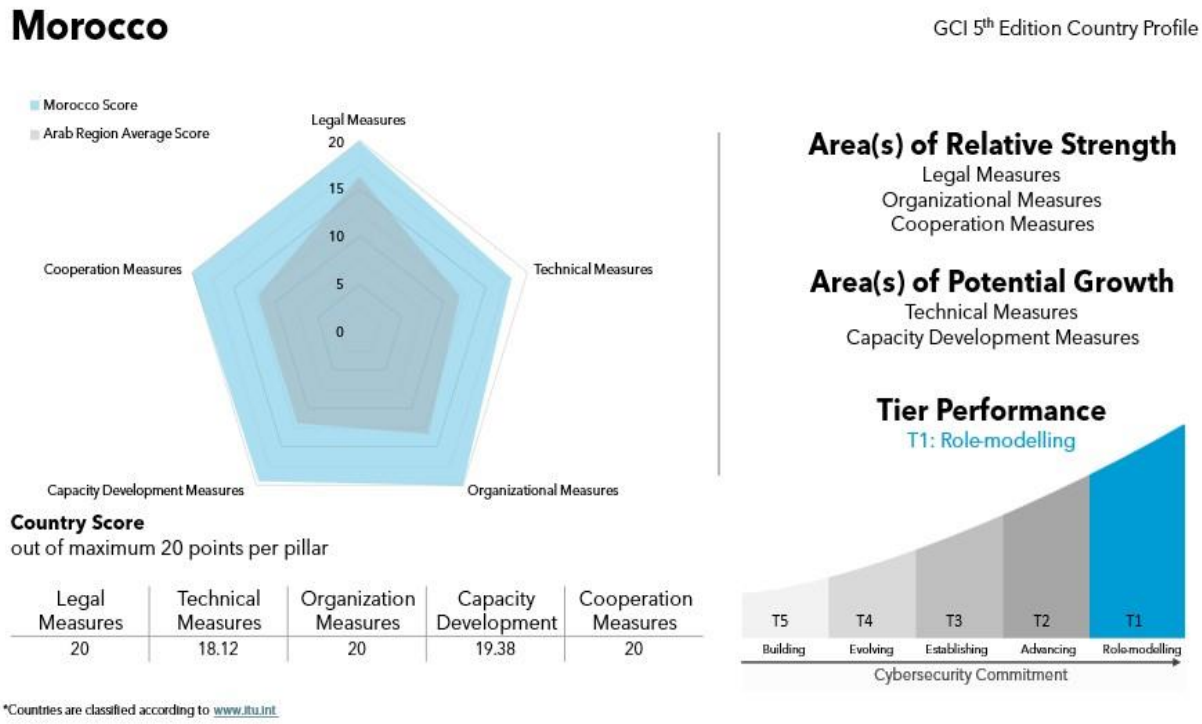


Figure 2[2] : Engagement en faveur de la cybersécurité

Selon l'UIT, les pays de la catégorie la plus élevée ont mis en œuvre des mesures complètes dans divers domaines de la cybersécurité, notamment des cadres juridiques solides, des capacités techniques telles que les équipes d'intervention nationales (groupes chargés de réagir aux violations de la sécurité, aux virus et à d'autres incidents potentiellement catastrophiques dans les entreprises confrontées à des risques de sécurité importants), des structures nationales de cybersécurité, des initiatives de renforcement des capacités et une participation active aux efforts de coopération internationale.

Bien que l'indice GCI (Global Cybersecurity Index) de l'UIT soit un outil précieux, il peut parfois sembler limité face à la complexité des enjeux du cyberespace. Le National Cyber Power Index (NCPI)

[2] Lien de l'étude : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

offre une perspective plus large, en prenant en compte des éléments comme les capacités défensives et offensives, ainsi que l'influence sur les normes globales.

Au cours des deux dernières années, le NCPI a catalysé les conversations et les débats entre les décideurs politiques, les universitaires et l'industrie sur le concept de cyberpuissance et sur la manière dont les États exploitent et peuvent exploiter davantage leurs capacités pour améliorer leur capacité globale à atteindre leurs objectifs nationaux.

> Le cadre fourni par le NCPI permet aux décideurs politiques d'envisager une gamme plus complète de défis et de menaces émanant d'autres acteurs étatiques. L'intégration de modèles qualitatifs et quantitatifs, avec plus de 1 000 sources de données existantes et 29 indicateurs pour mesurer la capacité d'un État, est plus complète que toute autre mesure actuelle de la cyberpuissance.
>
> Éric ROSENBACH

Le cyberespace, est le nouveau champ de bataille dans lequel les États-nations cherchent à se surpasser les uns les autres par le biais de moyens cybernétiques et à accroître leur cyberpuissance. D'ailleurs comme le souligne DJIMGOU NGAMENI [3]:

> D'après notre analyse, il est clair que les États cherchent non seulement à détruire et à désactiver l'infrastructure et les capacités d'un adversaire, mais aussi à renforcer et à améliorer les cyberdéfenses nationales, à recueillir des renseignements dans d'autres États, à accroître les compétences nationales en matière de cybertechnologie et de technologie commerciale, à contrôler et à manipuler l'environnement de l'information et à étendre leur influence en définissant des normes internationales en matière de cybersécurité et de normes techniques. La cyberpuissance doit être considérée dans le contexte des objectifs nationaux d'un État et les États doivent adopter, et adoptent de plus en plus, une approche nationale globale lorsqu'ils tentent de l'exploiter.

III. Cyberespace et géopolitique : Mesure plus ciblée de l'activité cybernétique

L'aphorisme selon lequel « mesurer, c'est savoir » peut s'appliquer au cyberespace. Des recherches objectives en sciences sociales, basées sur des données, peuvent aider à identifier les normes qui fonctionnent déjà et celles qui doivent être diffusées auprès d'autres. Les États et les autres parties prenantes agissent-ils conformément à l'appel de la Commission mondiale visant à protéger le cœur public de l'Internet ? À quelle fréquence les États semblent-ils « mener ou soutenir sciemment » des cyberopérations qui « endommagent » ou « compromettent de toute autre manière l'utilisation » d'infrastructures critiques, contrairement à la norme GGE (*Group of Governmental Experts*) de 2015 qui prétend interdire un tel comportement ?

Le coordinateur adjoint des États-Unis pour les questions liées au cyberespace au Département d'État a résumé avec justesse la situation après l'échec du processus GGE :

> Je suis arrivé à la conclusion regrettable que ceux qui ne veulent pas affirmer l'applicabilité de ces règles et principes juridiques internationaux croient que leurs États sont libres d'agir dans ou via le cyberespace

[3] Dans sa conclusion du NCPI de son article : L'Afrique peut-elle devenir une « cyberpuissance ? »

> pour atteindre leurs objectifs politiques sans aucune limite ni contrainte à leurs actions. C'est une vision dangereuse et indéfendable… Un rapport qui aborde le règlement pacifique des différends et les concepts connexes mais qui omet d'examiner les options légales dont disposent les États pour répondre aux activités cybernétiques malveillantes auxquelles ils sont confrontés ne parviendrait pas seulement à dissuader les États de se livrer à des activités potentiellement déstabilisatrices, mais également à envoyer un message stabilisateur à la communauté plus large des États, à savoir que leurs réponses à de telles activités cybernétiques malveillantes sont limitées par le droit international.

Des efforts de recherche ciblés peuvent répondre à ces questions.

Les États peuvent être plus proactifs dans l'articulation de leurs propres pratiques et de leur compréhension des normes, comme certains ont commencé à le faire. Cependant, en général, ils protègent le secret de leurs cyberopérations et sont particulièrement réticents à révéler leurs capacités offensives. Il est peu probable que cela change. Néanmoins, des efforts existent déjà pour suivre ces activités.

Evaluation des processus normatifs mondiaux en matière de cybersécurité à la croisée des chemins.

Comme le suggère le titre de l'atelier, « Cyberespace et géopolitique », les normes de comportement appropriées dans le cyberespace reflètent souvent les réalités politiques du système international. Plusieurs participants ont exprimé leur scepticisme quant aux progrès qui pourraient être réalisés dans le climat géopolitique actuel.

- Il est nécessaire de calibrer les attentes en matière de normes cybernétiques. Les caractéristiques et complexités nouvelles du cyberespace créent des obstacles importants à l'élaboration de normes efficaces. Le cyberespace lui-même représente une dimension relativement nouvelle de l'activité étatique. Si certains participants ont estimé que le développement des normes progressait lentement, d'autres ont suggéré que les normes cybernétiques émergent plutôt rapidement par rapport au rythme des normes dans d'autres cas historiques.

En l'absence de changements structurels dans le domaine qui modifient le calcul coûts-avantages des activités cybernétiques malveillantes, les normes cybernétiques ne donneront peut-être que des résultats modestes. Dans le même temps, il y a lieu d'être optimiste.

- Comme l'ont souligné certains participants, notamment ceux du secteur industriel, il existe des possibilités d'instanciation de normes dans le code informatique. En d'autres termes, des solutions techniques peuvent exister pour faire progresser l'adoption ou la diffusion de certaines normes cybernétiques.

Cela pourrait également réduire la vulnérabilité de systèmes cruciaux (par exemple, l'infrastructure électorale) en réduisant l'exposition de ces systèmes au cyberespace (par exemple, par le biais de bulletins de vote papier).

- Un troisième groupe de participants a affirmé qu'aucune grande puissance ne changerait son comportement en l'absence d'un choc majeur lié au cyberespace pour le système politique – un « cyber Hiroshima » selon les termes d'un participant. Ce n'est qu'après qu'un tel événement aura clarifié les coûts réels des opérations cybernétiques et (peut-être) suscité la révulsion populaire que les normes cybernétiques pourraient s'imposer parmi les acteurs qui cherchent actuellement à maximiser la flexibilité opérationnelle.

En l'absence de ces développements, il existe un écosystème apparemment fragmenté de processus de normes cybernétiques. Ce n'est cependant pas le pire endroit où se trouver. Le fait d'avoir une pléthore d'efforts multilatéraux, privés, industriels et multipartites crée des opportunités à la fois pour approfondir les engagements normatifs existants et pour élargir leur public cible.

Comme l'a suggéré un participant, le monde **«** est peut-être en train de piloter l'avion alors qu'il est encore en construction », mais il existe des moyens d'avancer : mesurer les normes existantes, qui s'y conforme et les divers processus qui promeuvent et distribuent ces normes, ainsi qu'un catalogue d'incitations pour améliorer leur capacité à avoir des effets réels sur la stabilité et la sécurité du cyberespace.

IV. Vers une Cyberdiplomatie : Construire un Internet Ouvert et Sécure dans un Monde Fragmenté

Les grandes évolutions de la géopolitique numérique : Sommes-nous à l'aube d'une Guerre Froide Numérique ? Antony BLINKEN, lors d'un entretien, met en lumière des enjeux cruciaux de la géopolitique numérique actuelle. La fragmentation d'Internet, sous l'influence de régimes autoritaires comme la Chine et la Russie, soulève des préoccupations profondes pour la préservation d'un Internet global et libre. Des millions d'individus se voient privés de leurs droits fondamentaux, tandis que des voix critiques sont étouffées dans des zones de censure.

L'initiative des États-Unis de promouvoir une « solidarité numérique » semble viser à établir des normes communes et à contrer les dérives autoritaires. Pourtant, cette promesse se heurte à une méfiance croissante envers les États-Unis, alimentée par des scandales de surveillance et de manipulation de données. Comment croire en une coopération authentique lorsque des lois comme la FISA 702 continuent de régir les pratiques de surveillance ? Cela crée un sentiment de colonisation numérique, où les droits des citoyens sont sacrifiés sur l'autel de la sécurité.

Prenons l'exemple de l'affaire *Cambridge Analytica*, qui a secoué le monde entier. Des millions de données personnelles ont été exploitées pour influencer des élections, sapant la confiance dans les processus démocratiques. Cet incident souligne l'urgence de garantir la transparence et la responsabilité

dans l'utilisation des technologies numériques. Les pays européens, qui adoptent des régulations strictes comme le RGPD, hésitent à se ranger derrière une stratégie qui pourrait sembler renforcer l'hégémonie atlantique. **La question demeure** : cette initiative sera-t-elle suffisante pour unir les alliés autour d'un Internet véritablement ouvert et éthique, ou ne fera-t-elle qu'accentuer les divisions existantes ? La réponse pourrait bien façonner le paysage numérique des années à venir.

- La défense d'un Internet « libre et ouvert » est un idéal louable, mais il ne peut se réaliser sans une réévaluation sérieuse des pratiques actuelles. Tant que des lois comme la FISA 702 subsisteront, la promesse d'un Internet ouvert et d'une solidarité numérique entre nations démocratiques restera difficile à croire. Les discours sur un Internet libre risquent d'apparaître comme de vains mots sans actions concrètes.

La question de la cybersécurité et des chaînes d'approvisionnement critiques est également essentielle dans ce contexte. Les récents cyberattaques contre des infrastructures vitales, comme celles touchant le secteur de la santé ou de l'énergie, illustrent à quel point nous devons protéger nos systèmes numériques. Les pays doivent s'assurer qu'ils ne deviennent pas trop dépendants des technologies dominées par un seul acteur. La coopération et la confiance entre alliés, surtout dans des domaines aussi sensibles, doivent se construire sur des bases solides et mutuellement respectueuses. Des initiatives comme le « Digital Markets Act » en Europe montrent que nous pouvons tracer une voie vers une souveraineté numérique.

Il est clair que des réformes structurelles et un dialogue ouvert sont nécessaires pour avancer vers un Internet qui reflète vraiment des valeurs démocratiques, sans arrière-pensées. La route est encore longue, mais chaque échange comme celui-ci est un pas dans la bonne direction. Ensemble, nous pouvons façonner un avenir numérique où chaque voix compte et où la technologie sert à renforcer nos libertés plutôt qu'à les restreindre.

V. La convergence de la technologie avec la géopolitique et les réalités sociales.

Les lacunes en matière de développement des capacités, la nécessité de renforcer les infrastructures techniques et l'importance d'une coopération régionale accrue sont autant de domaines nécessitant une attention immédiate. L'Afrique fait face à un manque de cadres juridiques pour la gestion des données et l'intelligence artificielle (IA), ce qui expose ses données à une exploitation par des puissances étrangères. Et pour assurer sa souveraineté numérique, le continent doit développer des infrastructures locales et des réglementations adaptées tout en équilibrant les partenariats internationaux.

Seulement « 2 % des données africaines sont hébergées sur le continent »

L'essor de la construction de centres de données en Afrique représente une phase de "capitalisme des données", qui reflète la dépendance numérique du continent. Il est crucial d'identifier les véritables bénéficiaires de ces centres de données. L'Afrique se trouve à un carrefour décisif dans son développement numérique et le risque cyber accélère à la vitesse de la transformation digitale avec des enjeux critiques pour développer une IA et une cybersécurité africaines.

- Comment aborder la gestion des données personnelles et de l'IA dans les pays sans cadre juridique robuste, comme certains pays africains, où les enjeux sont principalement d'ordre informationnel, représentant un véritable dilemme en matière de données ?
- L'Afrique se trouve aujourd'hui à un nouveau moment charnière de son histoire. Si le continent ne parvient pas à gérer correctement la transition vers l'IA, le fossé technologique entre l'Afrique et le reste du monde pourrait se creuser (de manière irréversible) ?
- Quid de la gestion des données personnelles et l'utilisation de l'intelligence artificielle (AI) dans les pays qui n'ont pas encore de cadres juridiques robustes [...] ?

Identifier le défi, c'est faire la moitié du chemin vers sa solution. La situation actuelle n'est pas prometteuse ; l'ensemble du continent compte moins de fermes de données que les Pays-Bas, ce qui est un indicateur frappant de la fracture numérique.

Certaines données de l'Afrique sont stockées à l'étranger traditionnellement en Europe et en Amérique du Nord, et de plus en plus en Chine. Et les connaissances sur l'Afrique sont également façonnées en dehors du continent, puisque, par exemple, moins de 2 % des rédacteurs de Wikipédia sont originaires du continent.

Cette pratique soulève d'importantes questions en matière de sécurité et de respect de la vie privée et limite la capacité de l'Afrique à exploiter ses données à des fins de croissance économique et d'innovation. Le continent doit agir de toute urgence pour sauvegarder et promouvoir ses données, ses connaissances et sa sagesse à l'ère de l'IA, dans le cadre du patrimoine commun de la culture et de la connaissance. Le système d'IA moderne doit refléter la sagesse africaine accumulée au fil des siècles.

La sagesse africaine, profondément ancrée dans les traditions orales et les pratiques culturelles, risque d'être négligée à l'ère de l'IA. Les systèmes d'IA, principalement développés en Occident, ne reflètent souvent pas les cultures et les valeurs africaines. Cet oubli peut conduire à des applications d'IA biaisées et culturellement insensibles, ce qui marginalise encore davantage le continent africain. Le fossé de la connaissance numérique est un autre problème critique. « Les bons sentiments ne font pas une politique de puissance et l'IA est la source de tous les pouvoirs au xxi* siècle. » Dr Laurent Alexandre - *La Guerre Des Intelligences*

Nous alimentons la machine numérique de demain, sans en avoir conscience. Nous pensons que le smartphone est le degré ultime de la supériorité technologique de l'Homme, sans comprendre qu'il est en réalité l'outil de sa transformation radicale voire de sa vassalisation.

La matière première de l'IA, c'est l'information ! D'où vient-elle ? De nous-mêmes, qui faisons des milliards de recherches Google ou déposons près de 10 milliards d'images sur Facebook, etc. Pour le Deep Learning, l'avalanche d'images et de données qui déferle sur le Web constitue une matière première quasi infinie et qui se renouvelle chaque jour. Ce sont leurs milliards de clients ou de visiteurs qui donnent aux géants du numérique leur supériorité écrasante. Sans le savoir, nous fournissons gratuitement à la machine des informations qui vont l'alimenter et lui donner les moyens de sa surpuissance.

> « Nous traversons une période charnière des relations internationales, caractérisée par une concurrence acharnée entre les nations et par des défis mondiaux communs tels que le changement climatique, la sécurité alimentaire et sanitaire et la croissance économique inclusive. La technologie jouera un rôle de plus en plus crucial pour relever ces défis… » **Le secrétaire d'État américain**, Antony J. BLINKEN

L'Afrique a un potentiel immense pour devenir un acteur clé dans le cyberespace, à condition de saisir cette opportunité avec détermination et vision. La feuille de route pour une Cyberstratégie proposerait :

I. Un audit national pour cartographier les initiatives de cybersécurité existantes et d'engager les parties prenantes à travers des forums pour favoriser le dialogue et la collaboration.
II. Ensuite, le développement de cadres législatifs harmonisés, l'investissement dans les infrastructures critiques et le renforcement des capacités offensives et défensives en cybersécurité par l'éducation pour former une main-d'œuvre qualifiée, capable de répondre aux défis du numérique.
III. Enfin, elle appelle à établir un cadre de gouvernance solide, avec des mécanismes de surveillance pour mesurer les progrès et promouvoir une culture de cybersécurité à travers des campagnes de sensibilisation.

Conclusion

L'élaboration d'une Cyberstratégie intégrée est essentielle pour naviguer dans un paysage numérique en constante évolution. Face aux défis de cybersécurité, à la fragmentation géopolitique et à la nécessité de préserver la souveraineté numérique, les dirigeants africains doivent démontrer un engagement ferme et coordonné. Cela nécessite non seulement des politiques adaptées qui répondent aux spécificités du continent, mais aussi un investissement significatif dans les infrastructures locales, l'éducation et la formation des talents. La collaboration entre États africains, ainsi qu'avec des partenaires internationaux, est primordiale pour créer un cadre de gouvernance robuste. De plus, l'intégration des principes de cyberdéfense, de cyber-résilience et de cyberdiplomatie dans les stratégies nationales renforcera la position de l'Afrique sur la scène mondiale. En abordant ces enjeux de manière proactive, le continent peut transformer les défis en opportunités, assurant ainsi une transformation numérique efficace et inclusive, et favorisant un avenir où chaque voix compte dans le cyberespace. Le chemin sera semé d'embûches, mais une approche progressive, collaborative et adaptée aux contextes locaux peut aider à surmonter les obstacles. L'avenir numérique de l'Afrique se construit sur la détermination, l'unité et l'innovation, transformant chaque défi en une opportunité pour bâtir un cyberespace inclusif et prospère. Ce n'est pas nécessairement impossible, mais c'est indéniablement complexe. L'avenir appartient à ceux qui croient en la beauté de leurs rêves... et qui ont assez de courage pour affronter les montagnes de paperasse qui les séparent de leur réalisation. Bonne chance à nous dans ce grand voyage numérique !

Afrique un jour, Afrique toujours [...] se relèvera ?

Références

Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation : Nnenna Ifeanyi-Ajufo : Pages 146-159 | Published online: 19 May 2023 https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2199960#abstract

Eric Rosenbach, codirecteur du Belfer Center et ancien chef d'état-major et secrétaire adjoint du ministère américain de la Défense (2022) https://www.belfercenter.org/publication/national-cyber-power-index-2022

Global Cybersecurity Index : https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Extrait du livre à paraître « Cyberstratégie Africaine, Tome 1 », du même auteur. Par DJIMGOU NGAMENI : Avril 2021 La-strategie-Africaine-de-transformation-numerique.pdf

Geopolitics Accelerates Need For Stronger Cyber Crisis Management : February 28, 2024 https://www.enisa.europa.eu/news/geopolitics-accelerates-need-for-stronger-cyber-crisis-management

Journal of African Foreign Affairs: Vol. 9, No. 3 (December 2022), pp. 57-81 (25 pages): Published By: Adonis & Abbey Publishers Ltd https://www.jstor.org/stable/27196111

Leçons d'Afrique en matière de cyber-stratégie: Par Abdul-Hakeem AJIJOLA et Nate D.F. Allen - 18 mars 2022 https://africacenter.org/fr/spotlight/lecons-dafrique-en-matiere-de-cyber-strategie/

The Imperative of Cyber Diplomacy and Cybersecurity in Africa: Oladotun E. AWOSUSI

La géopolitique pour comprendre le cyberespace - 2014 - Par Frédérick DOUZET https://shs.cairn.info/revue-herodote-2014-1-page-3?lang=fr
https://www.ifri.org/sites/default/files/atoms/files/etude_pannier_politiques-technologiques_2023.pdf

Frederick DOUZET : Les conflits dans le monde (Juillet 2016) : Chapitre 21. Le cyberespace, un champ d'affrontement géopolitique - Pages 327 à 343 https://shs.cairn.info/les-conflits-dans-le-monde--9782200611613-page-327?lang=fr

La souveraineté numérique : dix ans de débats, et après : Annales des Mines : N23 – Septembre 2023 https://www.annales.org/enjeux-numeriques/2023/en-23-09-23.pdf

STRATÉGIE DE TRANSFORMATION NUMÉRIQUE POUR L'AFRIQUE 2020-2030 https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_French.pdf
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

https://www.linkedin.com/posts/djimgou-ngameni-a7894322_expertcybersecurity-expert-strategie-activity-7234881999138672642-

https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-acrossroads?lang=en

Smith, B. (2017). 'The Need for a Digital Geneva Convention. https://blogs.microsoft.com/onthe-issues/2017/02/14/need-digital-genevaconvention/

https://www.atalayar.com/fr/articulo/nouvelles-technologies-innovation/maroc-parmi-leaders-mondiaux-cybersecurite-selon-lunioninternationale-des-telecommunications/20240919165121205323.html

À propos de l'Auteur :

Bara FALL est Consultant Architect & Cybersécurité et Co-Founder de ABC Cyber Community. Conférencier, il milite à travers ses prises de position et productions pour une culture #Cyberpourtous.

À propos du LARC :

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

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

Pour citer cet article :

Bara FALL, « Inscrire la cyberstratégie au cœur des priorités des Etats africains », Note N° 13 - LARC, Novembre 2024.