Dossier

L'autonomie stratégique africaine : fondements, obstacles et voies d'émancipation

REVUE AFRICAINE DE
Stratégie & Défense

ISSN en cours
www.stradef.fr

ISSN en cours

REVUE AFRICAINE DE

Stratégie & Défense

La **Revue Africaine de Stratégie & Défense** est une revue scientifique trimestrielle, francophone, à comité de lecture, consacrée à l'autonomie de défense des États africains dans ses dimensions politique, diplomatique, industrielle, doctrinale et opérationnelle.

COMITÉ ÉDITORIAL

Directeur de publication et édition

Ltn./Dr Protais Mbala Ndi
France
www.sidef.fr

Cyberdéfense et souveraineté numérique :

l'Afrique face au défi de l'autonomie technologique

Amadou, Faye Diallo
Chercheur en cybersécurité et relations internationales

Résumé.
L'expansion numérique du continent africain, aussi rapide que structurellement vulnérable, pose avec acuité la question de la cyberdéfense comme composante de la souveraineté. Cet article analyse les dépendances infrastructurelles de l'Afrique dans le cyberespace, cartographie les menaces étatiques et criminelles qui pèsent sur ses systèmes d'information, et évalue les réponses institutionnelles – de la Convention de Malabo aux stratégies nationales. Il propose un cadre conceptuel et opérationnel pour une cyberdéfense africaine autonome, articulée autour de la souveraineté des données, de la formation de cybercombattants et du développement d'infrastructures numériques endogènes.

Abstract.
Africa's rapid yet structurally vulnerable digital expansion raises acute questions about cyberdefence as a component of sovereignty. This article analyses Africa's infrastructural dependencies in cyberspace, maps state-sponsored and criminal threats targeting its information systems, and assesses institutional responses – from the Malabo Convention to national strategies. It proposes a conceptual and operational framework for autonomous African cyberdefence, built on data sovereignty, cyberfighter training, and the development of endogenous digital infrastructure.

Mots clés.
cyberdéfense ; souveraineté numérique ; cyberespace africain ; autonomie stratégique ; infrastructures numériques

Keywords.
cyberdefence; digital sovereignty; African cyberspace; strategic autonomy; digital infrastructure

Note bibliographique :

Amadou, Faye Diallo est chercheur indépendant. Spécialiste en cybersécurité et relations internationales.

Le cyberespace est devenu, au XXIe siècle, un domaine de conflictualité à part entière. Espace de projection de puissance, vecteur d'influence et terrain d'affrontement asymétrique, il constitue désormais la cinquième dimension de la conflictualité stratégique, après la terre, la mer, l'air et l'espace extra-atmosphérique (Ventre, 2011). Pour le continent africain, dont la transformation numérique s'accélère à un rythme sans precedent – avec plus de 570 millions d'utilisateurs d'Internet en 2023 selon l'Union internationale des télécommunications –, cette réalité revêt une urgence particulière. L'Afrique se connecte massivement, mais dans des conditions de dépendance structurelle qui interrogent sa capacité à exercer une souveraineté effective sur son propre espace numérique.

La problématique de la cyberdéfense africaine ne saurait se réduire à une simple transposition des modèles occidentaux. Elle s'inscrit dans une trajectoire historique spécifique, marquée par l'extraversion économique, la dépendance technologique et l'asymétrie des rapports de force dans l'ordre international (Bayart, 1999). Comme le souligne Kempf (2012), « la cyberstratégie ne peut se penser indépendamment de la géopolitique qui la sous-tend ». Pour l'Afrique, penser la cyberdéfense implique donc de penser simultanément l'autonomie technologique, la souveraineté des données et la capacité à produire, et non seulement à consommer, les outils numériques qui structurent désormais la puissance.

Cet article s'inscrit dans une perspective d'africano-centrisme méthodologique qui refuse tant la victimologie que l'afro-optimisme béat. Il vise à poser les termes d'une analyse rigoureuse des conditions de possibilité d'une cyberdéfense africaine souveraine. Comment les États africains peuvent-ils construire une autonomie stratégique dans le cyberespace alors que leurs infrastructures numériques demeurent largement contrôlées par des acteurs extracontinentaux ? Quelles sont les menaces spécifiques qui pèsent sur le cyberespace africain ? Les réponses institutionnelles existantes sont-elles à la hauteur des enjeux ? Quelles conditions – doctrinales, capacitaires, industrielles – doivent être réunies pour qu'émerge une véritable cyberdéfense continentale ?

Pour répondre à ces interrogations, notre démonstration procédera en quatre temps. Nous caractériserons d'abord les dynamiques d'expansion et les vulnérabilités structurelles du cyberespace africain (1). Nous cartographierons ensuite les menaces et les formes de conflictualité qui s'y déploient (2). Nous évaluerons les réponses institutionnelles existantes et leurs limites (3). Enfin, nous proposerons les jalons conceptuels et opérationnels d'une cyberdéfense souveraine (4).

1. Le cyberespace africain : expansion numérique et vulnérabilités structurelles

Le continent africain connaît une transformation numérique d'une ampleur et d'une rapidité remarquables. Toutefois, cette dynamique d'expansion s'accompagne de fragilités structurelles qui, loin de se résorber, tendent à se reproduire sous des formes renouvelées. Comprendre le cyberespace africain exige de saisir simultanément sa vitalité et ses contradictions.

1.1. Une connectivité en croissance exponentielle

L'Afrique est, depuis une décennie, le continent où la progression de la connectivité numérique est la plus rapide au monde. Selon les données de l'Union internationale des télécommunications (UIT, 2023), le taux de pénétration d'Internet sur le continent est passé de 9,6 % en 2012 à près de 40 % en 2023, avec des disparités considérables entre l'Afrique du Nord (plus de 65 %) et l'Afrique subsaharienne (environ 33 %). Le nombre d'abonnements mobiles-cellulaires dépasse le milliard, et la téléphonie mobile constitue le principal vecteur d'accès au réseau pour la grande majorité des populations africaines (GSMA, 2023).

Cette expansion s'appuie sur des dynamiques endogènes puissantes : urbanisation accélérée, jeunesse démographique, essor des services financiers mobiles (mobile money), développement du commerce électronique et numérisation progressive des administrations publiques. Le Kenya, avec M-Pesa, et le Sénégal, avec sa stratégie « Sénégal numérique 2025 », illustrent la capacité d'innovation africaine dans l'économie numérique. Le Rwanda, devenu un hub technologique continental, ambitionne de se positionner comme le « Singapour de l'Afrique » grâce à des investissements massifs dans les TIC.

Cependant, cette croissance quantitative ne doit pas masquer une réalité qualitative plus préoccupante. Comme le note Douzet (2014), « le cyberespace n'est pas un espace homogène : il est structuré par des rapports de pouvoir qui reproduisent, et parfois amplifient, les asymétries du monde physique ». En Afrique, la connectivité croissante ne s'accompagne pas d'une maîtrise proportionnelle des infrastructures, des protocoles et des données qui circulent sur le réseau. L'expansion numérique africaine est, pour une large part, une expansion sous dépendance.

La fracture numérique demeure par ailleurs considérable, non seulement entre l'Afrique et le reste du monde, mais au sein même du continent. Les zones rurales, qui concentrent encore plus de 55 % de la population africaine, restent largement exclues de la connectivité haut débit. Cette fracture n'est pas seulement économique : elle est stratégique, car elle crée des angles morts dans la surveillance et la défense du cyberespace national (Chéneau-Loquay, 2012).

1.2. Dépendances infrastructurelles et extraversion numérique

L'architecture physique du cyberespace africain révèle une extraversion structurelle qui constitue le premier défi de toute politique de cyberdéfense continentale. Cette extraversion se manifeste à trois niveaux : les infrastructures de connectivité, les infrastructures de stockage et les couches logicielles.

Au niveau des infrastructures de connectivité, le continent africain dépend massivement des câbles sous-marins à fibre optique pour son accès à l'Internet mondial. Plus de 95 % du trafic international africain transite par ces câbles, dont la quasi-totalité est détenue par des consortiums internationaux dominés par des entreprises extra-africaines : Alcatel Submarine Networks (France), SubCom (États-Unis), NEC (Japon), et plus récemment Google, Meta et Microsoft. Le projet « 2Africa » de Meta, qui déploie un câble de 45 000 km autour du continent, illustre cette logique d'investissement exogène

qui, si elle améliore la bande passante disponible, renforce simultanément la dépendance envers des acteurs privés étrangers (Blanc, 2019).

Les points d'atterrissement de ces cables – Djibouti, Mombasa, Dakar, Lagos, Le Cap – constituent des nœuds stratégiques dont la protection relève directement de la sécurité nationale. Or, comme le souligne un rapport de l'Union africaine (UA, 2022), « la plupart des États africains ne disposent pas de doctrine de protection des infrastructures critiques numériques, ni des moyens de surveillance nécessaires pour détecter les interceptions sur les câbles sous-marins ».

Au niveau du stockage des données, la situation est plus préoccupante encore. Selon les estimations de Xalam Analytics (2022), moins de 2 % de la capacité mondiale de datacenters est localisée en Afrique, et une proportion considérable des données générées sur le continent est stockée sur des serveurs situés en Europe ou en Amérique du Nord. Cette situation n'est pas seulement un enjeu commercial : elle constitue une vulnérabilité stratégique majeure, dans la mesure où les données des États, des entreprises et des citoyens africains sont soumises à des juridictions étrangères et potentiellement accessibles aux services de renseignement de puissances tierces (Berthier, 2018).

La couche logicielle reproduit cette même logique d'extraversion. Les systèmes d'exploitation, les applications cloud, les réseaux sociaux et les outils de communication utilisés massivement en Afrique sont conçus, détenus et contrôlés par des entreprises américaines (Google, Microsoft, Apple, Meta, Amazon) ou chinoises (Huawei, Alibaba, TikTok). EN effet, la dépendance logicielle est peut-être la forme la plus insidieuse de la dépendance numérique, car elle est invisible et omniprésente. Les États africains n'ont aucune visibilité sur les codes sources, les portes dérobées potentielles et les mécanismes de collecte de données intégrés à ces outils.

Cette triple dépendance – connectivité, stockage, logiciel – configure ce que nous proposons d'appeler une « extraversion numérique systémique », par analogie avec le concept d'extraversion développé par Bayart (1999) pour caractériser les économies politiques africaines. Dans le cyberespace comme dans l'économie, l'Afrique produit des données brutes (matière première numérique) qui sont traitées, valorisées et contrôlées ailleurs, avant de revenir sous forme de services dont le continent est consommateur captif. Cette structure reproduit, dans l'espace numérique, les mécanismes de l'échange inégal décrits par les théoriciens de la dépendance (Amin, 1973).

2. Menaces et conflictualité dans le cyberespace africain

Le cyberespace africain n'est pas seulement un espace de vulnérabilité passive : il est devenu un terrain d'affrontement actif où se déploient des menaces multiformes. L'espionnage étatique, la cybercriminalité organisée et les attaques contre les infrastructures critiques dessinent un paysage de menaces d'autant plus redoutable que les capacités de défense sont limitées.

2.1. Espionnage, ingérence et géopolitique des données

L'Afrique est devenue un espace de compétition géopolitique majeur dans le cyberespace, où les grandes puissances – et certaines puissances regionals – déploient des capacités offensives pour collecter du renseignement, influencer les processus politiques et sécuriser leurs intérêts stratégiques. Le continent, longtemps perçu comme un théâtre secondaire de la conflictualité cyber, est désormais pleinement intégré aux logiques de confrontation numérique globale (Desforges et Douzet, 2018).

L'affaire du siège de l'Union africaine à Addis-Abeba constitue un cas d'école. En janvier 2018, le quotidien français Le Monde révélait que les serveurs informatiques du bâtiment de l'UA – construit et offert par la Chine en 2012 – avaient été configurés pour transférer, chaque nuit entre minuit et deux heures du matin, l'intégralité de leurs données vers des serveurs situés à Shanghai (Tilouine et Kadiri, 2018). Si la Chine a démenti ces accusations, l'affaire a mis en lumière la vulnérabilité des institutions continentales face à l'espionnage numérique et la naïveté stratégique consistant à accepter des « cadeaux » technologiques sans en maîtriser l'architecture.

Cette affaire n'est pas isolée. Les révélations d'Edward Snowden en 2013 avaient déjà montré l'ampleur de la surveillance exercée par la National Security Agency (NSA) américaine sur le continent africain, notamment sur les communications des dirigeants et les câbles sous-marins (Greenwald, 2014). Les programmes MUSCULAR et TEMPORA, conduits respectivement par la NSA et le Government Communications Headquarters (GCHQ) britannique, interceptent systématiquement les données transitant par les points de connexion internationaux, dont plusieurs desservent directement le continent africain.

La France n'est pas en reste. Les capacités de la Direction générale de la sécurité extérieure (DGSE) en matière d'interception de communications numériques dans l'espace francophone africain sont documentées, même si elles demeurent largement classifiées (Follorou et Johannès, 2013). La Russie, à travers les activités du groupe Fancy Bear (APT28) et de l'Internet Research Agency, a par ailleurs été impliquée dans des opérations d'influence numérique ciblant des processus électoraux en Afrique, notamment à Madagascar en 2018 et en République centrafricaine (Dossier Centre, 2019).

Au-delà de l'espionnage classique, la géopolitique des données constitue un enjeu de souveraineté de premier ordre. Les données des citoyens, des entreprises et des administrations africaines, hébergées massivement hors du continent, sont soumises à des législations extraterritoriales – notamment le Cloud Act américain de 2018 – qui permettent aux autorités américaines d'exiger l'accès à des données stockées par des entreprises américaines, quel que soit le lieu géographique des serveurs (Berthier, 2018). Comme le souligne Ventre (2011), « la maîtrise des données est devenue l'équivalent numérique du contrôle territorial : qui détient les données détient le pouvoir ».

L'utilisation massive de logiciels espions commerciaux contre des cibles africaines constitue une menace supplémentaire. Le projet Pegasus, développé par l'entreprise israélienne NSO Group, a été utilisé pour surveiller des journalistes, des opposants et des dirigeants dans plus d'une dizaine de pays africains, dont le Maroc, le Rwanda, le Togo et l'Algérie (Forbidden Stories, 2021). Ces outils, initialement destinés à la lutte antiterroriste,

sont détournés à des fins de répression politique, brouillant la frontière entre sécurité nationale et surveillance autoritaire.

2.2. Cybercriminalité et fragilité des systèmes étatiques

La cybercriminalité constitue la menace la plus immédiatement visible et la plus coûteuse pour les économies africaines. Selon le rapport d'Interpol sur les cybermenaces en Afrique (Interpol, 2022), le continent a subi des pertes estimées à plus de 4 milliards de dollars en 2021 du fait de la cybercriminalité, un chiffre probablement sous-estimé compte tenu de la sous-déclaration des incidents. Les arnaques en ligne, le phishing, les rançongiciels (ransomware) et la compromission de messageries professionnelles (Business Email Compromise – BEC) constituent les vecteurs d'attaque les plus fréquents.

Le phénomène des « brouteurs » en Afrique de l'Ouest – terme familier désignant les escrocs en ligne, principalement actifs en Côte d'Ivoire, au Nigeria et au Ghana – illustre la dimension sociale de la cybercriminalité africaine. Si ces escroqueries sont souvent présentées sous un angle folklorique, elles participent d'un écosystème criminel plus sophistiqué qui mine la confiance dans l'économie numérique et ternit l'image du continent (Bogui, 2010). Toutefois, réduire la cybercriminalité africaine aux « brouteurs » serait une erreur analytique : le continent est également victime de groupes criminels transnationaux, souvent basés hors d'Afrique, qui ciblent les systèmes bancaires, les administrations publiques et les infrastructures critiques africaines.

Les attaques par rançongiciel contre des institutions publiques africaines se multiplient. En 2021, les systèmes informatiques de la Banque d'Ouganda ont été ciblés par le groupe Strontium. En 2022, le port de Durban (Afrique du Sud) a subi une cyberattaque qui a perturbé les opérations logistiques pendant plusieurs jours, avec des répercussions sur l'ensemble de la chaîne d'approvisionnement régionale. Au Sénégal, des attaques contre les systèmes d'information de ministères ont été signalées en 2023, sans que les autorités ne communiquent sur l'étendue des dommages (ANSSI-SN, 2023).

La fragilité des systèmes d'information étatiques africains est aggravée par plusieurs facteurs : obsolescence des équipements, absence de politiques de mise à jour systématique, insuffisance des ressources humaines qualifiées en cybersécurité, et manque de culture de la sécurité numérique au sein des administrations. Selon l'UIT (2022), seuls 17 pays africains sur 54 disposent d'un centre opérationnel de réponse aux incidents informatiques (CERT ou CSIRT) véritablement opérationnel. Cette carence capacitaire signifie que la majorité des États africains sont dans l'incapacité de détecter les intrusions dans leurs réseaux, et a fortiori d'y répondre de manière coordonnée.

Les infrastructures critiques – réseaux électriques, systèmes de distribution d'eau, transports, télécommunications – sont particulièrement exposées du fait de leur numérisation croissante sans sécurisation proportionnée. L'attaque contre le réseau électrique ukrainien en 2015, attribuée au groupe russe Sandworm, a démontré la possibilité de paralyser un pays par des moyens cyber (Greenberg, 2019). Le risque d'une attaque similaire contre des réseaux africains, structurellement moins résilients, est réel et croissant. Comme le souligne Kempf, « la numérisation sans cybersécurité n'est pas un progrès : c'est la création d'une vulnérabilité ».

3. Les réponses institutionnelles : entre ambition normative et déficit capacitaire

Face à l'ampleur des menaces et des vulnérabilités, les États africains et les organisations régionales ont progressivement élaboré des cadres normatifs et institutionnels dédiés à la cybersécurité. Toutefois, l'écart entre l'ambition affichée et les capacités réellement déployées demeure considérable, témoignant d'un déficit d'opérationnalisation qui fragilise la posture de défense continentale.

3.1. La Convention de Malabo et les cadres régionaux

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée le 27 juin 2014 à Malabo, constitue la première tentative de doter le continent d'un cadre juridique harmonisé en matière de cybersécurité. Ce texte, ambitieux dans ses objectifs, couvre trois domaines principaux : les transactions électroniques, la protection des données personnelles et la cybersécurité-cybercriminalité (UA, 2014). Il impose aux États parties l'obligation de définir une politique nationale de cybersécurité, de créer des autorités nationales compétentes et de mettre en place des mécanismes de coopération internationale.

Toutefois, la Convention de Malabo souffre de faiblesses structurelles qui limitent considérablement sa portée opérationnelle. En premier lieu, son processus de ratification est extrêmement lent : près de dix ans après son adoption, seuls 15 États sur les 55 membres de l'UA l'avaient ratifiée en 2024, seuil qui a finalement permis son entrée en vigueur formelle en juin 2023 (UA, 2023). Ce retard traduit le faible niveau de priorité accordé par les gouvernements africains aux enjeux de cybersécurité dans leurs agendas politiques, malgré la rhétorique officielle.

En second lieu, la Convention demeure un texte de principes qui ne prescrit pas de normes techniques contraignantes ni de mécanismes de vérification du respect des engagements. Comme l'observe Orji (2018), « la Convention de Malabo relève davantage du soft law que du hard law, car elle ne prévoit aucun mécanisme de sanction en cas de non-conformité ». L'absence d'organe continental de supervision – équivalent africain de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) – prive le cadre normatif d'un bras opérationnel.

Au niveau sous-régional, des initiatives complémentaires ont vu le jour. La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a adopté dès 2011 une directive sur la cybercriminalité et des actes additionnels sur la protection des données et les transactions électroniques. La Communauté de développement de l'Afrique australe (SADC) dispose d'un modèle de loi sur la cybercriminalité. L'Afrique de l'Est, à travers la Communauté d'Afrique de l'Est (CAE), a engagé des travaux d'harmonisation législative (Kshetri, 2019 : 67). Cependant, ces cadres régionaux souffrent des mêmes limites que la Convention continentale : faible mise en œuvre, capacités limitées et fragmentation des approches.

Le « Programme de référence pour la cybersécurité en Afrique » élaboré par la Commission de l'UA en partenariat avec l'UIT et Symantec en 2018, puis actualisé dans le cadre de l'Agenda 2063, témoigne d'une prise de conscience croissante au niveau

continental. Il propose un cadre stratégique articulé autour de cinq piliers : gouvernance, coopération, protection des infrastructures critiques, renforcement des capacités et développement industriel (UA-UIT, 2018 : 23). Mais là encore, le passage de la stratégie à l'opérationnel reste le maillon faible.

3.2. Les stratégies nationales : avancées et limites

À l'échelle nationale, une poignée d'États africains ont développé des stratégies de cybersécurité relativement abouties, tandis que la majorité du continent accuse un retard considérable. L'indice mondial de cybersécurité de l'UIT (Global Cybersecurity Index – GCI) permet de mesurer ces disparités : en 2022, seuls cinq pays africains figuraient dans la catégorie « haute performance » (score supérieur à 80/100), tandis que plus de trente se situaient en dessous du score de 30/100 (UIT, 2022).

Le Rwanda se distingue comme leader continental en matière de cybersécurité institutionnelle. Doté d'une stratégie nationale de cybersécurité depuis 2015, d'un CERT opérationnel (RW-CSIRT) et d'une législation dédiée, le pays a atteint le 5e rang africain dans le GCI 2022. Le Centre national de cybersécurité rwandais (NCSC) coordonne la politique nationale et dispose de capacités de veille et de réponse aux incidents reconnues. Le Rwanda a également investi dans la formation, avec la création d'un centre d'excellence en cybersécurité à Kigali.

Le Maroc constitue un autre cas avancé. L'Agence nationale de la sécurité des systèmes d'information (DGSSI), créée en 2011 et rattachée à l'Administration de la défense nationale, pilote la stratégie nationale de cybersécurité. Le maCERT (Moroccan Computer Emergency Response Team) assure la veille et la réponse aux incidents. Le Maroc a en outre développé des capacités de formation significatives à travers l'INPT (Institut national des postes et télécommunications) et l'Université Mohammed V, qui proposent des cursus spécialisés en cybersécurité (Yaacobi 2023). La stratégie marocaine « Maroc Digital 2025 » intègre explicitement la cybersécurité comme composante de la souveraineté numérique.

Le Sénégal a progressé significativement avec l'adoption de sa Stratégie nationale de cybersécurité (SNC 2022) et la création de l'ANSSI-SN (Agence nationale de la sécurité des systèmes d'information du Sénégal) en 2023. Le pays dispose d'un CERT (SN-CERT) et a engagé des partenariats avec l'ANSSI française pour le renforcement des capacités. Toutefois, les moyens alloués restent insuffisants au regard de l'ampleur des menaces (ANSSI-SN, 2023). Le Nigeria, première économie du continent, a adopté une stratégie nationale de cybersécurité en 2021 et créé l'Agence nationale de développement des technologies de l'information (NITDA), mais la coordination interinstitutionnelle demeure un défi.

Au-delà de ces quelques cas avancés, la grande majorité des États africains se caractérise par l'absence ou l'insuffisance des dispositifs institutionnels de cybersécurité. Selon l'UIT (2022), 28 pays africains ne disposaient toujours pas de législation spécifique sur la cybercriminalité en 2022, et 33 n'avaient pas de stratégie nationale formalisée. Les causes de ce retard sont multiples : concurrence des priorités (sécurité alimentaire, santé, éducation), faiblesse des moyens budgétaires, déficit de compétences techniques au sein

des administrations, et parfois réticence politique à encadrer un espace numérique perçu comme un outil de contrôle social plutôt que comme un objet de protection.

Un constat transversal s'impose : même dans les pays les plus avancés, les stratégies nationales de cybersécurité sont principalement défensives et orientées vers la lutte contre la cybercriminalité. La dimension proprement militaire de la cyberdéfense – capacités de renseignement d'origine cyber (ROCEM), capacités offensives, doctrine d'emploi – demeure largement absente des cadres institutionnels publiquement connus. Cette lacune est révélatrice : les États africains peinent encore à penser la cyberdéfense comme une composante de leur appareil de défense nationale, au même titre que les forces terrestres, navales ou aériennes.

4. Vers une cyberdéfense souveraine : conditions et perspectives

La construction d'une cyberdéfense africaine souveraine ne relève pas de l'utopie, mais d'un volontarisme stratégique informé par une analyse lucide des contraintes et des possibilités. Elle suppose de réunir simultanément des conditions infrastructurelles, doctrinales et humaines qui, si elles ne sont pas encore pleinement réalisées, font l'objet d'initiatives prometteuses qu'il convient d'amplifier et de coordonner.

4.1. Souveraineté des données et infrastructures numériques endogènes

La première condition d'une cyberdéfense souveraine est la maîtrise physique et juridique des données nationales. Tant que les informations stratégiques des États africains – données militaires, diplomatiques, économiques, de santé publique – seront stockées sur des serveurs situés hors du continent et soumises à des juridictions étrangères, toute prétention à la souveraineté numérique restera illusoire. La souveraineté des données exige un programme continental de développement d'infrastructures numériques endogènes, articulé autour de trois axes : datacenters souverains, points d'échange Internet (IXP) et réseau continental de fibre optique.

La construction de datacenters souverains – c'est-à-dire détenus par des capitaux africains, situés sur le territoire national et soumis exclusivement à la juridiction locale – constitue une priorité absolue. Des initiatives existent déjà : le datacenter de Diamniadio au Sénégal, inauguré en 2021, les investissements du groupe Liquid Intelligent Technologies en Afrique australe et de l'Est, ou encore les projets de datacenters gouvernementaux au Rwanda et au Ghana (Africa Data Centres, 2023). Cependant, ces capacités restent très insuffisantes au regard des besoins et de la croissance du volume de données. Un plan continental de développement de datacenters, adossé à des mécanismes de financement innovants – banques de développement, partenariats public-privé, fonds souverains – est indispensable.

Le développement de points d'échange Internet (IXP) nationaux et régionaux constitue le deuxième pilier de la souveraineté infrastructurelle. Un IXP permet au trafic local de rester local, au lieu de transiter par des serveurs internationaux – ce qui est encore le cas pour une proportion significative du trafic intra-africain. Selon les données de l'Internet Society (ISOC, 2022), l'Afrique compte désormais plus de 40 IXP opérationnels, contre moins de 10 il y a une décennie. Toutefois, nombre d'entre eux manquent de

participants et de capacité technique. Le projet AMS-IX en Afrique du Sud et le KINIX au Kenya sont des modèles de réussite qui mériteraient d'être répliqués (Kende et Rose, 2015 : 34).

Enfin, la souveraineté des données requiert un cadre juridique robuste. Les lois de protection des données personnelles adoptées par un nombre croissant d'États africains – 33 pays en 2023 selon la CNUCED – doivent être complétées par des dispositions spécifiques sur la localisation des données stratégiques et les conditions d'accès par des autorités étrangères. Le modèle du Règlement général sur la protection des données (RGPD) européen peut servir d'inspiration, mais doit être adapté au contexte africain, en tenant compte des spécificités des économies numériques continentales et de la nécessité de ne pas freiner l'innovation (Bygrave, 2014).

La question des logiciels libres et open source mérite une attention particulière dans la perspective de la souveraineté numérique. Le recours systématique aux logiciels libres dans les administrations publiques – à l'instar de la politique française en la matière (circulaire Ayrault de 2012) – permettrait de réduire la dépendance envers les éditeurs propriétaires étrangers, de garantir l'auditabilité du code et de stimuler l'émergence d'un écosystème de développeurs africains capables de maintenir et d'adapter ces outils. Plusieurs pays – Tunisie, Afrique du Sud, Kenya – ont engagé des politiques en ce sens, mais leur mise en œuvre reste partielle.

4.2. Formation, doctrine et capacités cyber offensives

La souveraineté numérique ne se décrète pas : elle se construit par la formation d'un capital humain qualifié, l'élaboration d'une doctrine adaptée et le développement de capacités opérationnelles crédibles. Sur ces trois plans, l'Afrique doit opérer un saut qualitatif considérable.

Le déficit de compétences en cybersécurité est massif sur le continent. Selon le rapport ISC² (2022), l'Afrique manquerait de plus de 100 000 professionnels qualifiés en cybersécurité, un chiffre qui ne cesse de croître avec la numérisation accélérée des économies. Cette pénurie affecte directement les capacités de défense : sans analystes formés à la détection des intrusions, sans experts en forensique numérique, sans ingénieurs capables de concevoir des architectures résilientes, aucune cyberdéfense n'est possible. La formation de « cybercombattants » - terme emprunté à la doctrine française (Ministère des Armées, 2019) – doit devenir une priorité stratégique continentale.

Plusieurs pistes de formation méritent d'être explorées et développées. La création de centres d'excellence régionaux en cybersécurité, sur le modèle du Centre d'excellence coopératif de cyberdéfense de l'OTAN à Tallinn (CCDCOE), permettrait de mutualiser les ressources et de créer des pôles d'expertise de niveau international. Le projet de « Cyber Academy » de l'UA, annoncé dans le cadre de l'Agenda 2063, devrait être concrétisé et doté de moyens suffisants. Au niveau national, l'intégration systématique de modules de cybersécurité dans les cursus d'ingénierie et d'informatique, la création de filières spécialisées de niveau master et doctorat, et le développement de certifications professionnelles adaptées au contexte africain constituent des chantiers prioritaires.

Au-delà de la formation technique, l'élaboration d'une doctrine de cyberdéfense proprement africaine est indispensable. Une telle doctrine doit articuler les dimensions

défensives (protection des systèmes d'information, résilience), informationnelles (veille stratégique, renseignement d'origine cyber) et offensives (capacités de rétorsion, dissuasion) dans un cadre adapté aux réalités africaines. Comme le souligne Kempf (2012), « une doctrine cyber doit être à la fois interarmées et interministérielle, car le cyberespace traverse toutes les frontières institutionnelles ». En Afrique, cette transversalité est d'autant plus nécessaire que les menaces elles-mêmes sont hybrides, mêlant criminalité, espionnage et déstabilisation politique.

La question des capacités offensives est sans doute la plus sensible et la moins documentée. Si plusieurs États africains – Rwanda, Maroc, Éthiopie, Nigeria – sont soupçonnés de disposer de capacités cyber offensives, aucun n'a officiellement déclaré une doctrine d'emploi de l'arme cyber. Or, comme le démontre la littérature stratégique (Libicki, 2009 ; Ventre, 2011), la dissuasion dans le cyberespace repose au moins partiellement sur la capacité – réelle ou perçue – de riposter à une agression. Pour les États africains, le développement de capacités offensives minimales constitue une condition de la crédibilité de leur posture de cyberdéfense, à condition que ces capacités s'inscrivent dans un cadre légal et éthique clairement défini.

L'articulation entre cyberdéfense et coopération continentale est le dernier levier stratégique à activer. L'ACSRT (Centre africain d'études et de recherche sur le terrorisme), basé à Alger, pourrait voir ses attributions étendues à la dimension cyber du terrorisme. La création d'un « Cyber Command » continental, coordonnant les efforts de détection, d'alerte et de réponse à l'échelle du continent, constituerait un saut qualitatif majeur – quoique politiquement complexe. À défaut d'une structure intégrée, le développement de mécanismes d'échange d'informations sur les menaces (threat intelligence sharing) entre CERT nationaux, sur le modèle du réseau FIRST (Forum of Incident Response and Security Teams), constituerait une avancée significative (Skierka et al., 2015).

La coopération Sud-Sud mérite également d'être intensifiée. L'Inde et le Brésil, qui ont développé des capacités de cyberdéfense significatives dans des contextes de pays émergents, offrent des modèles potentiellement plus adaptés aux réalités africaines que les architectures occidentales. Le cadre IBSA (Inde-Brésil-Afrique du Sud) et les mécanismes de coopération BRICS pourraient être mobilisés pour des transferts de compétences et de technologies en matière de cybersécurité. De même, la coopération intra-africaine entre pays plus avancés (Rwanda, Maroc, Afrique du Sud) et pays en phase de structuration constitue un levier sous-exploité qu'il conviendrait d'activer pleinement.

Conclusion

La cyberdéfense n'est plus, pour l'Afrique, un luxe réservé aux puissances technologiques avancées : elle est une nécessité stratégique immédiate, conditionnée par la transformation numérique accélérée du continent et par l'intensification des menaces dans le cyberespace. L'analyse développée dans cet article permet de tirer plusieurs conclusions opérationnelles.

Premièrement, l'Afrique ne part pas de rien. Malgré les vulnérabilités structurelles et les dépendances décrites, des dynamiques positives sont à l'œuvre : stratégies nationales en cours de déploiement, formation progressive de compétences, investissements croissants dans les infrastructures numériques, émergence d'un écosystème de startups

spécialisées. Le discours victimaire, s'il peut avoir une utilité politique, ne rend pas justice à la réalité des efforts engagés ni à la capacité d'innovation démontrée par plusieurs pays du continent.

Deuxièmement, la souveraineté numérique ne se conquiert pas par décret, mais par une stratégie industrielle patiente et un investissement massif dans le capital humain. Les États africains doivent passer d'une logique de consommation technologique à une logique de production et de maîtrise, ce qui suppose des arbitrages budgétaires courageux et une vision à long terme. La création de filières de formation d'excellence, le soutien à l'industrie numérique locale, le développement d'infrastructures souveraines et l'élaboration de doctrines adaptées constituent les quatre piliers d'une stratégie intégrée.

Troisièmement, la dimension continentale est indissociable de la dimension nationale. Aucun État africain, pris isolément, ne dispose des ressources suffisantes pour faire face seul à des menaces étatiques de haut niveau. La mutualisation des capacités, le partage de renseignement sur les menaces et la coordination des réponses – à l'échelle sous-régionale et continentale – sont des impératifs opérationnels, non des options politiques. L'Union africaine doit assumer un rôle de coordination renforcé, et les organisations sous-régionales doivent devenir des relais opérationnels effectifs.

Enfin, la cyberdéfense africaine doit se penser dans une perspective de puissance, et non seulement de protection. Le cyberespace offre aux États africains une possibilité de projection de puissance à coût relativement faible, susceptible de compenser – partiellement – les déséquilibres conventionnels. Les capacités cyber ne sont pas l'apanage des grandes puissances : de petits États determines – Estonie, Israël, Singapour – ont démontré qu'un investissement ciblé pouvait produire des capacités disproportionnées à la taille du pays. C'est dans cette logique d'efficacité stratégique que l'Afrique doit inscrire son effort de cyberdéfense.

Le cyberespace est un espace d'opportunité autant que de menace. Pour l'Afrique, la construction d'une cyberdéfense souveraine n'est pas seulement un impératif sécuritaire : c'est une condition de l'autonomie stratégique au XXIe siècle, et un investissement dans la puissance de demain.

Bibliographie

Africa Data Centres. 2023. State of Data Centres in Africa. Johannesburg : Africa Data Centres Association.

Amin, Samir. 1973. Le développement inégal : essai sur les formations sociales du capitalisme périphérique. Paris : Éditions de Minuit.

ANSSI-SN (Agence nationale de la sécurité des systèmes d'information du Sénégal). 2023. Rapport annuel sur l'état de la cybersécurité au Sénégal. Dakar : ANSSI-SN.

Bayart, Jean-François. 1999. « L'Afrique dans le monde : une histoire d'extraversion ». Critique internationale. Vol. 5, n° 1. p. 97-120.

Thierry, Berthier et Olivier Kempf. 2016. « Vers une géopolitique de la donnée ». Annales des Mines - Réalités industrielles. Vol. août 2016, n° 3. p.15-17

Bogui, Jean-Jacques. 2010. « La cybercriminalité, menace pour le développement : les escroqueries Internet en Côte d'Ivoire ». Afrique contemporaine. Vol. 234, n° 2. p. 155-170.

Bygrave, Lee Andrew. 2014. Data Privacy Law: An International Perspective. Oxford : Oxford University Press.

Blanc, Félix. 2019. « Géopolitique des câbles : une vision sous-marine de l'Internet ». Diplomatie.gouv. N° 6. p. 1-20.

Chéneau-Loquay, Annie. 2012. « La téléphonie mobile dans les villes africaines : une adaptation réussie au contexte local ». L'Espace géographique. Vol. 41, n° 1. p. 82-93.

Desforges, Alix et Frédérick Douzet. 2018. « Géopolitique du cyberespace : territoires, frontières et conflits ». dans Douzet, Frédérick (dir.). La Géopolitique du numérique. Paris : CNRS Éditions. p. 145-172.

Douzet, Frédérick. 2014. « La géopolitique pour comprendre le cyberespace ». Hérodote. N° 152-153. p. 3-21.

Yaacobi, Ahmed. 2023. « Cybersécurité : quels défis pour le Maroc ? ». La jaune et la rouge. N° 788.

Follorou, Jacques et Franck Johannès. 2013. « Révélations sur le Big Brother français ». Le Monde. 4 juillet 2013. https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html [consulté le 15/03/2024].

Forbidden Stories. 2021. « The Pegasus Project ». Forbidden Stories. https://forbiddenstories.org/case/the-pegasus-project/ [consulté le 20/01/2024].

Greenberg, Andy. 2019. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York : Doubleday.

Greenwald, Glenn. 2014. Nulle part où se cacher : l'affaire Snowden par celui qui l'a révélée au monde. Paris : JC Lattès.

GSMA. 2023. The Mobile Economy: Sub-Saharan Africa 2023. Londres : GSMA.

Interpol. 2022. African Cyberthreat Assessment Report 2022. Lyon : Interpol.

ISC². 2022. Cybersecurity Workforce Study 2022. Clearwater : ISC².

Kempf, Olivier. 2012. Introduction à la cyberstratégie. Paris : Economica.

Kende, Michael et Karen Rose. 2015. Promoting Local Content Hosting to Develop the Internet Ecosystem. Genève : Internet Society.

Kshetri, Nir. 2019. « Cybercrime and Cybersecurity in Africa ». Journal of Global Information Technology Management. Vol. 22, n° 2. p. 77-98.

Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Santa Monica : RAND Corporation.

Ministère des Armées (France). 2019. Politique ministérielle de lutte informatique offensive. Paris : Ministère des Armées.

Orji, Uchenna Jerome. 2018. « The African Union Convention on Cybersecurity: A Regional Response to Cybersecurity Threats ». Computer Law & Security Review. Vol. 34, n° 2. p. 237-255.

Skierka, Isabel et al. 2015. « CSIRT Basics for Policy-Makers ». Digital Policy Paper. Berlin : Global Public Policy Institute.

Tilouine, Joan et Ghalia Kadiri. 2018. « À Addis-Abeba, le siège de l'Union africaine espionné par Pékin ». Le Monde. 26 janvier 2018. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-

chinois_5247521_3212.html [consulté le 10/02/2024].

UA (Union africaine). 2014. Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo). Addis-Abeba : Union africaine.

UA (Union africaine). 2022. Rapport continental sur la cybersécurité en Afrique. Addis-Abeba : Commission de l'Union africaine.

UA (Union africaine). 2023. Statut de ratification de la Convention de Malabo. Addis-Abeba : Bureau du conseiller juridique de l'UA.

UA-UIT. 2018. Programme de référence pour la cybersécurité en Afrique. Addis-Abeba/Genève : UA-UIT.

UIT (Union internationale des télécommunications). 2022. Global Cybersecurity Index 2022. Genève : UIT.

Ventre, Daniel. 2011. Cyberguerre et guerre de l'information : stratégies, règles, enjeux. Paris : Lavoisier.

Xalam Analytics. 2022. Africa Data Centre Market: Size, Trends and Forecasts. Dakar : Xalam Analytics.