27042026

Les cahiers cyber Vladimir AMAN

N° 3, Avril 2026 • Analyses, décryptages, prospectives

« ANSSI Africaines»: La vraie illusion d'une fausse cybersécurité nationale

Crédit illustration: freepik

Dans les capitales d'Afrique francophone subsaharienne, un rituel s'est répété avec une régularité troublante au cours de ces dernières années : la création, par décret présidentiel ou loi organique, d'une *Agence Nationale de Sécurité des Systèmes d'Information (ANSSI).*

Bénin, Burkina Faso, Côte d'Ivoire, Niger, Guinée, Congo — la liste s'allonge, et avec elle la promesse implicite d'une cybersécurité nationale enfin digne de ce nom — ont adopté une approche nationale semblable en matière de cybersécurité.
Mais derrière la façade institutionnelle, qu'y a-t-il concrètement?

Une poignée d'agents volontaires mais sous-équipés, des budgets dérisoires et des missions d'une ambition inversement proportionnelle aux moyens disponibles.

La vérité, inconfortable mais nécessaire, est la suivante : **la majorité des ANSSI d'Afrique subsaharienne francophone sont des institutions vitrine, appliquant hors sol et sans véritable prise en compte des réalités structurelles, économiques et culturelles du continent; un modèle étranger dont les performances laissent elles-mêmes à désirer.**

« Ce sont moins les institutions qui protègent un cyberespace national, que de vraies capacités opérationnelles, des budgets sérieux, et une doctrine stratégique ancrée dans ses réalités socio-économiques et culturelles locales. »

Le modèle originel : une référence fragile

L'ANSSI France : ambitions déclarées, réalité nuancée

L'ANSSI française, créée par décret en juillet 2009 et rattachée au Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), est présentée depuis sa création comme le fer de lance de la cybersécurité nationale. Sa doctrine, formulée dès le Livre Blanc sur la Défense et la Sécurité Nationale de 2013, repose sur deux piliers : une posture robuste de protection des systèmes critiques et une capacité de réponse gouvernementale ajustée face aux agressions informatiques. La Revue stratégique de cyberdéfense (RSC) et les différentes lois de programmation militaire (2014 – 2019) constituent un véhicule législatif de transposition et fixation au plus haut niveau de la doctrine nationale et certaines mesures de cybersécurité.

Sur le papier, le dispositif est impressionnant. L'agence compte aujourd'hui plus de 600 agents, un budget hors masse salariale d'environ 23 millions d'euros en 2022 (soit environs 15 milliards FCFA), et coordonne la protection d'un écosystème d'Opérateurs d'Importance Vitale (OIV) répartis dans 12 secteurs d'activités.

Mais voici ce que les panégyriques institutionnels omettent systématiquement de mentionner : le modèle présente des insuffisances criardes. Imprimerie Nationale, Fédération Française de Basketball, France Identité, France Travail, Ecole Directe, la Centrale de financement, etc., ont toute été victimes de cyberattaques et de fuites de données record depuis le début de l'année.
En avril 2026, l'Agence Nationale des Titres Sécurisés (ANTS), service public français gérant passeports, permis de conduire et cartes d'identité, subissait une cyberattaque d'une ampleur sans précédent. Entre 18 et 19 millions de fichiers citoyens — noms, prénoms, dates de naissance, adresses, numéros de téléphone — se retrouvaient sur le dark web. Le vecteur d'attaque ? Une vulnérabilité IDOR (Insecure Direct Object Reference) d'une banalité consternante sur l'API du portail public, que le hacker lui-même a qualifiée de « faille vraiment stupide ».

Cet incident n'est pas isolé : dès septembre 2025, une première compromission supposée de l'ANTS avait déjà mis en alerte les autorités françaises. Ce n'est là que le symptôme le plus récent d'un mal chronique. Depuis cinq ans, les administrations françaises accumulent les incidents de sécurité majeurs. L'hôpital de Corbeil-Essonnes (2022), le ministère de l'Intérieur, des collectivités territoriales par dizaines — le CERT-FR, la cellule opérationnelle de l'ANSSI, enchaîne les alertes sans parvenir à endiguer la marée. La conclusion s'impose d'elle-même : **si le modèle originel, doté de centaines d'agents et de dizaines de millions d'euros, ne parvient pas à protéger efficacement ses propres systèmes critiques, comment ses homologues africains, infiniment moins dotés, y parviendraient-ils ?**

La greffe africaine : anatomie d'un transplant rejeté

1. Le mirage du classement international

Pour comprendre pourquoi les ANSSI africaines se sont multipliées, il faut comprendre la mécanique des incitations qui les a fait naître. L'Union Internationale des Télécommunications (UIT) publie depuis 2014 son Global Cybersecurity Index (GCI), un classement de 194 pays évalués sur cinq piliers : mesures juridiques, techniques, organisationnelles, développement des capacités, et coopération internationale. Ce classement est devenu la référence absolue pour les bailleurs de fonds, les institutions de développement et les gouvernements désireux de démontrer leur maturité numérique.
Or, l'une des composantes organisationnelles les mieux scorées dans ce classement est précisément l'existence d'une agence nationale dédiée à la cybersécurité. ***Créer une ANSSI, c'est cocher une case. C'est améliorer mécaniquement son positionnement dans l'index. C'est envoyer un signal favorable aux investisseurs étrangers et aux partenaires techniques.***

Le résultat dans le GCI 2024 est éloquent : parmi les 46 pays mondiaux classés en **Tier 1** (les « modèles »), aucun pays francophone d'Afrique subsaharienne ne figure [4]. Le Togo et le Bénin atteignent le Tier 2, mais la grande majorité des États de la région stagne aux Tier 3 et Tier 4. *

La Côte d'Ivoire, pourtant dotée d'une ANSSI formellement constituée en octobre 2024, reste dans les échelons inférieurs [5]. *Les pays africains de Tier 1 — Ghana, Kenya, Tanzanie, Rwanda, Maurice — sont significativement tous anglophones ou ont développé des approches sur mesure, non des copies conformes du modèle français.*

2. DES MISSIONS HORS-SOLS

Examinons concrètement ce que les textes fondateurs assignent aux ANSSI africaines. Au Burkina Faso, la Stratégie Nationale de Cybersécurité affiche l'ambition de « garantir un cyberespace de confiance favorable au développement économique et social » à l'horizon 2023. En Guinée, l'ANSSI est chargée, en tant que structure technique d'exécution chargée, de la sécurisation de l'ensemble des systèmes d'information (public et privé) et de la prévention des intrusions, des sensibilisations des usagers des équipements et installations informatiques.
En Côte d'Ivoire, l'ANSSI assure la mise en œuvre des plans d'actions, la coordination et la gestion des crises de cybersécurité, la coordination des actions de protection des infrastructures critiques et des systèmes d'information publics et privés ainsi que le pilotage des processus de prévention, de protection, de surveillance, de détection et de réponse aux incidents.
Ces formulations sont directement inspirées — parfois mot pour mot — des textes fondateurs de l'ANSSI française. Le problème est que les réalités auxquelles elles font face sont sans commune mesure :

- L'ANSSI française compte 600 agents. Les agences africaines équivalentes en comptent généralement entre 15 et 50, souvent moins.
- Le budget de l'ANSSI française est de 23 millions d'euros hors masse salariale. Les budgets africains équivalents se comptent en centaines de millions de francs CFA — soit une fraction infime du besoin.
- La France dispose d'un écosystème de R&D cybersécurité mature (Inria, CentraleSupélec, entreprises privées nationales).
- Les pays francophones d'Afrique subsaharienne souffrent d'une pénurie structurelle de talents : selon le GCI 2024, le manque de professionnels qualifiés est l'un des deux obstacles majeurs à la cybersécurité sur le continent.

Le fossé n'est pas seulement financier. Il est structurel, politique et culturel.

3. UNE GOUVERNANCE FRAGMENTÉE

En France, la coordination cyber repose sur une architecture intégrée : l'ANSSI est rattachée au Premier ministre via le SGDSN, et coordonne directement avec le COMCYBER (commandement militaire cyber). Cette intégration, décrite dans la loi de programmation militaire, crée des synergies opérationnelles réelles [9].
En Afrique subsaharienne, la plupart des ANSSI sont rattachées à des ministères techniques (Numérique, Télécommunications, voire Économie), sans mandat clair vis-à-vis des infrastructures critiques opérées par le secteur privé — opérateurs télécom, banques, énergie — ni des services les plus sensibles de l'État (défense, renseignement, justice). La gouvernance est fragmentée, les périmètres flous, et les mécanismes opérationnels de coordination quasi inexistants.
Résultat : selon le rapport INTERPOL de 2025 sur la cybercriminalité en Afrique, seuls 30 % des pays africains disposent d'un système de signalement des incidents, 29 % d'un référentiel de preuves numériques, et 19 % d'une base de données de renseignements sur les cybermenaces [10]. Dans la plupart des cas l'ANSSI existe, mais ses tentacules ne touchent pas réellement les systèmes qu'elle est censée protéger.

Une menace qui, elle, reste présente et grandissante.

1. LE PARADOXE DE LA CIBLE VALORISÉE

Il existe un phénomène contre-intuitif que les experts en sécurité offensive connaissent bien : la présence d'une agence nationale de cybersécurité peut attirer des attaquants. Non par crainte de la réponse, mais par défi. Compromettre un système officiellement protégé par une ANSSI constitue une démonstration de supériorité technique dans les milieux cybercriminels. En Afrique, où les ANSSI affichent des ambitions de protection très élevées mais disposent de capacités de réponse très limitées, cette logique crée un risque paradoxal : **l'existence de l'agence donne une fausse assurance aux autres acteurs, qui réduisent leur propre investissement sécuritaire en comptant sur elle — tout en signalant aux attaquants une cible nominalement gardée mais réellement vulnérable.**

2. LA FUITE DES CERVEAUX COMME FACTEUR AGGRAVANT

Un facteur structurel aggrave la situation : la fuite des cerveaux. Les rares experts nationaux formés en cybersécurité sont systématiquement aspirés par le secteur privé (banques, opérateurs télécom, multinationales), ou quittent le continent pour l'Europe ou l'Amérique du Nord. Les agences publiques et parapubliques, incapables de rivaliser sur le plan des rémunérations et du profil de carrière, se retrouvent structurellement sous-dotées en compétences de haut niveau— et ce, de façon durable. En effet, dans un contexte mondial où les compétences en cybersécurité sont extrêmement recherchées par les plus grandes firmes, les modèles classiques de gestion des talents tels que pratiqués dans les institutions étatiques africaines, représente un facteur limitant l'attractivité de ce secteur pour les jeunes diplômés en cybersécurité.

3. UNE EXPLOSION DES CYBERATTAQUES SANS RÉPONSE À LA HAUTEUR

Pendant que les Etats et leurs agences nationales peinent à se structurer et se doter de capacités de réponses alignées sur les enjeux, les attaquants, eux, ne se reposent pas. Au deuxième trimestre 2023, l'Afrique a enregistré le nombre moyen de cyberattaques hebdomadaires par organisation le plus élevé au monde, avec une augmentation de **23 %** par rapport à la même période en 2022. En 2024, dix attaques majeures ont frappé des infrastructures critiques africaines, dont le fournisseur d'énergie camerounais Eneo, le National Health Laboratory System sud-africain, et l'autorité kenyane du réseau routier urbain [12].

En Côte d'Ivoire, plus de 200 Go de données ont été dérobées à la compagnie aérienne Air Côte d'Ivoire dans le cadre d'une cyberattaque de type ransomware, au cours de l'année 2026. On note un intérêt croissant de groupes cybercrimimnels structurés pour des cibles dans les pays francophones d'Afrique.

Les chiffres publiés par Kaspersky donnent le vertige : plus de 27 millions de tentatives d'attaques ont été détectées en Côte d'Ivoire en 2024, dont 30% visant directement les infrastructures industrielles. Selon le même rapport de l'entreprise de cybersécurité une part grandissante de logiciels malveillants de type stealer et backdoors opérés depuis des centres de commande et contrôle ont été détectés sur le territoire ivoirien. **Ces chiffres aussi impressionnants soient-ils ne représentent que la pointe visible d'une réalité sous-évaluée et plus inquiétante.** Les plaintes pour cybercriminalité ont bondi de 84 % entre 2022 et 2024, passant de 6 579 à 12 100 cas. Plus de plaintes sont désormais à signalées l'ANSSI, mais il demeure la question de sa capacité à réduire l'ampleur de la menace. Par ailleurs, avec la modification du périmètre d'action de l'ANSSI-CI, un des enjeux majeurs sera sa capacité à détecter proactivement les incidents de sécurité sur les systèmes d'informations publics et privés.

Ce que les pays qui réussissent font différemment

1. LES LEÇONS DE MAURICE, DU GHANA ET DU RWANDA

Parmi les rares pays africains classés en Tier 1 du GCI 2024, un point commun frappe : ils n'ont pas simplement créé une agence, ils ont construit un écosystème.

Maurice, premier pays africain à obtenir la certification SIM3 (une marque d'excellence opérationnelle des CERT), a développé des outils propres, notamment le Maucors (signalement des cybercrimes), Maushield (partage d'informations sur les attaques), MauHNET (réseau de honeypots pour la détection précoce). L'approche adoptée est de type bottom-up, c'est-à-dire en partant de besoins concrets exprimés par les opérationnels, ensuite en développant des outils « in-house » majoritairement propulsés par des technologies open-source et maîtrisés, puis en formant des opérateurs nationaux.

Le Rwanda a, quant à lui, fait de la cybersécurité un élément central de sa Vision 2050, avec une intégration dans le système éducatif, un CERT national opérationnel 24h/24, et des partenariats public-privé réels. L'Autorité nationale de cybersécurité (NCSA) a été créée en 2017 par la loi n° 26/20171 avec pour mission de développer les compétences et les capacités en cybersécurité, afin de garantir la protection de l'intégrité et de la sécurité nationales et de favoriser le développement économique et social. Cette approche positionne l'autorité de cybersécurité comme un moteur de développement des capacités au profit des acteurs de l'écosystème.

Le Ghana a construit sa stratégie cyber en y intégrant explicitement les réalités de son économie numérique (mobile money, agriculture digitale), pas en transposant un document européen.

⚠ ***Dans ces trois pays, le modèle n'a pas été copié. Il a été créé sur mesure.***

2. LES CAS D'ÉCOLES

Au Bénin, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), a été créée sous la forme d'une agence sous tutelle de la Présidence de la République, par la loi portant Code du Numérique en son livre 6ème. Elle avait pour mission de veiller à la sécurité des systèmes d'information et des réseaux sur l'ensemble du territoire de la République du Bénin, protéger les systèmes d'information et des infrastructures critiques, assurer la coordination nationale et la coopération internationale en matière de lutte contre la cybercriminalité, et, d'autre part, au renforcement du cadre juridique et règlementaire, à la promotion de la confiance numérique, au développement des compétences et à la culture de la sécurité numérique.
Par la suite, elle a été fusionnée avec trois autres agences d'exécution pour donner naissance à l'Agence des Systèmes d'Information et du Numérique, un l'établissement public à caractère social et scientifique.

La Côte d'Ivoire de son côté, illustre à la fois les tensions et les espoirs liés à cette problématique. Créée officiellement par décret en octobre 2024, sous la forme d'une agence d'exécution, l'ANSSI-CI hérite d'une configuration complexe, fusionnant les attributions de la DITT, PLCC et certaines de l'ARTCI en matière de cybersécurité.
A peine deux ans après sa création, son champ d'action a déjà été redéfini (en 2026) avec la rétrocession des attributions de la lutte contre la cybercriminalité à la Police Nationale. Ce revirement illustre un balbutiement dans la structuration de la gouvernance nationale de la cybersécurité. L'ANSSI-CI, créée il y a moins de deux ans, doit encore prouver sa capacité à se doter de moyens adéquats, de l'autorité nécessaire et protéger les infrastructures critiques et les services publics critiques — bien au-delà du périmètre de la lutte contre la cyberescroquerie.

Quelles recommandations pour une cybersécurité africaine souveraine ?

Recommandation N°1: Fixer les ambitions et la doctrine nationale de cybersécurité dans document stratégique publié

Aucun pays d'Afrique francophone subsaharienne n'a, à ce jour, publié de document stratégique global intégrant la cybersécurité comme élément central de la sécurité nationale — à l'image du Livre Blanc français de 2013 ou de la Revue Stratégique Cyber (RSC). Or, ce document est le prérequis de tout. Il définit les menaces prioritaires, les actifs critiques, les responsabilités interinstitutionnelles, et le niveau d'ambition réaliste.

Sans lui, une ANSSI est un corps sans colonne vertébrale se déambulant au gré des intempéries cybernétiques et des évolutions technologiques.

Dans la plupart de ces pays, des bribes d'information liés à la doctrine peuvent être retrouvées dans l'énoncé des stratégies nationales de cybersécurité, traitant la cybersécurité et la cyberdéfense comme un problème sectoriel.

⚠ *Chaque État concerné doit mandater, dans un délai de 18 mois, la rédaction d'un tel document stratégique, impliquant non seulement les administrations, mais aussi le secteur privé, la société civile numérique, et des experts cybersécurité du continent.*

1 Doctrine stratégique

Recommandation N°2: Dimensionner les missions aux capacités réelles des Etats

L'inadéquation entre les missions inscrites dans les textes fondateurs et les moyens disponibles est la principale source de dysfonctionnement des agences nationales de cybersécurité. Une ANSSI de 20 agents ne peut raisonnablement pas protéger l'ensemble des infrastructures critiques d'un État de 20 millions d'habitants. Une approche cohérente devrait être de mandater simultanément plusieurs pôles de capacités déjà existants pour assumer des responsabilités dans le renforcement de la cybersécurité.

⚠ Les textes doivent être évolutifs et adopter une approche pragmatique en priorisant :

- ***Phase 1 (0-3 ans) :*** *Protection des systèmes d'information de l'État central uniquement. CERT national opérationnel. Mécanismes de signalement obligatoires pour les OIV.*
- ***Phase 2 (3-7 ans) :*** *Extension aux opérateurs d'importance vitale du secteur privé. Développement d'une filière de formation nationale. Audits de sécurité obligatoires pour les systèmes critiques.*
- ***Phase 3 (7-15 ans) :*** *Couverture complète, développement de capacités offensives (bug bounty, tests d'intrusion publics), contribution aux normes internationales*

2 Planification

Recommandation n°3: Ancrer la stratégie dans les réalités du numérique africain

L'économie numérique africaine est profondément différente du contexte européen. Le mobile money, vecteur d'inclusion financière pour des centaines de millions de personnes, est aussi le principal vecteur d'escroqueries numériques. L'agriculture connectée, l'e-gouvernement déployé sur smartphone, les data centers hébergeant des données régionales — ces réalités n'ont pas d'équivalent dans les documents stratégiques français de 2009.
Une ANSSI africaine doit protéger ces écosystèmes en premier lieu. Cela implique :

- Des unités spécialisées en sécurité des applications mobile money (M-Pesa, Orange Money, Wave…) en liaison directe avec les régulateurs bancaires et les opérateurs télécom.
- Des mécanismes d'évaluation et de contrôle strictes des mesures de sécurité implémentées par les opérateurs de télécommunications et de fournisseurs de services internet où plus de 80% de ces entreprises sont détenus par des capitaux privés étrangers
- Des protocoles de sécurité adaptés aux connexions intermittentes et à la réalité de pays où plus de 60 % du trafic internet transite par mobile.
- Une attention particulière aux données personnelles dans des contextes où l'état civil numérique est encore en construction — les risques d'usurpation d'identité y sont décuplés.

Recommandation n°4: Créer une mutualisation régionale des capacités

Aucun pays francophone subsaharien n'a la taille critique pour bâtir seul une cybersécurité nationale complète. La réponse doit impérativement être régionale. La Convention de Malabo de l'Union Africaine sur la cybersécurité, entrée en vigueur en 2023, fournit le cadre juridique [18]. Mais il faut maintenant construire les institutions et le cadre opérationnel :

- **Un CERT régional UEMOA/CEDEAO** avec des capacités d'intervention mutualisées, à l'image de l'AfricaCERT mais avec des moyens opérationnels réels.
- **Des exercices cyber régionaux obligatoires**, incluant scénarios d'attaque sur infrastructures critiques transfrontalières (réseaux électriques, câbles sous-marins, corridors de paiement intégrés).
- **Un référentiel de compétences africain en cybersécurité**, distinct des certifications euro-américaines, adapté au contexte local et valorisé par les recruteurs publics et privés. Les jeunes Africains sont formés et certifiés et valorisent des lois et des produits euro-américains, ce qui alimente la fuite des cerveaux vers ces territoires.

Recommandation n°5: Rompre avec la logique du classement pour construire une logique de résultats concrets

Le GCI de l'UIT est un outil utile, mais il est devenu une fin en soi pour de nombreux gouvernements africains. Or, un bon classement GCI n'implique pas nécessairement une cybersécurité ou une cyberdéfense éffective. La preuve : des pays bien classés dans le classement GCI ont subi des attaques majeures impactant des infrastructures critiques, faisant la preuve d'un niveau de maturité opérationnelle totalement déconnecté des considérations d'ordre purement « théorique ». Tandis que dans la pratique certains pays mal évalués par des normes démontrent un niveau de préparation opérationnel bien aligné avec les enjeux et les contextes locaux, sectoriels des cybermenaces.

⚠ *Chaque État concerné doit développer et adopter des indicateurs et métriques de cybersécurité basés sur les résultats, pas sur la conformité. Cela peut impliquer:*

- *Temps moyen de détection et de réponse des incidents majeurs sur des systèmes critiques (MTTD, MTTR)*
- *Temps moyen de mitigation des vulnérabilités critiques sur des systèmes essentiels*
- *Taux d'investissement des opérateurs d'importance vitale en matière de cybersécurité*
- *Taux de systèmes critiques audités annuellement*
- *Nombre de tentatives d'intrusion bloquées sur les OIV*
- *Taux de rétention des personnels qualifiés en cybersécurité dans le secteur public*
- *Etc.*

Recommandation n°6: Investir massivement dans la formation et retenir les talents

La pénurie de talents est le verrou de tout le reste. Sans experts, pas de détection, pas de réponse, pas d'anticipation. Les gouvernements doivent mettre en place :

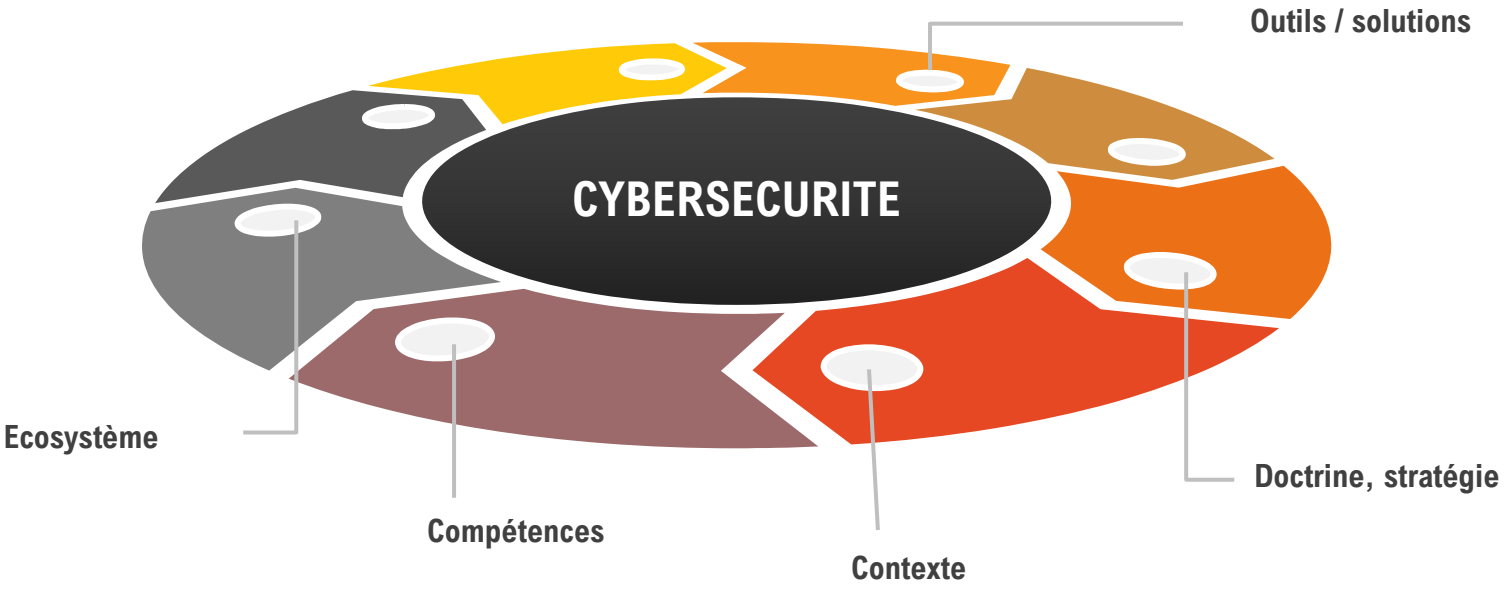
- Des filières universitaires nationales en cybersécurité avec des partenariats industriels garantissant l'employabilité (sur le modèle des écoles d'ingénieurs marocaines ou ghanéennes).
- Des obligations de service national cyber pour les diplômés bénéficiaires de bourses d'État, permettant de retenir les compétences dans le secteur public pendant au moins trois ans.
- Des grilles salariales compétitives dans les ANSSI, financées par une contribution prélevée sur les opérateurs numériques (télécom, banques digitales, plateformes) — dont les activités dépendent directement de la sécurité des infrastructures nationales.

Conclusion: Choisir entre la façade et la souveraineté

La plupart des Etats Africains ne peuvent pas s'offrir le luxe de multiplier des agences nationales de cybersécurité. Ils ont besoin de doctrine claire, politiques éclairées, et surtout de moyens dimensionnés à des objectifs réalistes. Le tout alimenté par une volonté politique de traiter la cybersécurité non comme un accessoire de communication institutionnelle, mais comme un pilier de la souveraineté nationale au même titre que la défense du territoire ou la stabilité monétaire. Dans un contexte régional de digitalisation croissante, la cybersécurité n'est plus un luxe; mais une exigence de souveraineté et de développement économique.

Le modèle français a eu le mérite d'exister, d'inspirer, d'aiguiller et de poser une architecture de référence. Mais il est né dans un contexte radicalement différent : une économie développée, un État central fort, une industrie de défense mature, et une tradition de grand corps d'État capable d'absorber les chocs.

Transposer ce modèle en Afrique subsaharienne sans adapter ni les structures, ni les priorités, ni les moyens, c'est condamner les agences créées à l'inefficacité — et pire, à donner aux décideurs un faux sentiment de sécurité pendant que les attaquants, eux, n'ont jamais été aussi actifs.
La vraie illusion n'est pas dans les hackers. Elle est dans les décrets et la « cybersécurité sur papier ».
Il est temps que l'Afrique cesse d'importer sa cybersécurité, et commence à l'inventer; afin de reconquérir une portion de sa souveraineté confisquée par les intérêts géopolitique et économique externes..



Références

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI France) — Wikipedia, 2024. Effectifs : ~600 agents. Budget hors masse salariale : 23M€ (2022) https://fr.wikipedia.org/wiki/Agence_nationale_de_la_sécurité_des_systèmes_d'information
- Livre Blanc sur la Défense et la Sécurité Nationale, France, 2013. Doctrine nationale de réponse aux agressions informatiques.
- Cyberattaque ANTS — Confirmation du ministère de l'Intérieur, 20 avril 2026. Fuite de 18 à 19 millions de fichiers citoyens. Vecteur : vulnérabilité IDOR sur l'API du portail national. https://www.clubic.com/actualite-609775
- Union Internationale des Télécommunications (UIT) — Global Cybersecurity Index (GCI) 2024. 194 pays évalués sur 5 piliers, classement en 5 niveaux (Tiers). Publication : 12 septembre 2024. https://cio-mag.com/analyse-de-la-situation-africaine-selon-le-global-cybersecurity-index-gci-2024
- Côte d'Ivoire — Rapport annuel ANSSI-CI 2024. Hausse des plaintes de 84% entre 2022 et 2024 (6 579 → 12 100 cas). https://cio-mag.com/cybercriminalite-en-cote-divoire-en-2024
- ANSSI Burkina Faso — Stratégie nationale de cybersécurité (SNCS-BF). Atelier de renforcement des capacités, novembre 2021. https://faso7.com/2021/11/23/cybersecurite-au-burkina-faso-anssi-renforce-les-capacites-de-50-acteurs/
- ANSSI Côte d'Ivoire — Création par décret, octobre 2024. Fusion DITT + attributions cybersécurité ARTCI. Source : CIO Mag, juin 2025.
- GCI 2024, UIT — Pénurie de talents en cybersécurité comme défi majeur du continent africain. https://cybersecuritymag.africa/nouveau-rapport-gci-2024-sur-la-cyber-en-afrique-decryptage-dun-expert/
- Assemblée Nationale française — Question n°23728 sur les budgets ANSSI et COMCYBER. Loi de Programmation Militaire 2019-2025. https://questions.assemblee-nationale.fr/q15/15-23728QE.htm
- INTERPOL — Rapport d'évaluation des cybermenaces en Afrique 2025. 30 % des pays africains disposent d'un système de signalement des incidents. https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2025
- AFCSM — Paysages des cybermenaces en Afrique en 2023. Afrique : +23 % de cyberattaques hebdomadaires par organisation au T2 2023. https://afcsm.com/paysages-des-cybermenaces-en-afrique-en-2023/
- AITN — Cybermenaces en Afrique : Les 10 attaques qui ont marqué 2024. Attaques Eneo Cameroun, NHLS Afrique du Sud, KURA Kenya. https://afriqueitnews.com/tech-media/cybermenaces-afrique-10-attaques-qui-ont-marque-2024/
- Conférence KNext 2025 (Kaspersky / Ministère ivoirien du Numérique) — 27 millions de tentatives d'attaque en Côte d'Ivoire en 2024. https://westafdaily.com/afrique-de-l-ouest
- Commission Économique des Nations Unies pour l'Afrique (CEA/ECA) — Le faible niveau de préparation aux cybermenaces coûte en moyenne 10 % du PIB. Source citée dans : AFCSM Paysages des cybermenaces en Afrique 2023.
- GCI 2024, UIT — Maurice : score parfait 100/100 sur les 5 piliers. Premier pays africain et de l'hémisphère Sud certifié SIM3. Outils : Maucors, Maushield, MauHNET. https://www.lemauricien.com/le-mauricien/global-cybersecurity-index-2024-maurice-no-1-en-afrique-rejoint-le-tier-1-mondial
- Convention de Malabo (Union Africaine) sur la cybersécurité et la protection des données personnelles — entrée en vigueur en 2023. https://www.makanisi.org/cybersecurite-uit-lafrique-en-progres/

AMAN VLADIMIR
Msc MBA Management de la Cybersécurité
C|CISO, CISSP, CEH, ISO 27001 LA/LI, ISO 27032 LCM
Expert Cybersécurité et Consultant International en Sécurité de l'Information,
Auteur-Conférencier

Limitation de responsabilité
Tous les efforts ont été déployés par l'auteur pour rendre le présent document le plus complet, exhaustif et précis possible. Cependant, aucune garantie n'est apportée sur la complétude et la précision des informations qui y sont contenues. Par conséquent, l'auteur décline toute responsabilité en ce qui concerne les pertes ou dommages résultant de la dépendance ou de l'usage des informations contenues dans le présent document.

Ce document est publié à titre d'analyse indépendante de l'auteur. Il n'engage ni les agences citées, ni aucune organisation internationale. Les données chiffrées sont issues de sources publiques référencées.