CYBER AFRICA FORUM · 6e ÉDITION · COTONOU 2026

Construire la confiance numérique de demain

25 recommandations stratégiques pour une Afrique souveraine, sûre et innovante

Contribution de 50Afrique et Afropreneurs Emerging Leaders · Sofitel Cotonou Marina · 16 et 17 novembre 2026



Cotonou, 16 novembre 2026 : Franck Kié, Commissaire général du Cyber Africa Forum, à la tribune du Dôme du Sofitel lors de la cérémonie d'ouverture.



Mahuna Akplogan, ministre de la Transformation digitale et de l'Innovation du Bénin, lors de la cérémonie d'ouverture.

Porteurs	50Afrique, think tank · Afropreneurs Emerging Leaders, mouvement de leadership et d'entrepreneuriat
Auteurs	Équipe du think tank 50Afrique et d'Afropreneurs Emerging Leaders
Cadre	Cyber Africa Forum (CAF), 6ᵉ édition — thème officiel « Construire la confiance numérique de demain »
Lieu et dates	Sofitel Cotonou Marina Hotel & Spa, Cotonou (Bénin), 16 et 17 novembre 2026
Destinataires	Chefs d'État et ministres, régulateurs, agences de cybersécurité, dirigeants d'entreprise, investisseurs, institutions panafricaines, bâtisseurs de l'écosystème tech
Statut	Contribution indépendante. Elle n'a été ni validée ni endossée par les organisateurs du Forum, ses intervenants ou les institutions citées.

Convention de lecture. Les faits établis sont sourcés (année, périmètre, source). Les analyses et propositions sont celles de 50Afrique et d'Afropreneurs Emerging Leaders ; les hypothèses sont signalées comme telles.

Sommaire

1. Mot d'ouverture 5
2. Résumé exécutif 7
3. Diagnostic stratégique de la confiance numérique en Afrique 9
4. Défis, opportunités et cartographie des décideurs 13
5. Les 25 recommandations stratégiques 17
   - Axe 1 — Faire de la cybersécurité une priorité de souveraineté nationale et économique 18
   - Axe 2 — Construire une intelligence artificielle africaine, responsable et souveraine 22
   - Axe 3 — Faire de la souveraineté numérique une réalité économique 24
   - Axe 4 — Garantir la protection des données et restaurer la confiance des citoyens 28
   - Axe 5 — Faire de l'innovation africaine un moteur de croissance et de souveraineté 31
   - Axe 6 — Développer une cyberdiplomatie et une coopération panafricaines fortes 33
   - Axe 7 — Protéger l'espace informationnel et combattre la désinformation 35
   - Axe 8 — Financer la transformation numérique et mobiliser les capitaux 37
   - Axe 9 — Faire du capital humain le socle de la confiance numérique 39
   - Axe 10 — Construire une économie numérique panafricaine interopérable et inclusive 41
6. Matrice des responsabilités par catégorie de décideurs 43
7. Feuille de route de mise en œuvre : 12 mois, 3 ans, 5 ans 47
8. Mécanisme de suivi et d'évaluation 50
9. Trois initiatives structurantes portées par 50Afrique et Afropreneurs Emerging Leaders 53
10. Échos du Forum : déclarations, propositions et analyse 56
11. Appel à l'action 63
12. Conclusion : maîtriser plutôt que subir 64
13. Annexes 65
14. Bibliographie 71
15. Quatrième de couverture 73

Mot d'ouverture

La confiance ne se décrète pas. Elle se construit, se mesure et se perd, parfois en une nuit. En juin 2024, un rançongiciel a paralysé le réseau public de laboratoires d'Afrique du Sud, et des médecins ont dû revenir au papier. En juillet 2023, une attaque par déni de service a rendu indisponible, plusieurs jours durant, le portail par lequel l'État kényan délivre des milliers de services. Ces épisodes ne disent pas que l'Afrique serait plus fragile qu'ailleurs. Ils disent que notre numérisation avance plus vite que notre capacité à la protéger.

C'est le point de départ de cette contribution. Nous ne voulons pas ajouter une déclaration de principe à celles qui existent déjà. L'Union africaine dispose d'une convention sur la cybersécurité, d'une stratégie continentale d'intelligence artificielle, d'un protocole sur le commerce numérique. Le problème n'est plus l'absence de textes. C'est l'écart entre les textes et les budgets, entre les stratégies et les équipes capables de les exécuter.

Notre conviction est simple : la confiance numérique est devenue une infrastructure économique, au même titre que l'énergie ou les ports. Un investisseur n'engage pas de capitaux patients là où les données fuient. Un citoyen n'adopte pas l'identité numérique s'il ne sait pas qui l'utilise. Une PME ne vend pas au-delà de ses frontières si ses paiements ne passent pas. Les économies africaines qui maîtriseront cette infrastructure capteront la valeur ; les autres la subiront.

Nous avons donc fait des choix. Vingt-cinq recommandations, chacune avec un destinataire, un mode d'exécution, un horizon et un indicateur. Cinq d'entre elles nous paraissent mûres pour devenir des engagements dès la clôture du Forum. Certaines dérangeront : nous plaidons par exemple pour mutualiser plutôt que multiplier les centres opérationnels de sécurité, et pour une localisation des données ciblée plutôt que générale.

Ce document est le fruit d'une démarche indépendante. Il n'engage ni les organisateurs du Cyber Africa Forum, ni ses intervenants. Il est une invitation au débat, et surtout à l'action : nous proposons d'en suivre la mise en œuvre, publiquement, année après année.

Si Cotonou peut être le lieu où l'on passe de l'intention à l'engagement chiffré, cette sixième édition aura rempli sa promesse.

Cédric Yamdjeu Fondateur de 50Afrique et du mouvement Afropreneurs Emerging Leaders

Résumé exécutif

L'Afrique ne manque plus de cadres juridiques sur le numérique ; elle manque de capacité d'exécution, de moyens dédiés et de mesure. Nos 25 recommandations visent cet écart, avec cinq engagements prioritaires et trois initiatives que 50Afrique et Afropreneurs Emerging Leaders proposent de porter.

Quatre convictions

1. **La confiance numérique est une condition de compétitivité, pas un coût de conformité.** Elle conditionne l'adoption des services publics en ligne, du mobile money, de l'identité numérique et l'arrivée de capitaux.
2. **La souveraineté utile est une capacité de décision, pas une autarcie.** Elle se joue sur trois leviers concrets : la commande publique, la classification des données et la qualité des contrats technologiques.
3. **Mutualiser vaut mieux que dupliquer.** Avec des talents rares et des budgets contraints, les centres opérationnels de sécurité, les capacités de calcul pour l'IA et les réponses aux crises gagnent à être régionaux ou sectoriels.
4. **Ce qui n'est pas mesuré n'est pas piloté.** Chaque recommandation porte un indicateur ; nous proposons un observatoire indépendant pour les suivre.

Cinq engagements prioritaires à annoncer à Cotonou

#	Engagement	Qui s'engage	Preuve à 12 mois
R1	Désigner les opérateurs d'importance vitale et leur imposer un socle de sécurité avec notification d'incident sous 72 heures	Gouvernements, agences nationales de cybersécurité	Décret publié, liste des secteurs, premier rapport d'incidents
R11	Garantir aux autorités de protection des données un budget plancher et une indépendance effective	Gouvernements, parlements	Ligne budgétaire dédiée, effectifs publiés, rapport annuel
R14	Lancer un programme « premier client public » pour les startups de cybersécurité et d'IA	Ministères du numérique et des finances, grandes entreprises	Premiers défis publiés, premiers contrats signés
R17	Connecter les CSIRT nationaux à un dispositif africain de partage d'information sur les menaces	Agences cyber, CSIRT, Commission de l'UA	Protocole de partage signé, premiers bulletins communs
R22	Créer des académies cyber et IA à vocation régionale avec au moins 30 % de femmes	Gouvernements, universités, entreprises, partenaires	Première cohorte lancée, taux d'insertion suivi

Trois initiatives portées par 50Afrique et Afropreneurs Emerging Leaders

- **Observatoire panafricain de la confiance numérique** : un tableau de bord annuel et public des 25 recommandations, pays par pays.
- **Pacte des dirigeants pour la cyber-résilience** : des engagements volontaires, vérifiables, pris par des directions générales publiques et privées.
- **Programme Afropreneurs Cyber & IA Leaders** : des cohortes de jeunes talents formés au leadership et confrontés à de vrais cas d'administrations et d'entreprises.

Ce qui est nouveau dans cette contribution. Elle assume des arbitrages (mutualiser plutôt que multiplier, localiser les données de manière ciblée, réguler l'IA d'abord par les lois existantes). Elle assigne chaque mesure à un responsable identifiable. Et elle propose un dispositif pour en suivre l'exécution, au lieu de s'arrêter à la clôture du Forum.

Diagnostic stratégique de la confiance numérique en Afrique

Le diagnostic tient en une phrase : les usages numériques africains sont massifs et croîssent vite, tandis que les capacités de protection, de calcul et de régulation restent minces et très inégalement réparties.

Les chiffres qui cadrent le débat

Dimension	Constat	Année et périmètre	Source
Usage d'Internet	36 % de la population utilise Internet ; 55 % en ville contre 21 % en zone rurale ; 31 % des femmes contre 40 % des hommes	2025, région Afrique de l'UIT	UIT, Facts and Figures 2025
Mobile money	1,2 milliard de comptes enregistrés et 174 services actifs	2025, Afrique subsaharienne	GSMA, State of the Industry 2026, via The Guardian Nigeria
Cybercriminalité	Plus de 30 % des infractions signalées en Afrique de l'Ouest et de l'Est sont liées au cyber	2025, 43 pays membres d'INTERPOL évalués	INTERPOL, Africa Cyberthreat Assessment 2025
Capacités de réponse	30 % des pays disposent d'un système de notification d'incidents, 29 % d'un système de traitement de la preuve numérique, 19 % d'une base de données sur les cybermenaces	2025, pays africains répondants	INTERPOL, via WeAreTech Africa
Maturité cyber des États	5 pays de la région Afrique en niveau 1 (Ghana, Kenya, Maurice, Rwanda, Tanzanie) ; Bénin, Togo, Afrique du Sud et Zambie en niveau 2	2024, Global Cybersecurity Index	UIT GCI 2024, via New Times ; Ecofin
Talents cyber	Moins de 300 000 professionnels ; déficit d'environ 68 800 postes, soit 23 %	2024, Afrique	BCG et Global Cybersecurity Forum, via African Arguments

Dimension	Constat	Année et périmètre	Source
Protection des données	44 pays dotés d'une loi, 38 autorités pleinement opérationnelles, 11 pays sans loi	Fin 2025, États membres de l'UA	Digital Policy Alert, janvier 2026
Infrastructures de calcul	18 % de la population mondiale, 0,6 % de la capacité mondiale de centres de données, environ 5 % des centres africains prêts pour l'IA	Octobre 2026, Afrique subsaharienne	Banque mondiale, Africa Economic Update, via Devdiscourse
Données pour l'IA	Environ 2 % des données mondiales d'entraînement viennent d'Afrique ; 710 jeux de données en swahili sur Hugging Face contre 88 844 en anglais	Octobre 2026	Banque mondiale, via FourWeekMBA
Financement des startups	4,1 milliards de dollars levés (dette incluse) ; 72 % captés par Kenya, Afrique du Sud, Égypte et Nigeria	2025, Afrique	Partech, via AllAfrica ; Tech In Africa
Désinformation	189 campagnes documentées, près de quatre fois plus qu'en 2022 ; au moins 39 pays ciblés	2023, Afrique	Africa Center for Strategic Studies, mars 2024

Ce que ces chiffres disent, et ce qu'ils ne disent pas

Un décalage de rythme. Le mobile money, l'identité numérique et les services publics en ligne progressent plus vite que les capacités de détection et de réponse. Les fraudes par hameçonnage, première menace selon INTERPOL, exploitent précisément cette adoption rapide par des utilisateurs peu formés.

Des textes en avance sur les moyens. Quarante-quatre lois sur les données, mais six sans régulateur actif. Une convention continentale (Malabo) entrée en vigueur en juin 2023 avec seulement 15

ratifications sur 55 États. Une stratégie continentale d'IA adoptée en juillet 2024, quand une minorité de pays dispose d'une stratégie nationale.

Un continent pluriel. Le Rwanda, Maurice, le Kenya ou le Ghana ont des dispositifs cyber parmi les plus aboutis au monde. D'autres pays construisent leurs premières briques. Les pays francophones, anglophones et lusophones ont hérité de traditions juridiques différentes, et les zones monétaires (UEMOA, CEMAC) offrent des leviers de mutualisation que d'autres n'ont pas. Une même recommandation ne s'applique donc pas partout au même rythme.

Le cas béninois, un révélateur utile. Le Bénin s'est doté d'un Code du numérique (loi n° 2017-20), d'une équipe nationale de réponse aux incidents (bjCSIRT) au sein de l'ASIN et d'un registre national des personnes physiques qui a recensé plus de 10,3 millions de personnes. Le rapport du bjCSIRT sur 2021-2024 recense pourtant 878 vulnérabilités détectées, dont 207 critiques, et 832 fuites de mots de passe, dont 406 dans le secteur financier. Avoir les institutions ne suffit pas : il faut l'hygiène quotidienne, les audits et les compétences. Sources : Conseil de l'Europe, Octopus ; ID4Africa 2026 ; Benin Web TV.

Ce que les chiffres ne disent pas. Les données africaines sur les incidents sont lacunaires : peu d'organisations déclarent, et les méthodologies varient. Les montants de pertes cités dans le débat public doivent être lus avec prudence. C'est une raison de plus pour rendre la notification obligatoire et l'observation indépendante.

Défis, opportunités et cartographie des décideurs

Six défis structurent la confiance numérique africaine ; chacun recouvre une opportunité économique pour qui sait la saisir.

Défi	Pourquoi il compte	Opportunité correspondante
Exécution plus lente que la législation	Des lois sans régulateur ni budget ne protègent personne et découragent les investisseurs	Un marché de la conformité, de l'audit et de la sécurité managée pour des prestataires africains qualifiés
Pénurie et fuite des compétences	Le déficit de talents freine à la fois la défense et l'innovation	Une jeunesse nombreuse, des programmes de masse déjà lancés, une diaspora qualifiée
Dépendance pour le calcul, le cloud et les équipements	Les décisions techniques et contractuelles se prennent souvent ailleurs	La commande publique et la classification des données comme leviers de négociation
Fragmentation des marchés et des règles	Une startup doit se conformer à autant de régimes que de pays	Le protocole de la ZLECAf sur le commerce numérique et ses annexes, adoptées en février 2025
Espace informationnel vulnérable	La désinformation alimente l'instabilité politique et sécuritaire	Des médias, des fact-checkers et des chercheurs africains capables de documenter et de répondre
Capital concentré et court	Quatre pays captent l'essentiel des fonds ; l'amorçage recule	L'épargne longue africaine (fonds de pension, assureurs) et les institutions de développement

Cartographie des parties prenantes

Note de méthode. La cartographie ci-dessous repose sur les catégories de participants annoncées par les organisateurs (ministres, régulateurs, dirigeants d'entreprise, investisseurs, entrepreneurs,

experts internationaux, responsables d'agences numériques) et sur les partenaires officiellement cités : les ministères béninois de l'Économie et des Finances et de la Transformation digitale, et l'ASIN pour le HackerLab. Aucune position n'est prêtée à un intervenant. Les recommandations s'adressent à des fonctions, non à des personnes. Sources : Digital Business Africa ; Osiris.

Catégorie	Principaux défis	Responsabilité dans la confiance	Décisions à sa main	Engagem raisonnab attendre
1. Décideurs politiques et gouvernements	Arbitrages budgétaires, horizons électoraux courts	Fixer le cap et financer l'exécution	Décrets, lois de finances, ratifications	Socle de sécurité c opérateur vitaux sou mois
2. Ministères (numérique, économie, finances, commerce, recherche)	Coordination interministérielle, compétences internes	Traduire les stratégies en programmes budgétés	Commande publique, programmes de formation, financements	Clauses c qualificati de révers dans les marchés
3. Régulateurs et autorités de protection des données	Moyens limités, indépendance fragile	Rendre les règles effectives et protéger les recours	Contrôles, sanctions, lignes directrices, bacs à sable	Plan de contrôle a publié
4. Agences de cybersécurité et structures de défense	Effectifs, veille 24/7, coopération transfrontalière	Prévenir, détecter, répondre, coordonner	Qualification des prestataires, exercices, partage d'information	Exercice crise nati annuel, connexio partage a
5. Banques, institutions financières, opérateurs de paiement	Fraude, hameçonnage, risques de tiers	Protéger l'épargne et les paiements	Budgets cyber, SOC sectoriels, standards d'authentification	Participat un SOC o ISAC sect
6. Télécommunications et infrastructures	Disponibilité, attaques par déni de service, énergie	Assurer la continuité des réseaux et des centres de données	Investissements, redondance, partage de menaces	Plans de continuité testés et partagés le CSIRT

Catégorie	Principaux défis	Responsabilité dans la confiance	Décisions à sa main	Engagem raisonnab attendre
7. Entreprises technologiques et fournisseurs	Pression concurrentielle, conformité multiple	Sécurité dès la conception, transparence	Choix d'architecture, localisation des équipes	Emplois technique locaux et transfert compéter mesurabl
8. Investisseurs, fonds, institutions financières internationales	Taille des tickets, risque de change, sorties	Apporter du capital patient et exiger une bonne gouvernance cyber	Thèses d'investissement, garanties, due diligence	Clause de maturité dans les diligence
9. Organisations panafricaines et partenaires au développement	Lenteur des ratifications, dispersion des programmes	Harmoniser, mutualiser, financer	Protocoles, programmes régionaux, conditionnalités	Feuille de de ratifica et d'harmon
10. Entrepreneurs, startups, chercheurs, jeunesse	Accès au marché et au capital, reconnaissance	Inventer des solutions adaptées et participer aux décisions	Produits, recherche, mobilisation citoyenne	Solutions certifiées participat aux instar de suivi

Les 25 recommandations stratégiques

Les recommandations sont réparties sur dix axes, avec davantage de poids pour la cybersécurité, l'IA, la souveraineté économique et la protection des données. Les cinq marquées PRIORITAIRE sont celles que nous proposons d'annoncer comme engagements à Cotonou. Horizons : court terme (0-12 mois), moyen terme (1-3 ans), long terme (3-5 ans).

Axe 1 — Faire de la cybersécurité une priorité de souveraineté nationale et économique

R1 — Désigner les opérateurs d'importance vitale et leur imposer un socle de sécurité opposable PRIORITAIRE

- **Constat.** Selon INTERPOL (2025), seuls 30 % des pays africains disposent d'un système de notification des incidents. En juin 2024, le rançongiciel qui a frappé le National Health Laboratory Service sud-africain a aussi atteint ses sauvegardes et obligé au retour au papier (Daily Maverick ; SAMJ).
- **Enjeu.** Sans liste officielle des opérateurs critiques, personne n'est comptable de leur protection, et l'État découvre les incidents par la presse.
- **Recommandation.** Désigner par décret, secteur par secteur, les opérateurs d'importance vitale (énergie, eau, banques et paiements, télécoms, santé, identité, régies financières) et leur imposer un socle minimal : authentification forte, sauvegardes hors ligne testées, journalisation, plan de continuité, notification au CSIRT national sous 72 heures.
- **Destinataires.** Présidences et primatures, ministères du numérique, agences nationales de cybersécurité, régulateurs sectoriels (banques centrales, régulateurs télécoms, autorités de santé).
- **Exécution.** Décret d'application des lois cyber existantes ; référentiel publié par l'agence nationale ; audits par des prestataires qualifiés ; sanctions graduées. Le Bénin dispose déjà d'un référentiel de qualification des prestataires et d'une liste des types d'incidents à remonter à l'ASIN, base réutilisable.
- **Horizon.** Court terme pour le décret et la liste ; moyen terme pour l'audit complet des opérateurs.
- **Indicateurs.** Part des opérateurs désignés audités ; délai médian entre détection et notification ; part disposant de sauvegardes hors ligne testées dans l'année.
- **Impact attendu.** Continuité des services essentiels (soins, paiements, électricité) et données fiables sur la menace réelle.

R2 — Mutualiser des centres opérationnels de sécurité (SOC) sectoriels et régionaux

- **Constat.** L'Afrique compte moins de 300 000 professionnels de la cybersécurité et un déficit d'environ 68 800 postes (BCG et Global Cybersecurity Forum, 2024). Un SOC fonctionnant 24 heures sur 24 exige des équipes que beaucoup d'États et d'entreprises ne peuvent réunir seuls.
- **Enjeu.** Multiplier des SOC nationaux sous-dimensionnés disperse les rares talents et produit une fausse sécurité.
- **Recommandation.** Créer des SOC partagés par secteur (finance, santé, énergie) et, dans les zones monétaires ou communautés régionales, des capacités mutualisées entre États.
- **Destinataires.** Banques centrales (BCEAO, BEAC et banques centrales nationales), associations professionnelles des banques et assureurs, ministères de la santé, agences cyber.
- **Exécution.** Modèle de coût partagé au prorata des actifs protégés ; opérateur public ou concession à un prestataire qualifié ; plateforme commune d'indicateurs de compromission ; financement de lancement par une institution de développement.
- **Horizon.** Moyen terme.
- **Indicateurs.** Nombre d'entités couvertes ; délai moyen de détection ; coût par entité comparé à un SOC interne.
- **Impact attendu.** Une protection professionnelle accessible aux banques moyennes, aux microfinances et aux hôpitaux.
- **Arbitrage assumé.** La mutualisation suppose de confier des données de sécurité à un tiers. La gouvernance (qui voit quoi, sous quel contrôle) doit être fixée avant la technique.

R3 — Organiser chaque année des exercices de crise cyber nationaux et transfrontaliers

- **Constat.** En juillet 2023, une attaque par déni de service revendiquée par le groupe « Anonymous Sudan » a rendu indisponible le portail eCitizen du Kenya, qui offre plus de 5 000 services, du 23 au 27 juillet, et perturbé d'autres opérateurs (Capital FM ; ngCERT).
- **Enjeu.** Une crise cyber est d'abord une crise de décision : qui parle, qui coupe, qui paie, qui informe.
- **Recommandation.** Tenir un exercice national annuel impliquant les ministres et directeurs généraux, et un exercice régional (CEDEAO, EAC, SADC, CEEAC) sur des scénarios réalistes : déni de service sur l'identité numérique, rançongiciel hospitalier, compromission d'un opérateur de mobile money.
- **Destinataires.** Agences cyber, cabinets des chefs de gouvernement, opérateurs vitaux, communautés économiques régionales.
- **Exécution.** Calendrier pluriannuel ; retours d'expérience publiés sous forme de synthèse ; corrections suivies.
- **Horizon.** Court terme pour le premier exercice national.
- **Indicateurs.** Nombre d'exercices ; part des mesures correctives mises en œuvre à six mois.
- **Impact attendu.** Des chaînes de décision rodées et une communication publique maîtrisée en cas d'attaque.

R4 — Rendre les conseils d'administration comptables du risque cyber

- **Constat.** Au Bénin, le bjCSIRT a recensé 832 fuites de mots de passe entre 2021 et 2024, dont 406 dans le secteur financier (Benin Web TV). Ces failles relèvent moins de la technologie que de la gouvernance.
- **Enjeu.** Tant que le risque cyber reste un sujet de direction informatique, il n'obtient ni budget ni arbitrage.
- **Recommandation.** Inscrire le risque cyber dans les codes de gouvernance des sociétés cotées et des établissements réglementés : comité des risques compétent, revue annuelle par le conseil, information publiée dans le rapport annuel.
- **Destinataires.** Régulateurs des marchés financiers, banques centrales et commissions bancaires, autorités de contrôle des assurances, conseils d'administration.
- **Exécution.** Circulaire prudentielle ; formation obligatoire des administrateurs ; questionnaire de maturité joint au reporting réglementaire.
- **Horizon.** Moyen terme.
- **Indicateurs.** Part des sociétés cotées publiant une information cyber ; part des administrateurs formés.
- **Impact attendu.** Des budgets de sécurité décidés au bon niveau et une meilleure note de risque pour les investisseurs.

Axe 2 — Construire une intelligence artificielle africaine, responsable et souveraine

R5 — Mutualiser une capacité de calcul régionale pour l'IA plutôt que des centres nationaux de prestige

- **Constat.** L'Afrique subsaharienne abrite 18 % de la population mondiale mais 0,6 % de la capacité mondiale de centres de données, et environ 5 % des centres africains sont prêts pour l'IA (Banque mondiale, octobre 2026). Le Rapport sur le développement dans le monde 2026 conseille aux pays en développement de ne pas courir après les grands modèles (Nairametrics).
- **Enjeu.** L'accès au calcul conditionne la recherche, les startups et l'usage de l'IA par les administrations. Le construire pays par pays coûterait cher pour des taux d'utilisation faibles.
- **Recommandation.** Créer des « communs de calcul » régionaux : quelques pôles dotés d'énergie fiable, accessibles par crédits aux universités, startups et administrations des pays participants.
- **Destinataires.** Ministères du numérique et de la recherche, Banque africaine de développement, Banque mondiale et IFC, opérateurs de centres de données, Smart Africa.
- **Exécution.** Accord-cadre régional ; achat groupé ou location de capacités ; tarification différenciée (recherche, startups, secteur public) ; gouvernance partagée entre États contributeurs.
- **Horizon.** Moyen terme pour un premier pôle pilote ; long terme pour un réseau.
- **Indicateurs.** Heures de calcul allouées à des acteurs africains ; taux d'utilisation ; nombre de projets soutenus.
- **Impact attendu.** Un accès abordable au calcul sans dépendre entièrement de régions cloud situées hors du continent.
- **Statut.** Proposition à tester par une étude de faisabilité (coûts, énergie, demande réelle) avant tout engagement d'investissement.

R6 — Constituer des corpus ouverts de langues et de données africaines, sous licences équitables

- **Constat.** Environ 2 % des données mondiales d'entraînement de l'IA viennent d'Afrique ; le swahili compte 710 jeux de données sur Hugging Face contre 88 844 pour l'anglais (Banque mondiale, octobre 2026). Des acteurs africains montrent la voie : Lelapa AI a publié InkubaLM, un petit modèle ouvert de 0,4 milliard de paramètres pour cinq langues africaines (Lelapa AI).
- **Enjeu.** Un modèle qui ne comprend ni le fon, ni le wolof, ni le haoussa exclut des millions de citoyens des services publics et financiers « intelligents », et reproduit des biais.
- **Recommandation.** Lancer des programmes nationaux et régionaux de collecte de données linguistiques (archives des radios publiques, débats parlementaires, contenus éducatifs) publiés sous licences garantissant un retour de valeur aux communautés.
- **Destinataires.** Ministères de la culture, de l'éducation et du numérique, médias publics, universités, académies des langues, startups.
- **Exécution.** Appels à projets ; protocole de consentement et d'anonymisation validé par l'autorité de protection des données ; licences qui facturent l'usage commercial par des acteurs non africains et réinvestissent dans la collecte.
- **Horizon.** Court terme pour le lancement ; moyen terme pour des corpus exploitables.
- **Indicateurs.** Volume de données publié par langue ; nombre de langues couvertes ; nombre de services publics disponibles en langue nationale.
- **Impact attendu.** Une IA utile en zone rurale et dans les langues réellement parlées, et un actif stratégique contrôlé par l'Afrique.

R7 — Encadrer l'IA à haut risque par les lois existantes et des bacs à sable, avant une loi générale

- **Constat.** En avril 2026, 45 pays africains avaient une loi sur les données personnelles mais seulement 16 une stratégie nationale d'IA (Algeria Tech, citant Yellow Card). Le Nigeria et le Malawi ont annoncé des bacs à sable réglementaires pour l'IA (Digital Policy Alert, 2026).
- **Enjeu.** Attendre une loi IA complète laisserait des usages à fort impact (crédit, recrutement, aides sociales, santé, sécurité) sans garde-fou pendant des années.
- **Recommandation.** Utiliser immédiatement les lois sur les données : analyse d'impact obligatoire pour les systèmes à haut risque, droit à une intervention humaine, registre public des algorithmes utilisés par l'administration. Ouvrir des bacs à sable pour tester les usages innovants sous supervision.
- **Destinataires.** Autorités de protection des données, ministères du numérique, banques centrales (notation de crédit), entreprises qui déploient des systèmes d'IA.
- **Exécution.** Lignes directrices conjointes ; modèle d'analyse d'impact algorithmique ; registre en ligne ; guichet unique pour les bacs à sable.
- **Horizon.** Court terme pour les lignes directrices ; moyen terme pour le registre.
- **Indicateurs.** Nombre d'analyses d'impact déposées ; nombre d'algorithmes publics inscrits au registre ; nombre de recours traités.
- **Impact attendu.** Une IA déployée plus vite parce qu'elle inspire confiance, et des entreprises qui savent ce que l'on attend d'elles.

Axe 3 — Faire de la souveraineté numérique une réalité économique

La souveraineté dont nous parlons n'est pas une autarcie. C'est la capacité à choisir ses partenaires, à en changer et à garder la maîtrise des décisions critiques.

R8 — Adopter une doctrine de classification des données publiques qui cible la localisation

- **Constat.** Le Kenya impose le stockage des données gouvernementales sur son territoire ; le Maroc rend obligatoire le stockage local des données sensibles ; le Ghana et le Nigeria envisagent des règles similaires (Digital Policy Alert, janvier 2026). Dans le même temps, le protocole de la ZLECAf sur le commerce numérique encadre les mesures de localisation.
- **Enjeu.** Une localisation généralisée renchérit les services et isole les marchés. Une absence de règle expose les données les plus sensibles à des juridictions étrangères.
- **Recommandation.** Classer les données publiques en trois ou quatre niveaux. Réserver l'hébergement national ou régional aux données souveraines (identité, défense, fiscalité, santé, état civil) ; autoriser le reste dans des clouds qualifiés, africains ou non, sous conditions contractuelles.
- **Destinataires.** Ministères du numérique, agences des systèmes d'information, autorités de protection des données.
- **Exécution.** Guide de classification ; inventaire des systèmes publics ; référentiel de qualification des hébergeurs ; cohérence vérifiée avec l'annexe de la ZLECAf sur les transferts de données.
- **Horizon.** Court terme pour le guide ; moyen terme pour l'inventaire complet.
- **Indicateurs.** Part des systèmes publics classifiés ; part des données souveraines hébergées sous juridiction nationale ou régionale.
- **Impact attendu.** Une souveraineté là où elle compte, sans pénaliser l'innovation ni le commerce intra-africain.

R9 — Faire de la commande publique un levier de sécurité et de production locale

- **Constat.** Le Ghana impose depuis 2023 une licence aux prestataires de cybersécurité et une accréditation aux professionnels, appliquée strictement depuis le 31 janvier 2026 (Cyber Security Authority ; Graphic). Le Bénin dispose d'un référentiel de qualification des prestataires de sécurité numérique (ASIN).
- **Enjeu.** L'État est souvent le premier acheteur de technologies. Ses marchés peuvent construire une industrie locale ou, au contraire, enfermer l'administration chez un fournisseur unique.
- **Recommandation.** Intégrer dans les marchés numériques publics : une exigence de qualification de sécurité ; des clauses de réversibilité et de portabilité des données ; un allotissement permettant aux PME locales de soumissionner, seules ou en groupement.
- **Destinataires.** Ministères des finances, autorités de régulation des marchés publics, agences numériques, acheteurs publics.
- **Exécution.** Cahiers des clauses types ; formation des acheteurs ; publication annuelle de la part des marchés numériques attribués à des entreprises locales.
- **Horizon.** Court terme pour les clauses types ; moyen terme pour la mesure.
- **Indicateurs.** Part des contrats avec clause de réversibilité ; part des montants attribués à des PME nationales ou africaines.
- **Impact attendu.** Des administrations moins captives et un marché intérieur qui fait grandir les entreprises africaines.

R10 — Négocier des partenariats technologiques avec des clauses de transfert de compétences mesurables

- **Constat.** Dans les centres de données africains, 39 % des opérateurs citent la rétention des compétences comme leur principal défi RH ; 67 % au Nigeria (TechEconomy, citant l'ADCA).
- **Enjeu.** Les grands contrats d'infrastructure (câbles, centres de données, cloud, identité) engagent pour des décennies. Mal négociés, ils importent la technologie sans les compétences.
- **Recommandation.** Inclure dans tout partenariat technologique public d'envergure des engagements chiffrés : part d'emplois techniques locaux, formation, maintenance assurée localement, documentation et accès aux journaux de sécurité. Diversifier les fournisseurs pour éviter le verrouillage.
- **Destinataires.** Gouvernements, ministères du numérique et des finances, entreprises technologiques internationales et africaines.
- **Exécution.** Grille de négociation commune partagée entre pays (par exemple sous l'égide de l'UA ou de Smart Africa) ; pénalités en cas de non-respect.
- **Horizon.** Moyen terme.
- **Indicateurs.** Part des postes techniques occupés par des nationaux trois ans après la signature ; nombre de contrats intégrant ces clauses.
- **Impact attendu.** Des investissements étrangers qui laissent derrière eux des équipes et des entreprises compétentes.

Axe 4 — Garantir la protection des données et restaurer la confiance des citoyens

R11 — Garantir l'indépendance et les moyens des autorités de protection des données PRIORITAIRE

- **Constat.** Fin 2025, 44 pays africains avaient une loi sur les données personnelles, mais six n'avaient pas de régulateur opérationnel. Les sanctions se multiplient là où les autorités ont des moyens : au Nigeria, la NDPC a infligé en février 2025 une amende de 32,8 millions de dollars à une plateforme de réseau social, réglée à l'amiable en novembre 2025 (Digital Policy Alert).
- **Enjeu.** Une loi sans régulateur crédible est une promesse non tenue envers les citoyens et un signal négatif pour les partenaires qui évaluent le niveau de protection avant d'autoriser des transferts.
- **Recommandation.** Doter chaque autorité d'un budget plancher voté par le parlement, de ressources propres (redevances, part des amendes), d'un mandat non révocable de ses dirigeants et d'effectifs techniques capables d'auditer.
- **Destinataires.** Gouvernements, parlements, ministères des finances.
- **Exécution.** Ligne budgétaire dédiée dans la loi de finances ; contrat d'objectifs et de moyens ; rapport annuel public présenté au parlement.
- **Horizon.** Court terme pour la ligne budgétaire ; moyen terme pour les effectifs cibles.
- **Indicateurs.** Budget et effectifs rapportés à la population ; nombre de contrôles ; délai moyen de traitement des plaintes.
- **Impact attendu.** Des droits effectifs, et une éligibilité renforcée aux mécanismes d'adéquation et aux flux de données internationaux.

R12 — Protéger spécifiquement les données biométriques et les registres d'identité

- **Constat.** Au Kenya, Worldcoin a collecté les données biométriques de plus de 300 000 personnes contre une rétribution en cryptomonnaie. Les activités ont été suspendues en août 2023 ; en mai 2025, la Haute Cour a ordonné la suppression des données, faute de consentement valide et d'analyse d'impact ; la suppression a été confirmée par le régulateur en janvier 2026 (TechPoint ; Dawan Africa). Dans le même temps, les États centralisent leurs registres : celui du Bénin a recensé plus de 10,3 millions de personnes.
- **Enjeu.** Une donnée biométrique compromise ne se change pas comme un mot de passe. Les registres d'identité sont des cibles de premier rang.
- **Recommandation.** Rendre obligatoires et publiques les analyses d'impact avant toute collecte biométrique ; interdire les contreparties financières à la collecte ; séparer les bases ; journaliser tous les accès ; auditer chaque année les registres nationaux par un tiers indépendant.
- **Destinataires.** Agences d'identification, ministères de l'intérieur, autorités de protection des données, opérateurs privés collectant de la biométrie (banques, télécoms).
- **Exécution.** Décret ou ligne directrice de l'autorité ; clauses dans les contrats des prestataires d'identité ; publication d'un résumé des audits.
- **Horizon.** Court terme.
- **Indicateurs.** Nombre d'analyses d'impact publiées ; incidents sur les registres ; part des accès journalisés et contrôlés.
- **Impact attendu.** Une identité numérique adoptée parce qu'elle est digne de confiance.

R13 — Ouvrir aux citoyens des voies de recours simples, mobiles et en langues nationales

- **Constat.** Les réclamations auprès des autorités passent souvent par des formulaires en ligne ou des courriers, inaccessibles à une grande partie de la population : en 2025, 21 % des ruraux africains utilisent Internet (UIT).
- **Enjeu.** Un droit que l'on ne peut pas exercer n'existe pas. La confiance naît aussi de la possibilité de se plaindre et d'obtenir réponse.
- **Recommandation.** Ouvrir des canaux de plainte par USSD, messagerie et centre d'appel, en langues nationales, avec un délai de réponse opposable. Exiger des entreprises qui traitent des données à grande échelle (télécoms, banques, plateformes) un point de contact local et un rapport annuel de transparence.
- **Destinataires.** Autorités de protection des données, opérateurs télécoms (pour les canaux USSD), associations de consommateurs.
- **Exécution.** Convention entre l'autorité et les opérateurs ; campagnes d'information ; tableau de bord public des plaintes.
- **Horizon.** Court terme.
- **Indicateurs.** Nombre de plaintes reçues par canal ; délai médian de réponse ; part de plaintes résolues.
- **Impact attendu.** Des citoyens qui passent du statut d'usagers vulnérables à celui de titulaires de droits.

Axe 5 — Faire de l'innovation africaine un moteur de croissance et de souveraineté

R14 — Lancer un programme « premier client public » pour les startups de cybersécurité et d'IA PRIORITAIRE

- **Constat.** Les startups africaines ont levé 4,1 milliards de dollars en 2025, mais l'amorçage recule : 311 tours, en baisse de 38 % par rapport au pic de 2022 (Tech In Africa, citant Partech). Les jeunes entreprises manquent surtout de premiers clients de référence.
- **Enjeu.** Un contrat avec une administration ou une grande entreprise vaut souvent plus qu'un tour de table : il valide le produit et ouvre d'autres marchés.
- **Recommandation.** Créer un programme de défis publics : une administration publie un problème réel, finance plusieurs prototypes en concurrence, puis achète la meilleure solution selon une procédure adaptée.
- **Destinataires.** Ministères du numérique et des finances, autorités des marchés publics, agences cyber, grandes entreprises publiques et privées.
- **Exécution.** Enveloppe budgétaire dédiée ; procédure d'achat d'innovation encadrée par la réglementation des marchés ; jury mixte public-privé ; HackerLab et compétitions existantes comme viviers.
- **Horizon.** Court terme pour les premiers défis ; moyen terme pour l'échelle.
- **Indicateurs.** Nombre de défis publiés ; nombre et montant des contrats signés ; chiffre d'affaires des lauréats à trois ans.
- **Impact attendu.** Des solutions conçues pour les réalités africaines et des champions locaux capables d'exporter.

R15 — Faciliter le passage à l'échelle régional par la reconnaissance mutuelle des bacs à sable

- **Constat.** Plusieurs régulateurs ont ouvert des bacs à sable (fintech, IA), mais chacun dans son périmètre national. Une startup qui a fait ses preuves à Kigali, Lagos ou Abidjan recommence à zéro ailleurs.
- **Enjeu.** La fragmentation réglementaire est l'une des raisons pour lesquelles le capital se concentre sur quatre grands marchés.
- **Recommandation.** Créer un « passeport réglementaire » : une entreprise admise et suivie dans le bac à sable d'un pays bénéficie d'une procédure accélérée dans les pays signataires.
- **Destinataires.** Banques centrales, régulateurs télécoms et des données, secrétariat de la ZLECAf, communautés économiques régionales.
- **Exécution.** Accord pilote entre trois ou quatre régulateurs volontaires ; critères communs ; extension progressive.
- **Horizon.** Moyen terme.
- **Indicateurs.** Nombre de startups opérant dans au moins trois pays ; délai moyen d'obtention d'une autorisation dans un second pays.
- **Impact attendu.** Des marchés régionaux réellement accessibles aux entreprises africaines.

Axe 6 — Développer une cyberdiplomatie et une coopération panafricaines fortes

R16 — Accélérer la ratification de la Convention de Malabo et l'entraide judiciaire opérationnelle

- **Constat.** La Convention de Malabo, adoptée en 2014, n'est entrée en vigueur que le 8 juin 2023 avec 15 ratifications sur 55 États ; Chatham House notait début 2024 une seule ratification supplémentaire depuis (Chatham House). Selon INTERPOL (2025), 86 % des pays jugent la coopération internationale entravée par la bureaucratie (PR Nigeria).
- **Enjeu.** Les cybercriminels opèrent sans frontières ; les enquêtes, elles, s'arrêtent à chaque frontière.
- **Recommandation.** Lancer une campagne de ratification assortie d'un calendrier, actualiser le texte par un protocole additionnel (IA, cryptoactifs, preuve électronique) et créer un réseau de points de contact judiciaires disponibles 24 heures sur 24.
- **Destinataires.** Ministères des affaires étrangères et de la justice, parlements, Commission de l'UA, AFRIPOL.
- **Exécution.** Feuille de route portée au Sommet de l'UA ; assistance technique pour la transposition ; modèles de demandes d'entraide standardisés.
- **Horizon.** Moyen terme.
- **Indicateurs.** Nombre de ratifications ; délai médian de traitement des demandes d'entraide ; nombre d'opérations conjointes.
- **Impact attendu.** Moins d'impunité, donc moins d'attractivité du continent pour les réseaux criminels.

R17 — Connecter les CSIRT nationaux à un dispositif africain de partage d'information sur les menaces PRIORITAIRE

- **Constat.** Seuls 19 % des pays africains disposent d'une base de données sur les cybermenaces (INTERPOL, 2025). L'UA a créé un groupe d'experts en cybersécurité (AUCSEG) pour conseiller la Commission (UA), et son Conseil de paix et de sécurité a adopté en 2024 une position africaine commune sur l'application du droit international au cyberespace (Chatham House).
- **Enjeu.** Une attaque détectée à Nairobi le lundi peut frapper Cotonou le mardi. Le partage rapide des indicateurs est la mesure la moins coûteuse et la plus rentable.
- **Recommandation.** Signer un protocole de partage entre CSIRT nationaux et sectoriels, opéré sur une plateforme commune, avec un bulletin africain de menaces et des niveaux de confidentialité clairs.
- **Destinataires.** Agences nationales de cybersécurité, CSIRT, Commission de l'UA, communautés économiques régionales, opérateurs vitaux.
- **Exécution.** Accord-cadre de partage ; s'appuyer sur les réseaux existants de CSIRT africains ; financement de lancement par les partenaires au développement.
- **Horizon.** Court terme pour le protocole ; moyen terme pour la plateforme.
- **Indicateurs.** Nombre de CSIRT connectés ; volume d'indicateurs partagés ; délai entre première détection et alerte régionale.
- **Impact attendu.** Une défense collective plus rapide que l'attaque.

Axe 7 — Protéger l'espace informationnel et combattre la désinformation

R18 — Créer des cellules indépendantes de réponse aux crises informationnelles, avec un protocole électoral

- **Constat.** L'Africa Center for Strategic Studies a documenté 189 campagnes de désinformation en 2023, près de quatre fois plus qu'en 2022 ; au moins 39 pays ont été ciblés et l'Afrique de l'Ouest concentre près de 40 % des campagnes (ACSS ; Mmegi). Les deepfakes abaissent encore le coût de la manipulation.
- **Enjeu.** La désinformation fragilise la confiance dans les institutions, les élections et les campagnes de santé publique. Mais une réponse autoritaire, comme les coupures d'Internet, détruit la confiance qu'elle prétend protéger.
- **Recommandation.** Mettre en place, dans chaque pays, une cellule associant régulateur des médias, organe de gestion des élections, fact-checkers et chercheurs, dotée d'un protocole public : détection, qualification, réponse par l'information, jamais par la censure générale. S'interdire les coupures d'Internet comme outil de gestion de crise.
- **Destinataires.** Régulateurs des médias, commissions électorales, ministères de la communication, médias, organisations de vérification, plateformes.
- **Exécution.** Charte d'indépendance ; financement mixte ; rapport public après chaque élection ; liens avec les centres de recherche.
- **Horizon.** Court terme dans les pays à échéance électorale proche ; moyen terme ailleurs.
- **Indicateurs.** Délai médian entre détection et réponse publique ; nombre de campagnes documentées ; nombre de coupures d'Internet (objectif : zéro).
- **Impact attendu.** Un espace public plus résistant, sans sacrifier la liberté d'expression.

R19 — Obtenir des plateformes une transparence effective et généraliser l'éducation aux médias

- **Constat.** Les grandes plateformes publient peu de données par pays africain sur la modération, la publicité politique ou les moyens consacrés aux langues africaines. Isolément, un État a peu de poids pour les obtenir.
- **Enjeu.** Sans données, ni les régulateurs ni les chercheurs ne peuvent mesurer les risques ; sans éducation, les citoyens restent désarmés.
- **Recommandation.** Négocier collectivement (UA ou communautés régionales) un socle d'obligations : rapports de transparence par pays et par langue, bibliothèque des publicités politiques, accès encadré des chercheurs aux données. Intégrer l'éducation aux médias et à l'information, y compris aux contenus générés par l'IA, dans les programmes scolaires.
- **Destinataires.** Commission de l'UA, communautés économiques régionales, régulateurs, plateformes, ministères de l'éducation.
- **Exécution.** Mandat de négociation commun ; code de conduite assorti d'un calendrier ; modules scolaires conçus avec des enseignants et des journalistes.
- **Horizon.** Moyen terme.
- **Indicateurs.** Nombre de plateformes publiant des rapports par pays ; part des élèves ayant suivi un module d'éducation aux médias.
- **Impact attendu.** Un rapport de force plus équilibré avec les plateformes et une génération plus vigilante.

Axe 8 — Financer la transformation numérique et mobiliser les capitaux

R20 — Réserver une part fixe de chaque projet numérique public à la sécurité et à l'exploitation

- **Constat.** Les projets numériques publics financent volontiers le déploiement initial, beaucoup moins la sécurité, la maintenance et les compétences qui les font durer. Le rapport du bjCSIRT pointe des failles récurrentes (contrôle d'accès, injection SQL, authentification) qui relèvent de cette sous-maintenance.
- **Enjeu.** Un service public numérique non sécurisé devient un passif : fuite de données, interruption, perte de confiance.
- **Recommandation.** Imposer qu'une part minimale de chaque projet numérique public, et des financements de bailleurs, soit affectée à la sécurité, aux audits et à l'exploitation sur la durée de vie du système. Nous proposons 10 % comme point de départ, à ajuster par étude.
- **Destinataires.** Ministères des finances, agences numériques, Banque mondiale, Banque africaine de développement, bailleurs bilatéraux.
- **Exécution.** Circulaire budgétaire ; clause type dans les accords de financement ; contrôle par les inspections des finances.
- **Horizon.** Court terme.
- **Indicateurs.** Part des projets respectant la règle ; part du budget effectivement consommée pour la sécurité.
- **Impact attendu.** Des investissements numériques qui produisent des services durables plutôt que des vulnérabilités.
- **Statut.** Le taux de 10 % est une hypothèse de travail de 50Afrique et d'Afropreneurs Emerging Leaders.

R21 — Mobiliser l'épargne longue africaine vers le capital patient technologique, avec partage des risques

- **Constat.** En 2025, la dette a représenté 41 % des financements des startups africaines et quatre pays ont capté 72 % des montants (Techloy ; Tech In Africa). Les investisseurs institutionnels africains restent peu présents dans le capital-risque.
- **Enjeu.** Les entreprises de cybersécurité, d'IA ou d'infrastructure ont besoin de capitaux longs. Dépendre surtout de capitaux étrangers expose aux cycles des marchés mondiaux.
- **Recommandation.** Créer des fonds de fonds régionaux dédiés aux technologies stratégiques, combinant capitaux publics, institutions de développement et épargne longue africaine (fonds de pension, assureurs), avec une première perte absorbée par des fonds publics ou concessionnels. Adapter, là où elles sont restrictives, les règles d'allocation des investisseurs institutionnels.
- **Destinataires.** Ministères des finances, régulateurs des pensions et des assurances, BAD, Afreximbank, IFC, fonds souverains, gestionnaires de fonds africains.
- **Exécution.** Structuration par une institution de développement ; gestionnaires sélectionnés par appel d'offres ; exigence de maturité cyber dans les due diligences.
- **Horizon.** Moyen terme.
- **Indicateurs.** Montants levés auprès d'investisseurs institutionnels africains ; nombre d'entreprises financées hors des quatre grands marchés.
- **Impact attendu.** Un financement plus stable et mieux réparti, au service d'entreprises stratégiques africaines.

Axe 9 — Faire du capital humain le socle de la confiance numérique

R22 — Créer des académies cyber et IA à vocation régionale, avec au moins 30 % de femmes PRIORITAIRE

- **Constat.** Les femmes ne représentent que 13,5 % des effectifs de la cybersécurité en Afrique, la part la plus faible au monde (IT-Online, citant BCG et GCF). Des modèles existent : l'École nationale de cybersécurité à vocation régionale de Dakar (2018, coopération franco-sénégalaise), le HackerLab de l'ASIN au Bénin, Cyber Shujaa au Kenya, le programme 3MTT au Nigeria, qui a formé près de 300 000 personnes fin 2025 (TechEconomy). Au Kenya, les employeurs peinent pourtant à recruter faute de compétences pratiques (The Standard).
- **Enjeu.** Former en masse ne suffit pas : il faut des profils opérationnels, et inclure la moitié de la population aujourd'hui sous-représentée.
- **Recommandation.** Créer ou renforcer, par grande région, des académies associant État, universités et entreprises, fondées sur l'alternance, la certification et les cas réels, avec un objectif d'au moins 30 % de femmes par cohorte.
- **Destinataires.** Ministères de l'enseignement supérieur, du numérique et de l'emploi, universités, entreprises employeuses, partenaires techniques et financiers.
- **Exécution.** Mutualisation entre pays d'une même région ; financement partagé (État, entreprises, bailleurs) ; engagement d'embauche des entreprises partenaires ; bourses réservées aux femmes.
- **Horizon.** Court terme pour la première cohorte ; long terme pour le réseau.
- **Indicateurs.** Nombre de certifiés ; taux d'insertion à six mois ; part des femmes ; part des diplômés employés sur le continent à trois ans.
- **Impact attendu.** Des équipes capables de défendre les systèmes africains et des emplois qualifiés pour la jeunesse.

R23 — Former les décideurs et mobiliser la diaspora par des missions d'expertise courtes

- **Constat.** Les décisions clés (budgets, contrats, crises) sont prises par des ministres, des directeurs généraux, des administrateurs, des magistrats, souvent peu formés aux enjeux numériques. L'ENC-VR de Dakar forme déjà des hauts fonctionnaires à la cyberdiplomatie (Osiris). La diaspora africaine compte de nombreux experts qui ne demandent qu'un cadre pour contribuer.
- **Enjeu.** La fuite des compétences ne se combat pas seulement en retenant : on peut aussi faire circuler.
- **Recommandation.** Instaurer un cursus court obligatoire pour les nouveaux ministres, directeurs généraux d'établissements publics et administrateurs de sociétés réglementées. Créer un statut d'« expert associé » permettant à des professionnels de la diaspora d'effectuer des missions de quelques semaines auprès d'administrations et d'agences.
- **Destinataires.** Gouvernements, écoles d'administration, régulateurs financiers, organisations de la diaspora, employeurs.
- **Exécution.** Modules de deux à trois jours ; vivier d'experts référencés ; prise en charge des frais par l'administration d'accueil ; clauses de confidentialité.
- **Horizon.** Court terme.
- **Indicateurs.** Nombre de décideurs formés ; nombre de missions d'experts réalisées ; satisfaction des administrations d'accueil.
- **Impact attendu.** De meilleures décisions plus tôt, et une diaspora qui devient une ressource stratégique.

Axe 10 — Construire une économie numérique panafricaine interopérable et inclusive

R24 — Rendre les identités numériques interopérables et mutuellement reconnues

- **Constat.** Le protocole de la ZLECAf sur le commerce numérique a été adopté en février 2024 et ses huit annexes, dont celles sur l'identité numérique et les transferts de données, en février 2025 ; le protocole n'est pas encore entré en vigueur (Mondaq ; Further Africa). En Afrique de l'Ouest, le Bénin construit son identité fondationnelle (NPI, RNPP) dans le cadre du projet régional WURI.
- **Enjeu.** Sans identité reconnue au-delà des frontières, l'ouverture d'un compte, la signature d'un contrat ou une vérification KYC restent nationales, et le marché unique reste théorique.
- **Recommandation.** Ratifier le protocole et ses annexes ; adopter des standards ouverts communs ; organiser la reconnaissance mutuelle des identités et des signatures électroniques, en commençant par des corridors pilotes.
- **Destinataires.** Agences d'identification, ministères du commerce et du numérique, secrétariat de la ZLECAf, banques centrales, autorités de protection des données.
- **Exécution.** Corridor pilote entre deux ou trois pays aux systèmes compatibles ; cas d'usage prioritaires (ouverture de compte, création d'entreprise) ; contrôle par les autorités de protection des données.
- **Horizon.** Moyen terme pour les pilotes ; long terme pour la généralisation.
- **Indicateurs.** Nombre de ratifications ; nombre de corridors opérationnels ; nombre de vérifications transfrontalières réalisées.
- **Impact attendu.** Une mobilité économique réelle pour les citoyens, les commerçants et les PME.

R25 — Connecter le mobile money et les PME aux paiements transfrontaliers, et reconnaître mutuellement les certifications

- **Constat.** L'Afrique subsaharienne compte 1,2 milliard de comptes de mobile money en 2025 (GSMA). Le système panafricain de paiement et de règlement PAPSS connectait 30 pays en novembre 2026 et vise environ 38 pays d'ici la fin de l'année (The Guardian Nigeria). Les PME restent pourtant mal reliées à ces infrastructures.
- **Enjeu.** Les paiements transfrontaliers en monnaies locales réduisent les coûts du commerce intra-africain. Leur sécurité est une condition de leur adoption.
- **Recommandation.** Raccorder les opérateurs de mobile money et les systèmes de paiement instantané nationaux à PAPSS ; exiger un niveau de sécurité commun (authentification, détection de fraude) ; reconnaître mutuellement les qualifications des prestataires de cybersécurité entre pays partenaires pour que les PME puissent acheter des services sécurisés au-delà de leurs frontières.
- **Destinataires.** Banques centrales, PAPSS et Afreximbank, opérateurs de mobile money, agences cyber, organisations patronales de PME.
- **Exécution.** Feuille de route de raccordement ; référentiel de sécurité commun ; accord de reconnaissance mutuelle des qualifications ; programmes d'accompagnement des PME.
- **Horizon.** Moyen terme.
- **Indicateurs.** Nombre d'opérateurs de mobile money raccordés ; volume de paiements transfrontaliers des PME ; taux de fraude.
- **Impact attendu.** Des PME qui vendent dans la région aussi simplement que dans leur ville.

Matrice des responsabilités par catégorie de décideurs

Chaque catégorie pilote quelques recommandations et contribue à d'autres ; la dernière colonne propose l'engagement que chacune peut annoncer publiquement, avec sa preuve.

Catégorie	Pilote	Contribue	Engagement à annoncer	Preuve attendue
Gouvernements	R1, R11, R16, R20	R3, R5, R8, R22, R23, R24	Décret sur les opérateurs vitaux et budget plancher pour l'autorité de protection des données	Textes publiés, ligne budgétaire votée
Ministères (numérique, finances, commerce, recherche)	R8, R9, R14	R5, R6, R10, R21, R24	Clauses types de sécurité et de réversibilité ; premiers défis « premier client public »	Cahier des clauses publié, défis lancés
Régulateurs et autorités de protection des données	R7, R12, R13	R4, R11, R15, R19	Lignes directrices sur l'IA à haut risque et canal de plainte mobile	Lignes directrices publiées, tableau de bord des plaintes
Agences de cybersécurité et défense	R2, R3, R17	R1, R9, R22, R25	Exercice national de crise et adhésion au partage africain de menaces	Rapport d'exercice, protocole signé
Banques, institutions financières, opérateurs de paiement	R25	R2, R4, R21	Participation à un SOC ou ISAC sectoriel ; raccordement à PAPSS	Convention d'adhésion, raccordement effectif
Télécommunications et infrastructures	—	R1, R3, R5, R10, R13	Plans de continuité testés ; canaux USSD pour les plaintes	Test annuel documenté, canal ouvert

Catégorie	Pilote	Contribue	Engagement à annoncer	Preuve attendue
Entreprises technologiques	—	R6, R10, R19, R22	Transfert de compétences chiffré ; rapports de transparence par pays	Rapport annuel d'emplois locaux
Investisseurs et institutions financières internationales	R21	R5, R14, R20	Clause de maturité cyber dans les due diligences ; contribution à un fonds de fonds	Politique d'investissement publiée
Organisations panafricaines et partenaires	R19, R24	R5, R10, R15, R16, R17	Feuille de route de ratification (Malabo, protocole ZLECAf)	Calendrier adopté, rapports d'étape
Universités et centres de recherche	R6	R5, R22	Corpus linguistiques ouverts ; cursus en alternance	Jeux de données publiés, cohortes lancées
Entrepreneurs et startups	—	R14, R15, R25	Solutions certifiées, sécurité dès la conception	Certifications obtenues
Jeunesse africaine	—	R18, R22, R23	Participation aux instances de suivi et aux cellules de réponse informationnelle	Sièges réservés, contributions publiées
Commissions électorales et régulateurs des médias	R18	R19	Protocole public de réponse aux crises informationnelles	Protocole publié avant le prochain scrutin

Catégorie	Pilote	Contribue	Engagement à annoncer	Preuve attendue
Parlements	—	R11, R16	Vote des moyens des régulateurs et des ratifications	Lois votées
Entreprises (directions générales et conseils)	R4	R2, R23	Revue annuelle du risque cyber par le conseil	Mention au rapport annuel

Feuille de route de mise en œuvre : 12 mois, 3 ans, 5 ans

Les douze premiers mois concentrent les décisions peu coûteuses et à fort effet : textes, budgets plancher, protocoles, premières cohortes. Les investissements lourds viennent ensuite, une fois les capacités de pilotage en place.

Poser les bases

0-12 mois · 2026-2027

R1 · Décret opérateurs vitaux

R11 · Budget plancher des APD

R14 · Premiers défis publics

R17 · Partage entre CSIRT

R22 · Première cohorte

R3 · Premier exercice de crise

R20 · Règle des 10 % sécurité

R7 R12 R13 · Lignes directrices

R6 · Lancement des corpus

◆ **CAF 2027 · 1er rapport de l'Observatoire**

Construire les capacités

1-3 ans · 2027-2029

R2 · SOC sectoriels mutualisés

R4 · Cyber au conseil

R5 · Pilote de calcul régional

R8 · Classification des données

R9 R10 · Clauses contractuelles

R15 · Passeport réglementaire

R16 · Ratifications Malabo

R21 · Fonds de fonds régional

R24 R25 · Corridors pilotes

◆ **Année 3 · Revue à mi-parcours**

Passer à l'échelle

3-5 ans · 2029-2031

R5 · Réseau de pôles de calcul

R6 · Corpus exploitables

R22 · Académies en réseau

R24 · Identités reconnues

R25 · Paiements PME généralisés

R18 R19 · Plateformes et écoles

Toutes · Évaluation indépendante

◆ **Année 5 · Évaluation finale**

En gras : les cinq engagements prioritaires.

Chaque phase se clôt sur un jalon public : le rapport de l'Observatoire à la 7e édition du Forum, une revue à mi-parcours en année 3, une évaluation indépendante en année 5. Les pays avancent à leur rythme : un pays déjà doté d'une agence cyber mature peut entamer la phase 2 dès la première année.

Mécanisme de suivi et d'évaluation

Nous proposons un suivi public, indépendant et annuel des 25 recommandations, restitué à chaque édition du Cyber Africa Forum.

Principes. Peu d'indicateurs, mais stables d'une année sur l'autre. Des sources vérifiables (textes publiés, rapports d'autorités, données UIT, INTERPOL, GSMA, Banque mondiale). Une distinction nette entre ce qui est annoncé, adopté, financé et effectivement mis en œuvre.

L'échelle de progression. Chaque recommandation est notée, pays par pays, sur cinq niveaux :

1. Annoncée : engagement public sans texte.
2. Adoptée : texte, décision ou contrat signé.
3. Financée : ressources inscrites au budget ou mobilisées.
4. Opérationnelle : dispositif en fonctionnement, premiers résultats mesurés.
5. Évaluée : effets mesurés par un tiers et rendus publics.

Tableau de bord resserré : dix indicateurs de tête.

Indicateur	Recommandation	Source envisagée
Pays ayant désigné leurs opérateurs vitaux et rendu la notification obligatoire	R1	Journaux officiels, agences cyber
Délai médian entre détection d'un incident majeur et notification	R1, R17	CSIRT nationaux
CSIRT connectés au dispositif africain de partage	R17	Commission de l'UA, réseaux de CSIRT
Budget et effectifs des autorités de protection des données par million d'habitants	R11	Rapports annuels des autorités
Analyses d'impact publiées avant collecte biométrique	R12	Autorités de protection des données
Contrats signés via les programmes « premier client public »	R14	Ministères, autorités des marchés publics
Ratifications de la Convention de Malabo et du protocole ZLECAf sur le commerce numérique	R16, R24	Commission de l'UA, secrétariat de la ZLECAf
Certifiés des académies cyber et IA, dont part de femmes et taux d'insertion	R22	Académies, employeurs
Coupures d'Internet décidées par des autorités	R18	Observatoires de la société civile
Opérateurs de mobile money raccordés aux paiements transfrontaliers	R25	PAPSS, banques centrales

Gouvernance du suivi. L'Observatoire panafricain de la confiance numérique (voir initiative 1) produit le rapport. Un comité scientifique indépendant valide la méthode. Les États et institutions concernés disposent d'un droit de réponse publié avec le rapport.

Calendrier. Premier état des lieux à six mois ; rapport complet à la 7e édition du Forum ; revue à mi-parcours à trois ans ; évaluation d'ensemble à cinq ans.

Limite assumée. Les données africaines sur les incidents et les compétences restent lacunaires. Le suivi commencera par les pays volontaires et s'élargira ; un pays sans données sera signalé comme

tel, jamais estimé.

Trois initiatives structurantes portées par 50Afrique et Afropreneurs Emerging Leaders

Nous ne voulons pas seulement recommander ; nous proposons de porter trois initiatives à la suite du Forum. Les partenaires cités sont des partenaires à solliciter : aucun n'est engagé à ce stade.

Initiative 1 — L'Observatoire panafricain de la confiance numérique

- **Objet.** Suivre chaque année, pays par pays, la mise en œuvre des 25 recommandations et publier un tableau de bord ouvert (voir le mécanisme de suivi).
- **Pourquoi nous.** Un think tank indépendant et un mouvement de jeunes leaders peuvent mesurer sans être juge et partie, et mobiliser des contributeurs dans de nombreux pays.
- **Gouvernance.** Secrétariat assuré par 50Afrique ; comité scientifique d'universitaires et d'experts africains indépendants ; correspondants nationaux issus du réseau Afropreneurs Emerging Leaders ; charte d'indépendance interdisant tout financement exclusif par une entité évaluée.
- **Partenaires à solliciter.** Universités et centres de recherche africains, réseaux de CSIRT, autorités de protection des données volontaires, médias spécialisés, organisateurs du Cyber Africa Forum pour la restitution annuelle.
- **Modèle de financement.** Fondations et partenaires au développement pour le socle ; mécénat d'entreprises plafonné par contributeur ; études approfondies financées à la demande, sans incidence sur la notation.
- **Premiers résultats attendus.** Une méthodologie publiée à trois mois ; un premier état des lieux sur une dizaine de pays volontaires, couvrant aires francophone, anglophone et lusophone, à six mois ; un rapport complet à la 7ᵉ édition du Forum.

Initiative 2 — Le Pacte des dirigeants pour la cyber-résilience

- **Objet.** Réunir des directions générales publiques et privées autour d'engagements volontaires, simples et vérifiables : authentification forte généralisée, sauvegardes hors ligne testées, exercice de crise annuel au niveau de la direction générale, formation du conseil, participation au partage d'information sectoriel.
- **Pourquoi ça peut marcher.** Les engagements sont peu coûteux mais très efficaces, et leur publication crée une émulation entre pairs.
- **Gouvernance.** Comité de pilotage paritaire public-privé ; 50Afrique et Afropreneurs Emerging Leaders assurent l'animation ; vérification par auto-évaluation renforcée, puis par audit tiers pour les signataires volontaires.
- **Partenaires à solliciter.** Agences nationales de cybersécurité, associations professionnelles des banques, des télécoms et des assureurs, organisations patronales, prestataires qualifiés.
- **Modèle de financement.** Cotisation modeste des signataires, modulée selon leur taille ; partenaires pour les outils et formations.
- **Premiers résultats attendus.** Une charte publiée et des premiers signataires dans les douze mois ; un rapport annuel publiant le taux de respect des engagements.

Initiative 3 — Le programme Afropreneurs Cyber & IA Leaders

- **Objet.** Former chaque année une cohorte de jeunes professionnels africains de la cybersécurité et de l'IA au leadership, à la gouvernance et à l'entrepreneuriat, en les confrontant à des cas réels soumis par des administrations et des entreprises.
- **Ce qui le distingue.** Il ne double pas les formations techniques existantes (HackerLab, 3MTT, Cyber Shujaa, ENC-VR) : il s'appuie sur leurs meilleurs profils pour former les futurs responsables de la sécurité, fondateurs et décideurs. Objectif d'au moins 40 % de femmes.
- **Gouvernance.** Porté par Afropreneurs Emerging Leaders ; comité pédagogique associant praticiens africains et experts de la diaspora ; sélection sur dossier et mise en situation.
- **Partenaires à solliciter.** Agences cyber organisatrices de compétitions, universités, entreprises accueillant des projets, experts de la diaspora mentors, fonds d'amorçage pour les projets entrepreneuriaux.
- **Modèle de financement.** Bourses financées par des entreprises et des fondations ; contribution des administrations bénéficiaires des projets ; gratuité pour les lauréats.
- **Premiers résultats attendus.** Une cohorte pilote dans les douze mois ; des projets livrés à des administrations ; un suivi des parcours à deux ans (postes à responsabilité, entreprises créées).

Statut. Les objectifs chiffrés (40 % de femmes, une dizaine de pays pilotes) sont des cibles proposées par 50Afrique et Afropreneurs Emerging Leaders, à confirmer avec les partenaires.

Échos du Forum : déclarations, propositions et analyse

Section enrichie au fil du Forum (16 et 17 novembre 2026). Dernière mise à jour : 17 novembre 2026, cérémonie d'ouverture et panel sur l'investissement numérique. Les propos sont rapportés d'après le compte rendu de la cérémonie, et non cités mot pour mot.

Les déclarations et engagements annoncés

Cérémonie d'ouverture — lundi 16 novembre 2026, Dôme du Sofitel Cotonou

La 6e édition du Cyber Africa Forum s'est ouverte lundi 16 novembre au Dôme du Sofitel Cotonou, sous le thème « Construire la confiance numérique de demain ». Cette édition entend faire de la cybersécurité, de la souveraineté numérique et de l'innovation des leviers essentiels du développement du continent.



Ouverture de la cérémonie au Dôme du Sofitel Cotonou, 16 novembre 2026.



L'assistance lors de la cérémonie d'ouverture.

Allocution de Franck Kié, Commissaire général du Cyber Africa Forum. Il a rappelé l'ambition portée par le Forum depuis 2020 : faire de l'Afrique un acteur majeur des réflexions et des décisions qui façonnent l'avenir numérique mondial. Il a surtout insisté sur la nécessité de transformer les échanges et les partenariats en projets concrets au service de la souveraineté numérique africaine.



Franck Kié, Commissaire général du Cyber Africa Forum, lors de son allocution d'ouverture.

Allocution de Mahuna Akplogan, ministre de la Transformation digitale et de l'Innovation du Bénin. Le ministre a présenté la confiance numérique comme reposant sur trois piliers : le citoyen, l'État et les talents. Il a appelé à mieux protéger les utilisateurs, à renforcer les dispositifs de cybersécurité et à offrir aux jeunes compétences africaines des perspectives professionnelles sur le continent.



Mahuna Akplogan, ministre de la Transformation digitale et de l'Innovation du Bénin.



Au premier rang de la cérémonie d'ouverture.

Les propositions issues des panels

Panel « Capitaux, risques et opportunités : où en est l'investissement numérique en Afrique ? »

Intervenants. Marc Wabi, Isabelle Djeni, Charles Kié, Eugène Saint-Grégoire, Ghislaine T. Samaké et Stanislas Zézé.

Ce qui a été dit. Le panel a porté sur les perspectives de croissance de l'investissement numérique en Afrique et sur les défis de son financement. Trois messages ressortent :

1. **Mobiliser les capitaux locaux.** Les acteurs africains doivent mieux mobiliser l'épargne et les capitaux du continent pour financer leurs secteurs stratégiques, en particulier la technologie et les infrastructures.
2. **Intégrer le risque cyber dans la décision d'investir.** Les intervenants ont insisté sur l'authentification multifacteur, les sauvegardes des données et l'audit des fournisseurs technologiques, pour mieux anticiper les risques liés aux investissements numériques.
3. **Changer d'échelle.** Il faut développer des projets structurants et transnationaux, capables d'attirer des financements importants.

Notre analyse du panel

Le panel confirme trois de nos partis pris, et pose une question qu'il faudra trancher.

Le capital local, condition de l'autonomie. L'appel à mobiliser les capitaux africains rejoint notre recommandation R21 : orienter l'épargne longue (fonds de pension, assureurs) vers le capital patient technologique, avec une première perte absorbée par des fonds publics ou concessionnels. Le constat chiffré est connu : en 2025, quatre pays ont capté 72 % des fonds levés par les startups africaines, et la dette a représenté 41 % des financements. Sans capitaux africains, la carte de l'innovation restera concentrée.

L'hygiène cyber devient un critère d'investissement. Les trois mesures citées par le panel (authentification multifacteur, sauvegardes, audit des fournisseurs) sont exactement le socle que nous proposons d'imposer aux opérateurs d'importance vitale (R1) et les engagements du Pacte des dirigeants pour la cyber-résilience (initiative 2). Nous en tirons une proposition concrète pour les investisseurs : intégrer une clause de maturité cyber dans toutes les due diligences, comme le prévoit la matrice des responsabilités. L'audit des fournisseurs renvoie aussi à nos clauses contractuelles (R9 et R10).

Changer d'échelle passe par la mutualisation. Les projets transnationaux appelés de ses vœux par le panel existent déjà dans notre feuille de route : SOC sectoriels et régionaux (R2), communs de calcul pour l'IA (R5), corridors d'identité et de paiement (R24 et R25). Ce sont des projets de taille suffisante pour intéresser les institutions de développement et les fonds d'infrastructure.

La question à trancher : qui porte le premier risque ? Mobiliser l'épargne locale vers des actifs technologiques jugés risqués suppose un mécanisme de partage des risques. Notre position : des garanties ou une première perte apportées par les États et les institutions de développement, en échange de règles de gouvernance et de sécurité exigeantes. C'est le sens du couple R20 (une part fixe des projets publics réservée à la sécurité) et R21 (le capital patient).

Message du panel	Nos recommandations	Engagement que nous proposons
Mobiliser les capitaux locaux	R21	Fonds de fonds régionaux ouverts aux fonds de pension et assureurs africains, avec première perte publique
MFA, sauvegardes, audit des fournisseurs	R1, R4, R9, R10, initiative 2	Clause de maturité cyber dans les due diligences ; adhésion au Pacte des dirigeants
Projets structurants et transnationaux	R2, R5, R24, R25	Un premier projet régional pilote, financé en partenariat public-privé

Les propos du panel sont rapportés d'après le compte rendu de la session, non cités mot pour mot. Les chiffres de 2025 proviennent du rapport Partech cité dans le diagnostic.

Notre lecture : convergences et écarts avec nos 25 recommandations

Première lecture après la cérémonie d'ouverture, à compléter à la clôture du Forum.

Des projets plutôt que des déclarations. L'appel de Franck Kié à convertir les partenariats en projets concrets rejoint le point de départ de notre contribution : l'écart entre les textes et l'exécution. C'est précisément ce que l'Observatoire panafricain de la confiance numérique (initiative 1) propose de mesurer, en distinguant ce qui est annoncé, adopté, financé et opérationnel.

Trois piliers qui recoupent nos axes. Les trois piliers posés par le ministre Akplogan correspondent à des recommandations précises :

Pilier énoncé à l'ouverture	Recommandations correspondantes	Ce qu'elles ajoutent
Le citoyen : mieux protéger les utilisateurs	R11, R12, R13 (données), R18, R19 (espace informationnel)	Des régulateurs dotés de moyens, une protection renforcée de la biométrie, des recours accessibles par mobile et en langues nationales
L'État : renforcer les dispositifs de cybersécurité	R1 à R4 (cybersécurité), R8 à R10 (souveraineté économique), R17	Un socle opposable pour les opérateurs vitaux, des SOC mutualisés, des exercices de crise, le partage africain des menaces
Les talents : des perspectives sur le continent	R22, R23	Des académies avec engagement d'embauche, un indicateur de rétention à trois ans, des missions courtes pour la diaspora

Ce que nous suivrons d'ici la clôture. Des engagements datés et chiffrés : des budgets, des textes, des calendriers. C'est à cette aune que nous mesurerons la traduction des intentions exprimées à l'ouverture.

Appel à l'action

Nous demandons à chaque catégorie d'acteurs présente à Cotonou de repartir avec un engagement daté et vérifiable, plutôt qu'avec une déclaration de plus.

- **Aux chefs d'État et aux gouvernements** : désignez vos opérateurs vitaux, donnez à vos autorités de protection des données les moyens de leur indépendance, ratifiez les instruments continentaux que vous avez contribué à écrire.
- **Aux régulateurs** : publiez vos plans de contrôle, ouvrez des canaux de plainte accessibles, coopérez avec vos homologues pour reconnaître mutuellement ce qui peut l'être.
- **Aux agences de cybersécurité** : organisez l'exercice de crise de l'année prochaine dès maintenant, et rejoignez le partage africain d'information sur les menaces.
- **Aux dirigeants d'entreprise** : inscrivez le risque cyber à l'ordre du jour de votre conseil, et rejoignez le Pacte des dirigeants pour la cyber-résilience.
- **Aux investisseurs et institutions financières** : intégrez la maturité cyber dans vos due diligences, et engagez du capital patient au-delà des quatre grands marchés.
- **Aux entreprises technologiques** : chiffrez vos engagements d'emplois et de compétences locales, et publiez-les.
- **Aux universités** : ouvrez vos données linguistiques, construisez des cursus en alternance avec les employeurs.
- **Aux entrepreneurs** : concevez sûr dès le départ, et répondez aux défis publics.
- **À la jeunesse africaine** : exigez votre place dans les instances qui décident de votre avenir numérique, et préparez-vous à les diriger.

Conclusion : maîtriser plutôt que subir

La confiance numérique sera l'un des grands facteurs de différenciation entre les économies africaines qui subiront les transformations technologiques et celles qui sauront les maîtriser pour créer de la valeur, protéger leurs populations et renforcer leur puissance économique.

Cette différenciation ne dépendra pas d'abord de la taille des pays ou de leur richesse. Le Rwanda et Maurice ont montré qu'un État de taille modeste peut se hisser parmi les plus avancés du monde en matière de cybersécurité. Elle dépendra de la constance : budgets maintenus, équipes fidélisées, engagements suivis.

L'Afrique n'a pas à choisir entre ouverture et souveraineté, entre innovation et protection. Elle doit apprendre à tenir les deux, avec lucidité sur ses contraintes et ambition sur ses capacités. C'est le sens de ces 25 recommandations.

50Afrique et Afropreneurs Emerging Leaders prennent un engagement simple : revenir devant le Forum, l'an prochain, avec les résultats. Ce qui aura été fait, ce qui ne l'aura pas été, et pourquoi.

Annexes

Annexe A — Récapitulatif des 25 recommandations

N°	Recommandation	Axe	Horizon	Pilote principal
R1 ★	Désigner les opérateurs d'importance vitale et leur imposer un socle de sécurité opposable	1	Court puis moyen terme	Gouvernements, agences cyber
R2	Mutualiser des SOC sectoriels et régionaux	1	Moyen terme	Agences cyber, banques centrales
R3	Organiser chaque année des exercices de crise cyber nationaux et transfrontaliers	1	Court terme	Agences cyber
R4	Rendre les conseils d'administration comptables du risque cyber	1	Moyen terme	Régulateurs financiers, conseils d'administration
R5	Mutualiser une capacité de calcul régionale pour l'IA	2	Moyen puis long terme	Ministères du numérique, institutions de développement
R6	Constituer des corpus ouverts de langues africaines	2	Court puis moyen terme	Universités, médias publics
R7	Encadrer l'IA à haut risque par les lois existantes et des bacs à sable	2	Court puis moyen terme	Autorités de protection des données
R8	Adopter une doctrine de classification des données publiques	3	Court puis moyen terme	Ministères du numérique
R9	Faire de la commande publique un levier de sécurité et de production locale	3	Court puis moyen terme	Ministères des finances, autorités des marchés publics

N°	Recommandation	Axe	Horizon	Pilote principal
R10	Négocier des partenariats technologiques avec transfert de compétences mesurable	3	Moyen terme	Gouvernements
R11 ★	Garantir l'indépendance et les moyens des autorités de protection des données	4	Court puis moyen terme	Gouvernements, parlements
R12	Protéger spécifiquement les données biométriques et les registres d'identité	4	Court terme	Agences d'identification, autorités de protection des données
R13	Ouvrir des voies de recours simples, mobiles et en langues nationales	4	Court terme	Autorités de protection des données
R14 ★	Lancer un programme « premier client public »	5	Court puis moyen terme	Ministères du numérique et des finances
R15	Créer un passeport réglementaire par reconnaissance mutuelle des bacs à sable	5	Moyen terme	Banques centrales, régulateurs
R16	Accélérer la ratification de la Convention de Malabo et l'entraide judiciaire	6	Moyen terme	Gouvernements, Commission de l'UA
R17 ★	Connecter les CSIRT à un dispositif africain de partage des menaces	6	Court puis moyen terme	Agences cyber, CSIRT
R18	Créer des cellules indépendantes de réponse aux crises informationnelles	7	Court ou moyen terme	Commissions électorales, régulateurs des médias
R19	Obtenir la transparence des plateformes et généraliser l'éducation aux médias	7	Moyen terme	Commission de l'UA, communautés régionales

N°	Recommandation	Axe	Horizon	Pilote principal
R20	Réserver une part fixe des projets numériques publics à la sécurité	8	Court terme	Ministères des finances, bailleurs
R21	Mobiliser l'épargne longue africaine vers le capital patient	8	Moyen terme	Investisseurs, régulateurs des pensions
R22 ★	Créer des académies cyber et IA régionales avec au moins 30 % de femmes	9	Court puis long terme	Gouvernements, universités, entreprises
R23	Former les décideurs et mobiliser la diaspora	9	Court terme	Gouvernements, écoles d'administration
R24	Rendre les identités numériques interopérables et mutuellement reconnues	10	Moyen puis long terme	Agences d'identification, secrétariat de la ZLECAf
R25	Connecter le mobile money et les PME aux paiements transfrontaliers	10	Moyen terme	Banques centrales, opérateurs de paiement

★ Engagement prioritaire proposé à l'issue du Forum.

Annexe B — Glossaire des sigles

Sigle	Signification
APD	Autorité de protection des données personnelles
ASIN	Agence des systèmes d'information et du numérique (Bénin)
BAD	Banque africaine de développement
BCEAO / BEAC	Banques centrales des États de l'Afrique de l'Ouest / des États de l'Afrique centrale
bjCSIRT	Équipe nationale de réponse aux incidents de sécurité du Bénin
CAF	Cyber Africa Forum
CEDEAO, EAC, SADC, CEEAC	Communautés économiques régionales d'Afrique de l'Ouest, de l'Est, australe et centrale
CSIRT	Équipe de réponse aux incidents de sécurité informatique
ENC-VR	École nationale de cybersécurité à vocation régionale (Dakar)
IA	Intelligence artificielle
ISAC	Centre sectoriel de partage et d'analyse de l'information sur les menaces
KYC	Connaissance du client (vérification d'identité)
MFA	Authentification multifacteur
PAPSS	Système panafricain de paiement et de règlement
PME	Petites et moyennes entreprises
SOC	Centre opérationnel de sécurité
UA	Union africaine
UIT	Union internationale des télécommunications

Sigle	Signification
USSD	Service de messages courts interactifs accessible sans Internet sur téléphone mobile
ZLECAf	Zone de libre-échange continentale africaine

Annexe C — Méthode

Formulation des recommandations. Chaque recommandation suit la même grille : constat, enjeu stratégique, recommandation (commençant par un verbe d'action), destinataires, mécanisme d'exécution, horizon, indicateurs et impact attendu.

Horizons. Court terme : 0 à 12 mois. Moyen terme : 1 à 3 ans. Long terme : 3 à 5 ans.

Statut des affirmations. Les faits établis sont sourcés, avec année et périmètre. Les analyses et les propositions sont celles de 50Afrique et d'Afropreneurs Emerging Leaders. Les cibles chiffrées que nous proposons (10 % des projets publics réservés à la sécurité, 30 % ou 40 % de femmes, une dizaine de pays pilotes) sont signalées comme des hypothèses de travail.

Sources. Priorité aux sources institutionnelles (Union africaine, UIT, Banque mondiale, INTERPOL, autorités nationales) et aux rapports sectoriels reconnus. Lorsqu'un rapport primaire n'était pas accessible directement, la source secondaire qui le cite est indiquée dans la bibliographie.

Échos du Forum. Les déclarations et échanges du Forum sont rapportés d'après les comptes rendus des sessions, sans citation mot pour mot. Aucune position n'est prêtée à un intervenant au-delà de ce qui a été rapporté.

Limites. Les données africaines sur les incidents, les compétences et les financements restent lacunaires et hétérogènes. Les comparaisons entre pays doivent être lues avec prudence.

Bibliographie

Sources consultées en novembre 2026. Lorsqu'un rapport primaire n'était pas accessible directement, la source secondaire qui le cite est indiquée.

Cyber Africa Forum 2026

- Digital Business Africa — Cyber Africa Forum 2026 : Cotonou réunira 1 500 décideurs
- Osiris — Cyber Africa Forum 2026 : IA, cybersécurité et confiance numérique au programme
- APA News — Cotonou accueillera le Cyber Africa Forum 2026

Institutions panafricaines et internationales

- Union africaine — Stratégie continentale d'intelligence artificielle, juillet 2024
- Union africaine — Groupe d'experts en cybersécurité (AUCSEG)
- Chatham House — The AU took important action on cybersecurity at its 2024 summit (février 2024)
- Forvis Mazars — Convention de Malabo, entrée en vigueur le 8 juin 2023
- UIT — Measuring digital development: Facts and Figures 2025
- UIT Global Cybersecurity Index 2024, via The New Times ; via Agence Ecofin
- INTERPOL — Rapport 2025 sur l'évaluation des cybermenaces en Afrique (communiqué) ; synthèse WeAreTech Africa ; synthèse PR Nigeria
- Banque mondiale — Africa Economic Update, octobre 2026, via Devdiscourse ; via FourWeekMBA
- Banque mondiale — Rapport sur le développement dans le monde 2026, via Nairametrics
- GSMA — State of the Industry Report on Mobile Money 2026, via The Guardian Nigeria
- Africa Center for Strategic Studies — Mapping a Surge of Disinformation in Africa (mars 2024)

Protection des données, commerce numérique, IA

- Digital Policy Alert — The Year of the Teeth: Data Protection in Africa Roundup (janvier 2026)
- Algeria Tech — synthèse du rapport Yellow Card (avril 2026)
- Mondaq — What the AfCFTA Digital Trade Protocol means for Africa ; Further Africa (juillet 2026)
- Lelapa AI — InkubaLM, a small language model for low-resource African languages

Cas nationaux

- Bénin : Conseil de l'Europe, profil Octopus ; ID4Africa 2026, présentation Bénin ; Benin Web TV, rapport bjCSIRT 2021-2024 ; ASIN, référentiel de qualification des prestataires
- Ghana : Cyber Security Authority, licences et accréditations ; Graphic Online
- Kenya : Capital FM, eCitizen ; ngCERT, avis sur l'attaque ; TechPoint, Worldcoin ; Dawan Africa, suppression confirmée ; The Standard, Cyber Shujaa

- Nigeria : TechEconomy, programme 3MTT
- Sénégal : Osiris, ENC-VR de Dakar ; Osiris, formation à la cyberdiplomatie
- Afrique du Sud : Daily Maverick, NHLS ; South African Medical Journal

Talents, financement, infrastructures

- African Arguments, citant BCG et Global Cybersecurity Forum 2024 ; IT-Online
- Partech Africa Tech VC Report 2025, via AllAfrica ; Tech In Africa ; Techloy
- TechEconomy, citant l'Africa Data Centres Association (février 2026)
- The Guardian Nigeria — PAPSS (novembre 2026)

Quatrième de couverture

Construire la confiance numérique de demain : 25 recommandations stratégiques pour une Afrique souveraine, sûre et innovante

La confiance numérique sera l'un des grands facteurs de différenciation entre les économies africaines qui subiront les transformations technologiques et celles qui sauront les maîtriser pour créer de la valeur, protéger leurs populations et renforcer leur puissance économique.

L'Afrique ne manque plus de textes sur le numérique ; elle manque de moyens d'exécution et de mesure. Cette contribution au Cyber Africa Forum 2026 propose 25 recommandations, chacune assortie d'un destinataire, d'un mode d'exécution, d'un horizon et d'un indicateur. Elle identifie cinq engagements prioritaires et trois initiatives : un Observatoire panafricain de la confiance numérique, un Pacte des dirigeants pour la cyber-résilience et le programme Afropreneurs Cyber & IA Leaders.

50Afrique est un think tank engagé dans la réflexion stratégique, la production d'idées et la formulation de propositions pour le développement du continent africain.

Afropreneurs Emerging Leaders est le mouvement de 50Afrique dédié au leadership, à l'entrepreneuriat, à l'innovation et à l'émergence d'une nouvelle génération de décideurs et de bâtisseurs africains. Créé en 2020, il porte le Fellowship AOYL, le Forum AEL et des publications, et réunit plus de 100 fellows sur 4 continents.

Contact : 50Afriquemagazine@gmail.com

© 2026 50Afrique × Afropreneurs Emerging Leaders. Contribution indépendante : elle n'engage ni les organisateurs du Cyber Africa Forum, ni ses intervenants, ni les institutions citées.

© 2026 50Afrique × Afropreneurs Emerging Leaders · Entrepreneurs en mouvement

Contribution indépendante au Cyber Africa Forum 2026. Elle n'engage ni les organisateurs, ni les intervenants, ni les institutions citées.