VERISTORE TECHNOLOGIES
Cellule de Veille Strstégique

ANALYSE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Vingt-et-un mois d'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire depuis sa création : montée en charge, cadre normatif, positionnement régional et gouvernance de la double tutelle

Document d'analyse en sources ouvertes – août 2026
Réf. VST-VIT-CYB-2026/ANSSI-01
Analyste Senior - Veristore Technologies

SYNTHÈSE EXÉCUTIVE

L'essentiel

L'ANSSI ivoirienne a vingt-et-un mois. Cette brièveté interdit toute évaluation de performance : il n'existe ni statistique d'incidents publiée, ni série budgétaire détaillée, ni recul suffisant pour lui imputer un résultat. Ce qui peut être évalué, en revanche, est la qualité de sa mise en place. Elle est solide, et le présent document en fait l'inventaire détaillé. L'écart qui subsiste avec les meilleurs dispositifs régionaux n'est pas un écart de conception : c'est un écart de calendrier.

6 mois	Entre le décret de création et le transfert effectif des missions — un délai court pour une reprise de compétence réglementaire
250 → 500	Professionnels formés en six mois, pour un objectif annoncé de 500 experts, avec un second parcours et une filière académique déjà programmés
78,95 / 100	Score au Global Cybersecurity Index 2024 — mesure antérieure à la création de l'agence, qui constitue sa ligne de base
6 ans	Écart de calendrier avec le dispositif régional le plus proche et le mieux classé, dont le modèle est transposable sans réforme institutionnelle

Trois constats

- **Le dispositif construit est de bonne facture.** En vingt-et-un mois, l'agence a récupéré ses compétences, publié un référentiel opposable, ouvert une chaîne d'audit et de certification graduée, installé des schémas de qualification de prestataires, formé un premier corps d'auditeurs et conduit publiquement le bilan de la stratégie sortante. La section 2 détaille onze acquis vérifiables.
- **L'écart régional est un écart de temps, non de doctrine.** Le dispositif ouest-africain le mieux classé dans le voisinage immédiat a construit sa position sur six années d'antériorité. Aucun de ses instruments décisifs n'est hors de portée de l'ANSSI ivoirienne, et aucun n'exige de modifier l'architecture institutionnelle retenue en 2024.
- **Le point de bascule est le passage du déclaré au vérifiable.** Le cadre normatif est en place ; ce qui manque est la publication régulière des grandeurs qui permettent à un tiers — bailleur, assureur, investisseur, évaluateur international — de constater le travail accompli. C'est aussi ce qui déterminera le prochain classement du pays.

Objet et portée

Évaluation en sources ouvertes de la **mise en place** d'une institution, non de sa performance. Aucune donnée classée, aucun test technique, aucune sollicitation de système. Les limites de l'exercice sont exposées en section 6 plutôt que dissimulées. Le document ne met en cause aucun agent public à titre personnel.

SECTION 1

Vingt-et-un mois de montée en charge

L'Agence Nationale de la Sécurité des Systèmes d'Information a été créée par le **décret n° 2024-958 du 30 octobre 2024**. Le Conseil des ministres qui l'a adoptée a présenté l'agence comme concentrant les attributions antérieurement réparties entre plusieurs structures de lutte contre la cybercriminalité et de protection des systèmes d'information. La passation de charges avec l'Autorité de Régulation des Télécommunications est intervenue le **30 avril 2025** : six mois entre l'acte de création et la reprise effective des missions, ce qui constitue un délai court pour un transfert de compétence réglementaire entre deux personnes publiques.

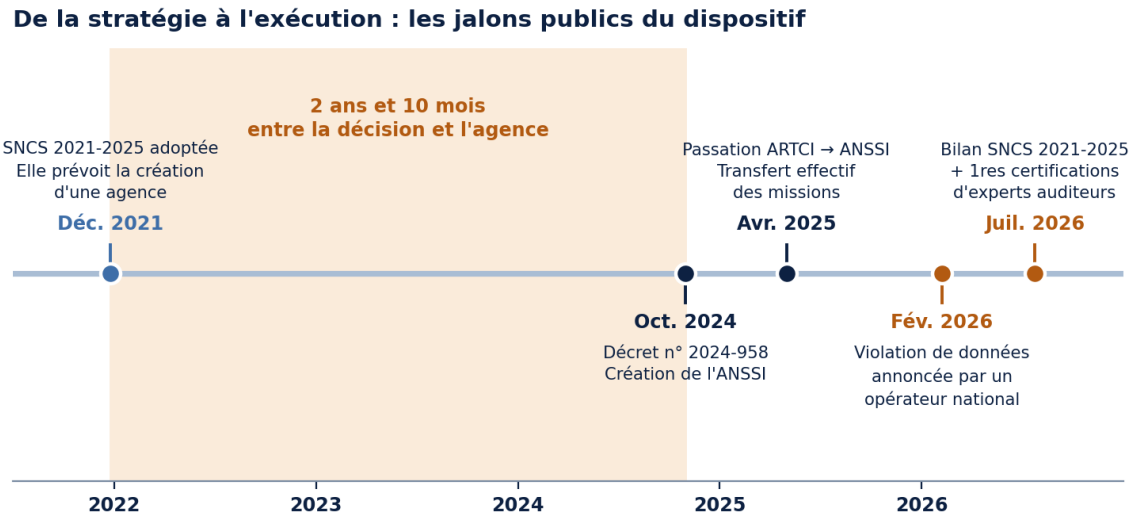

Figure 1 — Jalons publics du dispositif, de l'adoption de la stratégie nationale de cybersécurité à l'état des lieux de juillet 2026.

Un décalage que l'État documente lui-même

La première Stratégie Nationale de Cybersécurité, adoptée en décembre 2021 pour la période 2021-2025, comportait six objectifs stratégiques — renforcement du cadre légal, protection du cyberespace, confiance numérique, refonte du cadre institutionnel, capital humain, coopération internationale — pour un budget estimé à 18 milliards de FCFA, et prévoyait expressément la création d'une agence nationale. Celle-ci a vu le jour deux ans et dix mois plus tard.

Ce diagnostic n'est pas une reconstruction extérieure : le projet de stratégie 2026-2030 rattache lui-même le bilan d'achèvement des projets au démarrage tardif du bras opérationnel de l'État, conjugué aux effets durables de la pandémie. Une administration qui inscrit son propre retard dans un document de planification adopte une posture d'évaluation que peu d'équivalents régionaux assument aussi ouvertement. C'est, en soi, un indicateur de gouvernance favorable — à condition que le diagnostic débouche sur des échéances opposables.

SECTION 2

Ce qui a été construit : inventaire des acquis

Les évaluations comparatives internationales réduisent souvent une administration à un score. Cette section fait l'inverse : elle recense ce qui a été effectivement produit depuis octobre 2024, élément par élément. Onze acquis sont établis et vérifiables en sources ouvertes. Plusieurs d'entre eux n'ont pas d'équivalent à un stade aussi précoce dans les dispositifs voisins.

A. Architecture et compétences

- **1. La fin de la dispersion des compétences.** Avant 2024, la cybersécurité ivoirienne était répartie entre plusieurs structures aux mandats partiellement recouvrants. Le décret de création les concentre dans une entité unique. La fragmentation institutionnelle est l'une des causes les plus constantes de sous-performance en matière de cybersécurité : elle dilue la responsabilité de la réponse et empêche l'interlocuteur unique dont le secteur privé a besoin. Ce point de départ est bon.
- **2. Une double tutelle qui élargit la portée de l'agence.** Le rattachement simultané au ministre chargé de la Transition Numérique et au ministre chargé de la Sécurité donne à l'ANSSI un accès direct à la chaîne judiciaire tout en préservant son interface technique avec les opérateurs. Peu d'agences comparables disposent des deux. C'est un actif institutionnel, dont la section 5 examine la condition d'usage.
- **3. Un transfert de compétence mené en six mois.** La reprise des missions antérieurement exercées par le régulateur sectoriel a été formalisée par une passation de charges documentée et publiquement annoncée. Les transferts de compétence réglementaire s'étalent fréquemment sur plusieurs exercices ; celui-ci a été conduit sans interruption apparente de service.

B. Production normative et instruments de contrôle

- **4. Un référentiel national opposable.** Le Référentiel Général de Sécurité des Systèmes d'Information dans son édition 2025 fixe les règles organisationnelles et techniques auxquelles la conformité est appréciée. Disposer d'un référentiel national propre, et non d'un simple renvoi à des normes internationales, est le marqueur d'une doctrine souveraine : c'est ce qui rend l'audit opposable en droit interne.
- **5. Une chaîne de certification à issues graduées.** À l'issue d'un audit, l'organisation reçoit un certificat si elle est conforme, un certificat sous conditions en cas de non-conformité mineure, et fait l'objet d'un nouvel audit en cas de non-conformité majeure. Cette gradation est un signe de maturité réglementaire : elle évite l'alternative brutale entre conformité et sanction, et crée une trajectoire de mise à niveau exploitable par les opérateurs.
- **6. Une obligation de déclaration des incidents significatifs.** Elle constitue le préalable indispensable à toute réponse coordonnée et à toute statistique nationale. Son existence place déjà la Côte d'Ivoire dans le groupe des États qui ont franchi ce pas réglementaire.
- **7. Des schémas de qualification des prestataires.** La qualification des prestataires d'audit et des prestataires de services de confiance électronique organise et contrôle le marché privé. Son effet dépasse la conformité : elle crée les conditions d'une industrie nationale de la cybersécurité plutôt qu'un recours systématique à des prestataires étrangers.

C. Capacités opérationnelles et capital humain

- **8. Un centre national de réponse aux incidents.** Le CI-CERT, rattaché à l'agence, assure la réponse rapide, l'investigation technique de l'origine des attaques et des vulnérabilités exploitées, ainsi que la prévention et la sensibilisation. Il est complété par un dispositif public d'alertes, de veille et de panorama des menaces.
- **9. Un premier corps d'experts auditeurs certifiés, et une filière derrière lui.** Les premiers certificats ont été remis le 29 juillet 2026 ; plus de 250 professionnels — directeurs des systèmes d'information, responsables de la sécurité, auditeurs — ont été formés en six mois pour un objectif de 500. Le point décisif n'est pas le volume mais la **continuité prévue** : un second parcours dédié aux experts d'intégration, un catalogue et un calendrier de formation 2026-2027, et l'ouverture de masters en cybersécurité en partenariat avec un établissement supérieur national. L'agence traite le capital humain comme un flux à produire, non comme une opération ponctuelle.

- **10. Une certification adossée au référentiel national.** Le parcours d'expert auditeur articule la maîtrise du référentiel national et la capacité à conduire des audits de conformité, là où les certifications internationales généralistes restent déconnectées du droit applicable. C'est un choix de souveraineté rarement fait aussi tôt, et il conditionne l'effectivité de la chaîne d'audit décrite plus haut.
- **11. Une méthode de planification ouverte et inscrite dans le cadre national.** Le bilan de la stratégie 2021-2025 et l'examen du projet 2026-2030 ont été conduits le 23 juillet 2026 en associant administrations, secteur privé, opérateurs d'infrastructures critiques, universitaires et partenaires techniques et financiers. La stratégie suivante est conçue comme la déclinaison sectorielle d'un pilier du plan national de développement — elle n'est donc pas un document autonome sans traduction budgétaire — et place explicitement la redevabilité parmi ses valeurs directrices.

> **Ce que cet inventaire établit**
>
> Sur les onze acquis recensés, sept relèvent de la construction normative et opérationnelle, et quatre engagent la trajectoire au-delà de l'exercice en cours. Aucun ne relève de l'annonce : chacun correspond à un acte, un texte, un dispositif ou une promotion identifiables. À vingt-et-un mois, l'agence a franchi les étapes qui, dans les dispositifs comparables de la sous-région, ont généralement demandé trois à quatre ans. **Le rythme de construction n'est pas le problème ; le point de départ l'était.**

Récapitulatif

Acquis	Nature	Ce qu'il rend possible
1. Compétences concentrées	Institutionnel	Un interlocuteur unique et une responsabilité de réponse identifiée
2. Double tutelle	Institutionnel	L'accès à la chaîne judiciaire sans perdre l'interface technique
3. Transfert en six mois	Institutionnel	L'exercice effectif des missions sans interruption de service
4. RGSSI 2025	Normatif	Un référentiel opposable en droit interne
5. Certification graduée	Normatif	Une trajectoire de mise à niveau plutôt qu'une sanction binaire
6. Déclaration obligatoire	Normatif	La réponse coordonnée et, à terme, la statistique nationale
7. Qualification des prestataires	Normatif	Un marché privé structuré et une industrie nationale
8. CI-CERT	Opérationnel	La détection, l'investigation technique et l'alerte
9. Corps d'auditeurs et filière	Capital humain	L'exécution effective des audits, et son renouvellement
10. Certification adossée au RGSSI	Capital humain	Des auditeurs formés au droit applicable, non à un standard générique
11. Planification ouverte	Gouvernance	Un rattachement budgétaire et un engagement de redevabilité

SECTION 3

Le cadre normatif

Le reproche le plus fréquemment adressé aux dispositifs cyber de la région — l'absence de base juridique — ne s'applique pas ici. L'architecture normative ivoirienne est en place et articulée.

Instrument	Objet	Portée opérationnelle
Loi n° 2017-803 du 7 déc. 2017	Orientation de la société de l'information	Socle législatif général du numérique
Décret n° 2021-917 du 22 déc. 2021	Procédures d'audit, de contrôle et de certification des systèmes d'information	Fonde la chaîne de certification et ses trois issues
Décret n° 2024-958 du 30 oct. 2024	Création, attributions, organisation et fonctionnement de l'ANSSI	Institue l'agence et sa double tutelle
RGSSI, édition 2025	Règles de sécurité organisationnelles et techniques	Référentiel de conformité opposable, base des audits
Obligation de déclaration	Notification des incidents significatifs à l'État	Condition d'une réponse coordonnée et d'une statistique nationale
Schémas de qualification	Prestataires d'audit et de services de confiance électronique	Structure et contrôle le marché privé de la prestation

Où se situe la contrainte

Un référentiel opposable ne vaut que par le nombre d'audits effectivement conduits, et un régime de déclaration que par le nombre de déclarations recueillies. Sur le premier point, l'agence a produit son premier vivier d'auditeurs en vingt-et-un mois, ce qui est rapide au regard des cycles de formation ; l'ordre de grandeur reste toutefois sans commune mesure avec la demande, l'Union internationale des télécommunications évaluant à **100 000 le déficit continental** d'experts cyber hautement qualifiés. Sur le second, aucune statistique de déclaration n'est à ce jour publiée.

Une seconde différence mérite d'être relevée, car elle explique une part de l'écart mesuré en section 4 : l'ensemble ivoirien repose sur une loi d'orientation générale et des décrets, là où plusieurs dispositifs mieux classés reposent sur un texte législatif spécifique — code du numérique ou loi de cybersécurité — qui donne au référentiel, à l'obligation de déclaration et au régime de sanction une assise de rang supérieur. Ce point est repris en section 7.

> **Les deux indicateurs à publier**
>
> Ni le nombre de textes, ni le nombre de conventions signées ne mesurent un dispositif de cybersécurité. Deux grandeurs le font : le **taux de couverture d'audit des opérateurs soumis au référentiel** et le **nombre annuel d'incidents déclarés**. Tant qu'elles ne sont pas publiées, aucun tiers ne peut apprécier le travail accompli autrement que par des indices composites internationaux dont la section suivante montre les limites — et qui, par construction, retardent d'un à deux ans sur la réalité.

SECTION 4

Positionnement régional

Le Global Cybersecurity Index de l'Union internationale des télécommunications évalue l'engagement des États sur cinq piliers — mesures juridiques, techniques, organisationnelles, développement des capacités et coopération — et les répartit en niveaux. Dans l'édition 2024, la Côte d'Ivoire obtient **78,95 points sur 100**, au niveau *Establishing*.

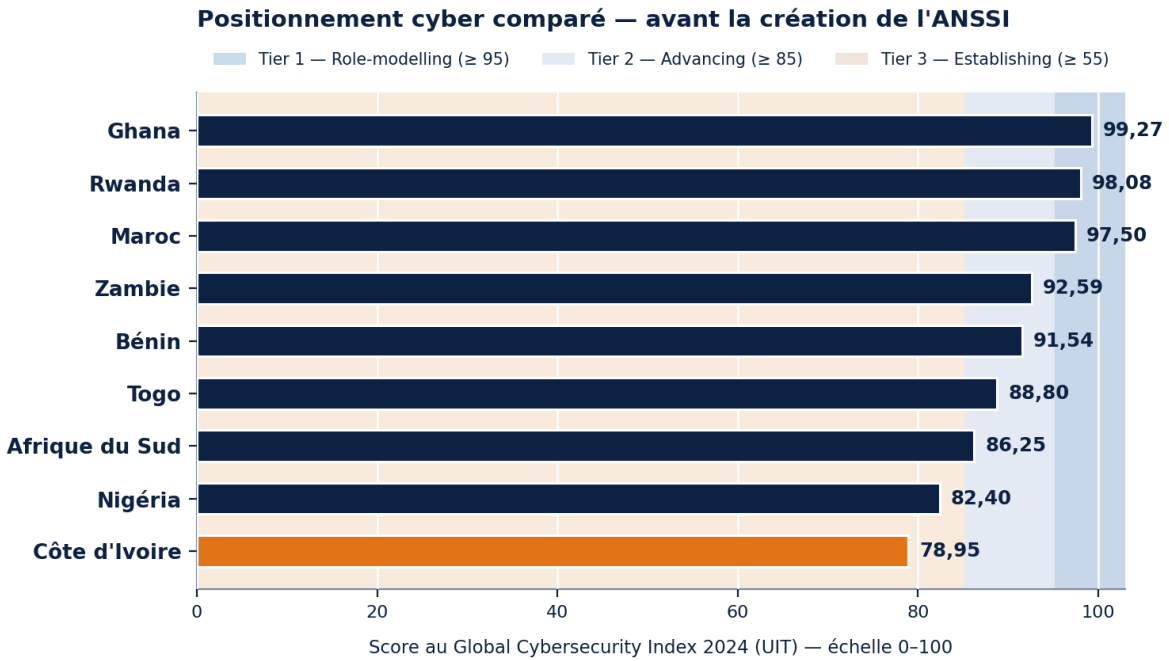

Figure 2 — Scores au Global Cybersecurity Index 2024. Les bandes de fond matérialisent les seuils de niveau publiés par l'UIT.

- **Le voisinage immédiat est devant.** Le Ghana atteint 99,27 et figure au niveau *Role-modelling*, avec le Rwanda et le Maroc. Le Bénin (91,54) et le Togo (88,80) sont au niveau *Advancing*.
- **Le score mesure l'héritage, pas l'agence.** L'édition 2024 a été publiée avant la création de l'ANSSI. Ces 78,95 points décrivent la situation dont l'agence a hérité. Ils ne lui sont pas imputables — et constituent à ce titre la ligne de base la plus utile dont on dispose. Aucun des onze acquis recensés en section 2 n'y figure.
- **La mesure porte sur l'engagement documenté, non sur la sécurité atteinte.** L'indice évalue l'existence et la documentation de dispositifs. Un État qui produit beaucoup de textes sans les appliquer y progresse ; un État qui applique sans publier y stagne. C'est précisément la raison pour laquelle la recommandation de publication formulée en section 3 a un effet direct sur le classement.

> **La ligne de base, et le rendez-vous**
>
> C'est le point méthodologique central de cette évaluation. La prochaine édition de l'indice sera la première à intégrer l'existence de l'agence, le référentiel général, le régime de certification, les schémas de qualification et le corps d'auditeurs. L'écart entre 78,95 et le score suivant constituera la première mesure extérieure et comparable de ce que l'ANSSI aura produit. Toute appréciation de performance antérieure à cette publication relève de l'opinion.

SECTION 5

La gouvernance de la double tutelle

L'ANSSI est une agence d'exécution placée sous deux tutelles distinctes : celle du ministre chargé de la Transition Numérique pour les matières administratives et techniques propres à la gouvernance et aux missions générales de cybersécurité ; celle du ministre chargé de la Sécurité pour les activités et faits de cybersécurité susceptibles de qualification pénale ou touchant à la sûreté de l'État.

Le dispositif est cohérent avec la nature du domaine : un incident cyber peut relever simultanément de la panne technique, de l'infraction pénale et de l'atteinte à la sûreté nationale. Un rattachement unique au ministère technique aurait privé l'agence de l'accès à la chaîne judiciaire ; un rattachement unique à la Sécurité aurait éloigné le secteur privé. La formule retenue évite les deux écueils, et il faut souligner qu'elle n'est pas une singularité : la double tutelle est le schéma dominant dans la sous-région. Ce qui varie d'un pays à l'autre est l'identité du second ministère — les Finances dans le dispositif béninois, la Sécurité en Côte d'Ivoire. Le premier choix sécurise le financement ; le second sécurise la portée judiciaire.

Le point d'attention n'est pas le conflit, c'est le seuil

Le risque usuellement prêté aux doubles tutelles — la rivalité entre ministères — n'est pas le plus probable ici. Le point sensible est celui de la qualification : un incident bascule d'une tutelle à l'autre dès lors qu'il devient « susceptible de qualification pénale ». Or cette appréciation intervient nécessairement après les premières constatations techniques, c'est-à-dire au moment même où la victime décide, ou non, de déclarer.

Il en découle un effet qu'aucun texte ne corrige seul : une entreprise qui anticipe qu'une déclaration ouvrira un canal pénal peut préférer traiter l'incident en interne. La sous-déclaration devient alors une réponse rationnelle à une incertitude de qualification, et non un défaut de civisme. C'est le principal frein potentiel à la constitution de la statistique nationale d'incidents — celle-là même dont l'absence empêche aujourd'hui de mesurer le dispositif. Le remède est simple et peu coûteux : un protocole public précisant qui qualifie, à quel moment, et ce que la déclaration déclenche ou ne déclenche pas.

> **Une gouvernance dotée d'un portage politique élevé**
>
> La direction générale de l'agence est confiée à un officier général et la présidence de son conseil de surveillance à un officier général de rang supérieur. Ce portage confère à l'agence une capacité d'articulation avec l'appareil de sécurité et un poids interministériel que peu d'agences comparables possèdent à ce stade de leur existence. Il appelle en contrepartie un effort explicite de lisibilité vis-à-vis des opérateurs privés, dont la coopération volontaire fournit l'essentiel de la détection.

Où sont rattachées les autorités comparables

Dispositif	Rattachement	Ce que ce choix privilégie
Côte d'Ivoire	Transition Numérique + Sécurité	La portée judiciaire et l'articulation avec l'appareil de sécurité
Bénin	Numérique + Économie et Finances	La sécurisation budgétaire et la capacité d'investissement technique
Ghana	Ministère unique, autorité créée par la loi	La force normative et la redevabilité parlementaire
Rwanda	Supervision de la Présidence	L'autorité interministérielle et la rapidité de décision

La double tutelle n'est donc pas une particularité ivoirienne : elle est le schéma dominant. Ce qui distingue les dispositifs est l'identité du second rattachement, et chacun de ces choix emporte un avantage propre.

SECTION 6

Ce que cette évaluation ne peut pas établir

Une évaluation qui n'énonce pas ses angles morts n'est pas une évaluation. Quatre questions, parmi les plus importantes, restent hors de portée des sources ouvertes. Elles ne traduisent aucune défaillance de l'agence : elles résultent de l'état actuel de la publication.

Question	Pourquoi elle ne peut être traitée	Ce qui la rendrait traitable
Le niveau réel de menace subie	Aucune statistique nationale d'incidents déclarés n'est publiée	Panorama annuel, même agrégé et anonymisé
La couverture des opérateurs critiques	La liste ou les critères de désignation ne sont pas publics	Publication des critères, à défaut de la liste
Les moyens effectifs de l'agence	Ni budget exécuté ni effectifs ne sont publiés séparément	Ligne budgétaire identifiée en loi de finances
L'effet propre de l'ANSSI	Le dernier indice comparable est antérieur à sa création	Prochaine édition du GCI, comparée aux 78,95

Deux signaux extérieurs, à manier avec précaution

Des données de télémétrie privée situent la Côte d'Ivoire parmi les pays africains les plus exposés, avec une part élevée d'ordinateurs industriels visés par des maliciels en 2024. Par ailleurs, un opérateur national du transport aérien a rendu publique, en février 2026, une violation de ses systèmes d'information.

Ces deux éléments doivent être lus pour ce qu'ils sont. Une mesure de télémétrie dépend du parc installé de l'éditeur qui la produit et ne constitue pas une mesure d'incidence nationale. Un incident rendu public par sa victime atteste d'un fait, non d'une tendance — et témoigne d'ailleurs, en creux, d'une pratique de divulgation qui va exactement dans le sens recherché par le régime de déclaration. Ni l'un ni l'autre ne permet de conclure sur l'état de sécurité du cyberespace ivoirien.

Ce que l'agence publie déjà

Il serait inexact de conclure de ce qui précède que le dispositif ivoirien serait opaque. L'agence met à la disposition du public un ensemble de ressources dont l'existence constitue en elle-même un acquis : un canal de déclaration et de signalement d'incident, un dispositif d'alertes et de veille, un panorama des menaces, un espace dédié aux responsables de la sécurité des systèmes d'information, une foire aux questions juridique, ainsi que le corpus des réglementations, normes et référentiels applicables. Cette orientation de service est peu fréquente à ce stade de maturité institutionnelle.

La distinction est donc précise, et il importe de ne pas la caricaturer : ce qui fait défaut n'est pas la communication, qui est active et régulière, mais la publication périodique de grandeurs agrégées permettant la comparaison dans le temps. Un panorama des menaces décrit un état ; une statistique annuelle d'incidents déclarés mesure une évolution. Le premier informe, le second atteste.

> **Une limite partagée, non une singularité ivoirienne**
>
> L'absence de statistique nationale publiée sur les incidents déclarés est la règle plutôt que l'exception dans la sous-région : la quasi-totalité des dispositifs ouest-africains est dans la même situation. Ce constat atténue la portée critique de l'observation, mais il en renforce la portée stratégique. Le premier État de la sous-région à publier une telle série n'améliorera pas seulement son classement : il se dotera d'un argument vérifiable vis-à-vis des investisseurs, des assureurs et des partenaires financiers, dans un domaine où aucun de ses voisins ne peut aujourd'hui en produire.

SECTION 7

Le modèle de référence recommandé : le Bénin

Trois dispositifs africains devancent nettement la Côte d'Ivoire : le Ghana, le Rwanda et le Bénin. Le mieux classé n'est pas nécessairement le plus utile à imiter. Le critère pertinent n'est pas la performance du modèle, mais sa **transposabilité** : un dispositif n'est reproductible que si le pays qui l'adopte partage la même tradition juridique, le même ordre de grandeur économique et une architecture institutionnelle compatible. Sur ces trois critères, le modèle béninois est celui qui s'impose.

Critère de transposabilité	Bénin	Ghana	Rwanda
Tradition juridique	Droit civil, francophone — identique	Common law — techniques légistiques différentes	Système mixte, anglophone
Espace économique et monétaire	UEMOA, franc CFA — identique	Hors UEMOA, cedi	Hors UEMOA, Afrique de l'Est
Ordre de grandeur	Économie plus petite : modèle atteignable à moyens comparables	Économie et filière numérique plus larges	Trajectoire portée par un modèle administratif spécifique
Architecture de tutelle	Double tutelle, comme la Côte d'Ivoire — compatible	Autorité sous ministère unique, créée par loi	Rattachement à la Présidence — incompatible sans réforme
Coût de transposition	Faible : instruments adoptables dans le cadre juridique existant	Élevé : suppose une loi spécifique et un régime de licences	Élevé : suppose de défaire la double tutelle de 2024

Le tableau compare l'aptitude à la transposition, non la qualité des dispositifs. Le Ghana demeure le modèle le plus performant de la région.

Pourquoi la transposabilité prime sur le classement

Une recommandation d'inspiration n'a de valeur que si elle est exécutable. Le Ghana obtient le meilleur score du continent et son dispositif est à juste titre cité comme référence : autorité instituée par une loi du Parlement, régime de licences opposable aux prestataires de services de cybersécurité, fonds dédié alimenté par des ressources propres, rapport annuel présenté devant le Parlement. Mais cet ensemble repose sur une loi-cadre de près de cent articles adoptée dans un système de common law. Le transposer intégralement suppose d'ouvrir un cycle législatif complet, c'est-à-dire exactement le type de délai que la stratégie 2026-2030 cherche à comprimer.

Le Rwanda présente la même difficulté sous une autre forme. Son autorité est établie par la loi, placée sous la supervision de la Présidence de la République, dotée de l'autonomie administrative et financière et liée par un contrat de performance. L'architecture est remarquable, mais elle repose sur un rattachement unique au sommet de l'exécutif. La reproduire supposerait de défaire la double tutelle instituée en 2024 — une réforme dont le coût excéderait le bénéfice, alors même que cette double tutelle constitue, comme la section 5 l'a établi, un actif de la configuration ivoirienne.

Le Bénin, à l'inverse, partage avec la Côte d'Ivoire la tradition civiliste, l'espace économique et monétaire, un ordre de grandeur de moyens comparable et — point rarement relevé — le principe même de la double tutelle. Ses instruments s'insèrent dans le cadre juridique ivoirien existant sans réforme préalable. C'est la raison, et la seule, pour laquelle il est retenu ici.

> **Une inspiration, non un décalque**
>
> La trajectoire béninoise comporte une étape qui n'est **pas** recommandée à la Côte d'Ivoire : la fusion, en juin 2022, de quatre agences d'exécution du numérique en une structure unique, l'agence de sécurité des systèmes d'information y devenant un pôle. Cette rationalisation répondait à une dispersion propre au Bénin. La Côte d'Ivoire vient au contraire de concentrer ses compétences dans une agence dédiée ; une réorganisation déferait le gain de 2024. L'inspiration porte sur les instruments, non sur l'organigramme.

Six ans d'antériorité, non un écart de doctrine

La démonstration la plus utile n'est pas le comparatif de scores, mais le comparatif de calendriers. Le Bénin a créé son agence de sécurité des systèmes d'information par décret du 14 novembre 2018, après avoir adopté son code du numérique la même année et installé son centre de réponse aux incidents dès 2017. La Côte d'Ivoire a créé la sienne le 30 octobre 2024. L'écart de 12,59 points constaté à l'indice 2024 recouvre donc, pour l'essentiel, un écart de six années d'exercice.

Deux trajectoires institutionnelles comparées

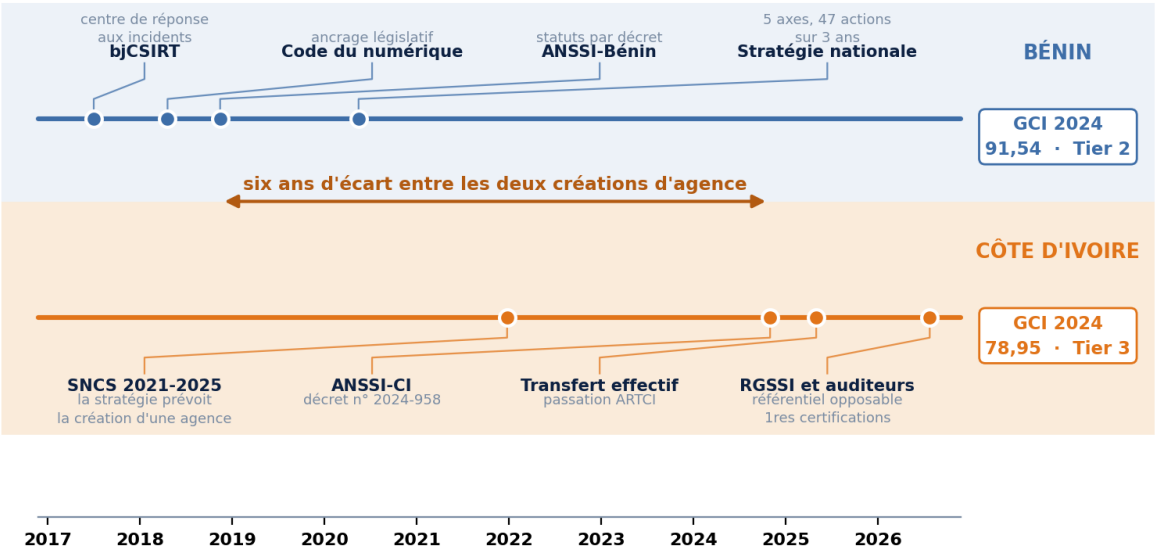

Figure 3 — Trajectoires institutionnelles comparées. Les jalons retenus sont ceux qui produisent un effet mesurable sur les piliers de l'indice international.

Cette lecture a une conséquence directe pour la stratégie 2026-2030 : elle suggère que la priorité n'est pas de concevoir un modèle nouveau, mais de **comprimer un calendrier**. Quatre instruments béninois y contribuent, et aucun n'exige de modifier le décret de 2024.

Instrument 1 — L'ancrage législatif

Le dispositif béninois repose sur un code du numérique adopté par le législateur, les statuts de l'agence étant approuvés par décret en application de ce code. La hiérarchie est donc inversée par rapport à la situation ivoirienne, où le référentiel et l'obligation de déclaration reposent sur des textes réglementaires. L'enjeu est pratique : un régime de sanction administrative et une obligation de déclaration acquiert leur pleine opposabilité, notamment vis-à-vis des opérateurs privés et devant le juge, lorsqu'ils sont adossés à une norme de rang législatif.

Instrument 2 — La stratégie courte et dénombrable

La stratégie nationale de sécurité numérique béninoise, opérationnelle depuis mai 2020, a été bâtie sur **cinq axes déclinés en quarante-sept actions, pour une durée de trois ans**. Ce format n'est pas un détail de rédaction. Une stratégie de trois ans à actions dénombrées se prête à un suivi d'exécution ; un document-cadre quinquennal à objectifs généraux ne s'y prête pas. La stratégie ivoirienne 2026-2030 étant en cours de finalisation, c'est l'instrument le plus immédiatement adoptable, et le seul dont la fenêtre se refermera avec l'adoption du document.

Instrument 3 — Les actifs techniques souverains

Le Bénin a construit, avant d'étendre son périmètre réglementaire, un socle technique détenu par l'État : centre national de réponse aux incidents dès 2017, infrastructure à clés publiques nationale, laboratoire d'analyse forensique, politique de protection des infrastructures critiques. Ce sont précisément ces actifs qui alimentent le pilier technique de l'indice international, et ce sont eux qui donnent à une agence la capacité de constater par elle-même plutôt que de dépendre des déclarations qu'elle reçoit.

La Côte d'Ivoire dispose du premier de ces actifs avec le CI-CERT. L'infrastructure à clés publiques et le laboratoire forensique constituent les deux jalons suivants, et le second présente ici un intérêt particulier : un laboratoire forensique national est l'outil qui rend opérationnelle la seconde tutelle de l'agence, en produisant la preuve technique exploitable par la chaîne pénale.

Instrument 4 — La politique de sécurité opposable à l'État lui-même

Le dispositif béninois s'appuie sur une politique de sécurité des systèmes d'information de l'État qui s'impose à l'ensemble des agences, institutions et sociétés d'État, avec des règles à mettre en œuvre et une responsabilité opérationnelle identifiée au sein de chaque entité. C'est le levier le plus rapide qui soit, pour une raison évidente : l'État maîtrise son propre périmètre. Il ne dépend d'aucune adhésion volontaire du secteur privé, il produit immédiatement de la matière d'audit, et il fournit à l'agence un terrain d'application où éprouver son référentiel avant de l'étendre.

> **Deux emprunts ciblés aux autres modèles**
>
> Recommander un modèle principal n'interdit pas deux greffes précises, chacune limitée à un mécanisme dont la transposition ne coûte presque rien.
>
> **Du Ghana — le rapport annuel.** L'autorité ghanéenne est tenue de remettre un rapport annuel au ministre, qui le présente au Parlement ; ce rapport expose l'activité de l'autorité, l'état de la cybersécurité du pays et l'emploi des ressources qui lui sont affectées. C'est le mécanisme qui résout, en une seule disposition, les trois angles morts identifiés en section 6.
>
> **Du Rwanda — le contrat de performance.** L'autorité rwandaise fonctionne sur la base d'un contrat de performance dont les modalités de conclusion et d'évaluation sont fixées par la loi. Une agence dont les objectifs sont contractualisés et évalués devient mesurable par construction, sans qu'aucun évaluateur extérieur ait à reconstituer ses résultats.

Dans quel ordre

L'ordre d'adoption n'est pas indifférent, car ces instruments se conditionnent les uns les autres. La **stratégie à actions dénombrées** vient en premier, non parce qu'elle serait la plus importante, mais parce que sa fenêtre est la plus étroite : elle se referme à l'adoption du document en cours de finalisation. La **politique de sécurité opposable au périmètre État** vient ensuite, parce qu'elle produit la matière d'audit sans laquelle le corps d'auditeurs nouvellement certifié resterait sous-employé. Le **protocole de qualification** et le **rapport annuel** interviennent au même moment, car le premier libère la déclaration et le second en publie le résultat : publier une statistique d'incidents avant d'avoir levé le frein à la déclaration reviendrait à publier un chiffre trompeur.

Les **actifs techniques souverains** et l'**élévation de l'assise normative** relèvent enfin du temps long : le premier suppose un investissement, le second un cycle législatif. Les engager tôt est nécessaire ; en attendre un effet à court terme ne le serait pas.

SECTION 8

Recommandations pour le cycle 2026-2030

Les recommandations qui suivent sont classées par coût de mise en œuvre croissant. Les trois premières ne supposent ni texte nouveau, ni ressource additionnelle significative.

Recommandation	Contenu	Origine	Effet attendu
1. Publier un rapport annuel	Panorama agrégé des incidents déclarés, taux de couverture d'audit, emploi des ressources	Ghana	Rend le dispositif vérifiable ; alimente directement les piliers de l'indice international
2. Formater la stratégie en actions dénombrées	Axes déclinés en actions numérotées, horizon court, revue à mi-parcours	Bénin	Transforme un document-cadre en instrument de suivi d'exécution
3. Publier un protocole de qualification	Qui qualifie un incident, à quel moment, et ce que la déclaration déclenche ou non	Analyse propre	Lève le frein à la déclaration privée, première source de détection
4. Étendre la politique de sécurité à tout le périmètre État	Règles opposables à l'ensemble des entités publiques, responsable identifié dans chacune	Bénin	Levier le plus rapide : ne dépend d'aucune adhésion externe
5. Compléter le socle technique souverain	Infrastructure à clés publiques nationale, puis laboratoire d'analyse forensique	Bénin	Capacité de constatation propre ; rend la seconde tutelle opérationnelle
6. Contractualiser les objectifs de l'agence	Contrat de performance assorti de modalités d'évaluation	Rwanda	Rend l'agence mesurable par construction
7. Élever l'assise normative	Consolidation législative du référentiel, de l'obligation de déclaration et des sanctions	Bénin, Ghana	Opposabilité pleine, notamment devant le juge

Appréciation d'ensemble

À vingt-et-un mois, l'ANSSI a fait davantage que ce qu'une agence naissante accomplit habituellement : reprise complète de ses missions en six mois, référentiel national opposable, chaîne de certification graduée, schémas de qualification, centre de réponse aux incidents, premier corps d'auditeurs adossé au référentiel national et filière académique engagée. Le retard que le pays doit combler ne lui est pas imputable : il s'est constitué entre 2021 et 2024, avant son existence.

La question ouverte n'est donc pas celle de sa performance passée, qui n'est pas mesurable, mais celle de la vitesse de rattrapage. Le modèle béninois montre que l'écart régional se referme en six ans par accumulation d'instruments ; il montre aussi que trois de ces instruments peuvent être adoptés dès l'exercice en cours. Le premier verdict extérieur tombera avec la prochaine édition de l'indice international : la décision qui pèsera le plus sur ce verdict est celle de publier.

ANNEXE

Note méthodologique et sources

Périmètre et méthode

- **Nature de l'exercice.** Évaluation de mise en place institutionnelle, en sources ouvertes exclusivement. Aucun test technique, aucune sollicitation de système, aucune collecte sur infrastructure tierce n'a été conduite.
- **Période couverte.** Du 30 octobre 2024, date du décret de création, au 8 août 2026. La période antérieure n'est mobilisée que pour établir le délai entre la décision stratégique et sa mise en œuvre.
- **Panel de comparaison.** Neuf États africains dont les scores 2024 sont publiquement documentés. Les États dont le score n'est pas publiquement vérifiable ont été écartés du graphique plutôt qu'estimés.
- **Choix du modèle de référence.** Le modèle recommandé en section 7 a été sélectionné sur cinq critères de transposabilité explicités et non sur le rang obtenu à l'indice international. Le dispositif le mieux classé de la région n'est pas celui recommandé, et les motifs de cet écart sont publiés.
- **Traitement des indices tiers.** Le Global Cybersecurity Index est reproduit sous sa méthodologie propre, que Veristore ne valide ni ne conteste. Sa limite principale est explicitée dans le corps du document : il mesure l'engagement déclaré et documenté des États, non le niveau de sécurité effectivement atteint.
- **Aucun indice composite propre** n'a été construit. Une agence de vingt-et-un mois ne se prête pas à une notation synthétique : l'exercice aurait donné une apparence de mesure à un jugement.

Sources mobilisées

Côte d'Ivoire — décret n° 2024-958 du 30 octobre 2024 ; décret n° 2021-917 du 22 décembre 2021 ; loi n° 2017-803 du 7 décembre 2017 ; communications du Conseil des ministres ; portail et documents publics de l'ANSSI (missions, CI-CERT, réglementations, RGSSI, Stratégie Nationale de Cybersécurité 2021-2025 et projet 2026-2030) ; communiqué de l'Autorité de Régulation des Télécommunications relatif à la passation de charges.
Bénin — loi n° 2017-20 portant code du numérique ; décret n° 2018-529 du 14 novembre 2018 approuvant les statuts de l'agence ; décret n° 2022-324 du 1er juin 2022 portant fusion des agences d'exécution du numérique ; publications de l'agence et entretiens publics de ses responsables sur la stratégie nationale de sécurité numérique.
Ghana — Cybersecurity Act, 2020 (Act 1038) et publications de l'autorité nationale de cybersécurité.
Rwanda — loi n° 26/2017 du 31 mai 2017 établissant l'autorité nationale de cybersécurité ; stratégie nationale 2024-2029.
International — Union internationale des télécommunications, Global Cybersecurity Index 2024 et travaux dérivés de cartographie africaine.
Presse nationale et spécialisée pour la chronologie des événements publics. Données de télémétrie privée citées sous réserve expresse de représentativité.

Avertissement

Document établi en sources ouvertes à la date du 8 août 2026. Il ne contient aucune information classée, ne résulte d'aucune commande institutionnelle et n'engage aucune administration ivoirienne ou étrangère. Les appréciations analytiques relèvent de la seule responsabilité de Veristore Technologies. Aucun agent public n'est mis en cause à titre personnel : les fonctions citées le sont en tant qu'éléments d'architecture institutionnelle. Les comparaisons internationales portent sur des dispositifs, non sur des États. Les indices mobilisés faisant l'objet de révisions périodiques, toute décision fondée sur ce document devrait être précédée d'une actualisation.

Analyste Senior · Veristore Technologies — Réf. VST-VIT-CYB-2026/ANSSI-01