AFRICAN CYBERSTRATEGY INDEX (ACSI)

Proposition de critères et indicateurs d'évaluation et de pondération

Le présent document a pour but de décrire la méthodologie utilisée pour concevoir un Indice Africain de Cyberstratégie (ci-dessous abrégé ACSI pour *African Cyberstrategy Index*). Il précise également la liste de critères pertinents mobilisés pour évaluer le niveau de maturité des États africains en matière de cyberstratégie.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

INTRODUCTION GÉNÉRALE

Dans un monde de plus en plus régi par les dynamiques numériques, le cyberespace s'impose comme une arène stratégique majeure au sein de laquelle se dessinent les nouvelles lignes de force de la souveraineté, de la puissance et de la sécurité. L'Afrique, continent en pleine mutation numérique, est appelée à formuler ses propres réponses à ces enjeux, non seulement pour protéger ses intérêts, mais également pour affirmer sa voix dans la redéfinition des normes et structures de gouvernance globale du cyberespace. C'est dans cette perspective que s'inscrit le développement de l'**Indice Africain de Cyberstratégie (ACSI)**, pensé comme un outil d'analyse, d'évaluation et d'orientation des efforts nationaux dans la construction d'une souveraineté numérique durable et géopolitiquement pertinente.

1. Contexte d'émergence

L'émergence de l'ACSI s'inscrit dans une époque marquée par l'intensification des inégalités numériques, la dépendance accrue aux technologies étrangères, la montée en puissance des menaces cybernétiques transnationales d'origine étatique ciblant le continent et l'absence d'outils africains systématisés pour mesurer les efforts en matière de stratégie dans le cyberespace. Tandis que plusieurs indices internationaux — à l'instar du *Global Cybersecurity Index* (ITU) ou du *National Cyber Power Index* (Harvard) — proposent des lectures globales, aucun n'intègre suffisamment les réalités africaines, ni ne tient compte des défis spécifiques que pose la construction d'un cyberpouvoir autonome dans des contextes de vulnérabilité structurelle. Le *National Cyber Power Index* par exemple est fondé sur l'idée que les Etats évalués ont une certaine indépendance technologique et une autonomie d'action dans le cyberespace, ce qui n'est pas la réalité de la plupart des pays africains. Le Laboratoire Africain de Recherches en Cyberstratégie (LARC)

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

entend donc combler ce vide méthodologique en proposant une matrice d'analyse conçue **par** et **pour** les réalités africaines.

2. Justification du sujet et du corpus

La création d'un indice dédié à l'évaluation stratégique des politiques cyber en Afrique répond à un double impératif : scientifique, d'une part, en tant qu'outil de formalisation et de systématisation des approches africaines de la cyberstratégie ; décisif, d'autre part, en tant qu'outil d'aide à la décision (gouvernance) et élément catalyseur d'un alignement entre les ambitions de souveraineté numérique et les mécanismes concrets de planification et d'évaluation. Le corpus à partir duquel est élaborée cette réflexion comprend les politiques publiques nationales, les traités et conventions continentales, les pratiques observées au sein des organisations (institutions, entreprises, etc.) de cybersécurité, ainsi que les contributions d'experts issus du continent. Il s'appuie également sur les travaux internationaux comparatifs et sur une veille stratégique des dynamiques régionales et globales du cyberespace.

3. Définition

L'**Indice Africain de Cyberstratégie (ACSI)** est un instrument d'évaluation multidimensionnel destiné à mesurer le niveau de **maturité stratégique des États africains dans le cyberespace**, c'est-à-dire leur capacité à concevoir et mettre en œuvre des politiques et actions cohérentes, autonomes, résilientes et géopolitiquement influentes en matière numérique. Il repose sur une grille de critères pondérés qui permettent, par une démarche scientifique le calcul d'une note pour chaque pays, d'objectiver le niveau d'intégration du cyberespace dans la stratégie nationale de développement, de défense, de sécurité et de puissance.

4. **Objectif**

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

L'ACSI est conçu pour mesurer la **maturité stratégique** des pays africains dans le cyberespace en évaluant leur capacité à utiliser le cyberespace pour atteindre des objectifs nationaux, protéger et défendre leurs intérêts vitaux, renforcer leur souveraineté numérique, et influencer les dynamiques géopolitiques. L'indice se base sur des critères multiples, eux même issus d'une série d'indicateur par critère, qui mesurent à la fois l'intégration du cyberespace dans la stratégie nationale et la gestion des défis et opportunités que celui-ci génère.

5. Cadre conceptuel et théorique

Le développement de l'ACSI s'ancre dans un **cadre théorique transdisciplinaire** combinant la pensée stratégique, la théorie des systèmes complexes, les études sur la souveraineté numérique, l'autonomie stratégique dans le cyberespace, ainsi que l'analyse des politiques publiques. D'un point de vue conceptuel, l'ACSI s'inspire de la notion de **cyberpuissance** (cyber power), comprise comme la capacité d'un État à façonner et contrôler les dynamiques du cyberespace à des fins d'influence, de sécurité et de développement. La grille d'évaluation repose également sur les logiques d'**analyse multicritères** en usage dans les sciences de la décision, et intègre une lecture critique de la dépendance technologique, du positionnement géopolitique, ainsi que des capacités nationales d'adaptation et de projection. L'approche retenue est enfin résolument **afrocentrée**, c'est-à-dire attentive aux configurations politiques, institutionnelles, économiques et culturelles propres au continent africain.

6. Problématique

Comment mesurer de manière rigoureuse, contextualisée et opérationnelle, le niveau de maturité stratégique des États africains dans le cyberespace ? Quels indicateurs doivent être mesurés pour rendre compte à la fois de leur

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

souveraineté numérique, de leur posture géopolitique, de leurs capacités de projection stratégique et de leur résilience face aux menaces cyber ? Comment calcule-t-on la note à attribuer à chaque pays sur la base de ces différents critères ? En somme, sur quels fondements scientifiques et empiriques peut-on construire un indice susceptible de refléter la réalité africaine et d'orienter les politiques futures ?

7. Hypothèses

La construction de l'Indice Africain de Cyberstratégie repose sur plusieurs hypothèses de travail, qui orientent à la fois le choix des critères, l'architecture conceptuelle de l'outil, et enfin l'approche de calcul de la note.

La première hypothèse postule que la maturité cyberstratégique d'un État africain ne saurait être exclusivement appréhendée à l'aune de sa capacité technologique ou de ses performances économiques, mais doit intégrer des paramètres géopolitiques, institutionnels et culturels propres au continent. L'absence d'une infrastructure souveraine ne signifie pas nécessairement l'absence de stratégie : certaines nations développent en effet des formes de résilience ou d'autonomisation partielle (interdépendance stratégique), à travers des partenariats, des dispositifs réglementaires ou des écosystèmes innovants.

La seconde hypothèse suppose qu'il existe un lien direct entre la clarté d'une vision stratégique nationale du cyberespace et l'efficacité des politiques publiques mises en œuvre. Un État doté d'une stratégie explicite, cohérente, transversale et bien articulée sur le plan institutionnel sera mieux à même de défendre ses intérêts numériques, de se positionner géopolitiquement et de répondre aux menaces hybrides, même en contexte de ressources limitées.

Une troisième hypothèse, d'ordre méthodologique, avance qu'un indice pensé à partir d'une approche contextuelle et multicritère peut permettre

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

d'objectiver les efforts en matière de cyberstratégie sans imposer un modèle unique. L'ACSI vise donc non pas à normer, mais à **reconnaître**, **valoriser** et **orienter** des trajectoires différenciées, en prenant acte de la pluralité des modèles africains.

Enfin, une quatrième hypothèse plus politique présume que la formalisation d'un tel indice contribuera, à moyen et long termes, à la consolidation d'une diplomatie cyber africaine. Nous avons en somme, la présomption de fournir aux États et aux institutions continentales un instrument de plaidoyer, d'aide à la décision, de coordination et de souveraineté.

8. Résultats escomptés

L'élaboration de l'ACSI vise à produire une **grille de lecture analytique robuste et évolutive** des politiques cyber en Afrique. Parmi les résultats attendus, on peut citer : une meilleure visibilité des efforts nationaux et régionaux en matière de cyberstratégie ; la mise à disposition d'un outil de pilotage stratégique pour les décideurs publics ; la création d'un référentiel africain de la cyberstratégie contribuant à la souveraineté cybernétique du continent ; et enfin, une incitation à la coopération régionale fondée sur des critères partagés et comparables.

Ce cadre de recherche constitue le socle de l'Indice Africain de Cyberstratégie tel qu'il est proposé dans le présent rapport. Les pages qui suivent déclinent, critère par critère, les fondements, indicateurs et modalités de pondération retenus, dans le but d'offrir un outil rigoureux, opératoire et scientifiquement fondé pour évaluer la maturité cyberstratégique des États africains.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

ÉNONCÉ DES CRITÈRES ET INDICATEURS D'ÉVALUATION DE L'ACSI

Les critères retenus dans l'ACSI ne sont ni arbitraires ni purement normatifs. Ils procèdent d'une analyse fine des dimensions constitutives de toute stratégie cyber : la **souveraineté numérique**, entendue comme la capacité à produire, gérer et sécuriser les ressources numériques stratégiques ; la **gouvernance**, en tant que mécanisme de coordination du dispositif organisationnel, des politiques et des institutions ; la **projection stratégique**, qui renvoie à l'usage du cyberespace comme levier d'influence régionale ou mondiale ; la **résilience face aux menaces**, dans un contexte marqué par l'essor des menaces hybrides et complexes d'origine étatique; le **financement et l'investissement massif**, indispensable pour créer une base industrielle du numérique et impulser le développement d'un écosystème local ; enfin, la **capacité de formation et d'innovation**, élément moteur du développement technologique et de l'autonomie. Ces critères ont été affinés grâce à une consultation d'experts africains du domaine et à un examen comparatif des cadres existants à l'échelle mondiale, tout en tenant compte de la diversité des contextes africains. Par ailleurs, les pondérations attribuées à chaque critère résultent d'un **équilibre entre pertinence stratégique, faisabilité de la mesure, et diversité des contextes nationaux**.

Avertissement : Les critères et indicateurs présentés dans cette grille d'évaluation constituent une version actualisée suite aux retours des experts consultés. Bien que cette version ait été rigoureusement affinée pour refléter les meilleures pratiques et la pertinence contextuelle pour les États africains, il est important de noter que ces éléments restent évolutifs. Les résultats obtenus via l'Indice Africain de Cyberstratégie (ACSI) doivent être interprétés comme une photographie de la maturité numérique à un instant donné, et peuvent être ajustés à mesure que de nouvelles données, recommandations

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

ou tendances émergent. L'usage de ces critères implique donc une vigilance méthodologique et une actualisation périodique pour garantir la pertinence de l'évaluation.

1. Souveraineté numérique et autonomie technologique

(Poids : 22%)

Description : Évalue la capacité d'un pays à contrôler les leviers d'autonomie et de souveraineté de son cyberespace (réduire sa dépendance aux technologies étrangères, développer ses propres infrastructures, plateformes et contenus, etc.).

Indicateurs

- Niveau de dépendance aux technologies, produits ou services étrangers (notamment en termes de propriété et contrôle d'accès aux infrastructures critiques) et d'exposition / consommation des contenus étrangers.
- Existence d'un cadre légal et règlementaire sur la localisation, la protection, l'accès et la portabilité des données (personnelles, sensibles, stratégiques) pour garantir le contrôle national.
- Existence d'un dispositif spécifique d'identification (liste nationale d'OIV) et de protection des infrastructures critiques du pays, et niveau de mise en œuvre effective
- Progrès réalisés dans le développement de technologies locales (data centers, réseaux de fibre optique, infrastructure numérique, etc.) et des contenus locaux.
- Niveau d'autonomie d'appréciation, de décision et d'action dans le cyberespace (y compris la capacité de s'y défendre ou d'y mener

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

des opérations cyber-offensives)

Sources : Rapports gouvernementaux et autres publications officielles (Textes de lois et règlements, discours, et organigramme gouvernemental)

2. Stratégie nationale du cyberespace, gouvernance veille stratégique

(Poids : 20%)

Description : Évalue dans quelle mesure le pays intègre le cyberespace dans sa stratégie nationale, et son approche pour gérer ses ressources et menaces numériques de manière holistique.

Indicateurs

- Existence d'un document national de stratégie cyber actualisé, clair avec une vision à long terme, aligné avec les priorités stratégiques nationales (sécurité, défense, développement économique, etc.), et qui reflète explicitement la prise en compte du cyberespace comme milieu stratégique et d'affrontement.
- Mise en place d'un dispositif obligatoire d'homologation de solutions numériques étrangères et de certification des solutions nationales avant utilisation dans les OIV.
- Existence des capacités d'analyse prédictive et prospective, d'anticipation et de veille stratégique dans le cyberespace
- Mise en place de structures étatiques de gouvernance numériques (ministères, agences nationales et entités publiques spécialisées, experts gouvernementaux désignés, unité militaire dédiée, etc.) chargée de la protection et la défense du cyberespace nationale

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

- Existence d'une doctrine de cyberdéfense claire dans les armées du pays

- Existence de mécanismes de coordination public-privé, inter-agences et intersectorielle de très haut niveau pour la gestion du cyberespace (entité de coordination rattachée au premier ministère ou à la présidence de la république, groupe de travail, plateforme de partage d'information, etc.)

Sources : Rapports gouvernementaux et autres publications officielles (Textes de lois et règlements, discours, et organigramme gouvernemental)

3. Capital humain, innovation, recherche et écosystème du cyberespace

(Poids : 18%)

Description : Évalue la capacité du pays à développer et à renforcer son capital humain en matière d'expertise cyber, à créer un écosystème propice à la recherche et à l'innovation pour la protection et la défense du cyberespace, et à faire émerger une base industrielle solide dans ce secteur.

Indicateurs

- Existence et ampleur des programmes de sensibilisation, de formation et de développement des compétences relatives à la protection et la défense du cyberespace, aussi bien dans les secteurs publics et privés

- Mise en place des dispositifs et structures d'encadrement et d'accompagnement des entreprises technologiques locales (incubateurs, centres d'innovation, etc.)

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

- Partenariats avec des centres de recherche et des universités pour développer des technologies émergentes du domaine cyber
- Investissement dans la recherche et le développement dans le domaine du cyberespace et des innovations technologiques récentes (IA, Blockchain, Quantique, etc.).
- Mise en place d'un système de labélisation des produits, services et compétences nationales de protection et défense du cyberespace.

Sources : Enquêtes auprès d'institutions éducatives et professionnelles, données financières des budgets nationaux, études académiques, rapports indépendantes, textes de lois, centres d'excellences, etc.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

4. Adaptabilité, réactivité et résilience face aux menaces cybernétiques transnationales

(Poids : 15%)

Description : Mesure la capacité du pays à surveiller, à détecter et à répondre aux menaces cybernétiques transnationales, telles que les cyberattaques, la cybercriminalité, et la désinformation. Mesure aussi sa capacité de résilience pour garantir la disponibilité des services essentiels.

Indicateurs

- Mise en place de systèmes de détection et de réponse aux cybermenaces sur les infrastructures critiques ;
- Existence ou Développement des capacités offensives et défensives dans le cyberespace
- Existence d'un plan national résilience (continuité et reprise

d'activités spécifiques aux OIV) et de gestion de crise cyber

- Collaboration avec des partenaires internationaux pour lutter contre les cybermenaces globales (ex. : partage d'informations et de renseignement, etc.)
- Fréquence d'organisation locale ou de participation aux initiatives internationales d'exercices de simulation de crise cyber (cyber drills)
- Existence et efficacité des capacités de collecte, analyse et diffusion des renseignements sur les cybermenaces, mais aussi de réponse et de récupération après une cyberattaque (CIRT/CERT nationaux, SOC, centres d'analyse, etc.)

Sources : Rapports d'incidents publiés par les gouvernements ou les entreprises, doctrine militaire, textes de lois.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

5. Stratégie de financement et d'investissement dans les infrastructures numériques

(Poids : 13%)

Description : Évalue les investissements réalisés dans les infrastructures numériques critiques et leur niveau d'autonomie par rapport aux acteurs étrangers, afin de soutenir la souveraineté numérique et les ambitions stratégiques du pays.

Indicateurs

- Investissements publics et privés dans les infrastructures numériques critiques (réseaux, data centers, IPX, etc.) ;
- Existence de fonds publics dédiés, ou d'incitations réglementaires,

pour encourager et soutenir financièrement la sécurisation et la résilience cyber des infrastructures critiques ;

- Investissements dans la R&D et le capital humain pour les nouvelles technologies cyber
- Existence d'un cadre légal spécifique et incitatif, favorable aux investissements privés dans les projets d'innovation et de sécurité numérique ;
- Partenariats transnationaux pour le financement de projets et d'initiatives transnationales cyber (bailleurs de fonds et organisations internationales compétentes, etc.)

Sources : Études techniques, rapports d'experts et organisations spécialisées, textes (lois, règlements, décrets, etc.),

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

6. Positionnement géopolitique et diplomatie du cyberespace

(Poids : 12%)

Description : Évalue le rôle diplomatique et géopolitique du pays dans les affaires mondiales et régionales du cyberespace, notamment la participation à des initiatives régionales et internationales sur la cybersécurité, la participation aux groupes de travail ou d'experts gouvernementaux, ainsi que la présence dans les instances mondiales de gouvernance du cyberespace. Évalue également la capacité du pays à utiliser le cyberespace comme un levier stratégique pour sa projection internationale, son influence et son pouvoir.

Indicateurs

- Participation active dans des forums internationaux et multilatéraux de cybersécurité et dans les groupes d'experts gouvernementaux (ex. : ONU, GAC, GGE des Nations Unies)
- Relations diplomatiques bilatérales et multilatérales pour la coopération sur les problématiques relatives au cyberespace (partage de renseignement cyber, exercices conjoints de cyberdéfense, etc.)
- Engagement dans les discussions internationales sur la régulation du cyberespace (protection des données, gouvernance numérique, extraterritorialité du droit, etc.)
- Présence dans les institutions de gouvernance d'Internet (ICANN, IGF, etc.)
- Engagement et leadership dans les projets régionaux et mondiaux de développement numérique (Ex : initiative Smart Africa, réseau africain de fibre optique, African Open Data Center, IPX régional, etc.)
- Développement d'initiatives de Soft Power numérique (ex. : influence sur la culture numérique, gouvernance mondiale du cyberespace)

Sources : Analyse des accords et partenariats signés, analyse de la composition des groupes de travail internationaux et des organigrammes des instances de gouvernance mondiale en rapport avec le cyberespace, etc.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

MÉTHODOLOGIE DE CALCUL DE L'INDICE AFRICAIN DE CYBERSTRATÉGIE

L'ACSI vise à évaluer de manière quantitative et comparative la maturité cyberstratégique des pays africains. Cette évaluation repose sur une architecture méthodologique rigoureuse, structurée autour de plusieurs niveaux d'analyse et un mécanisme d'agrégation précis. L'approche se décline en plusieurs étapes clés :

Étape 1. Identification des Critères fondamentaux

La méthodologie s'articule autour de **6 critères principaux**. Ces critères représentent pour nous les piliers essentiels d'une cyberstratégie nationale robuste et couvrent les dimensions clés de la posture d'un pays dans le cyberespace (Gouvernance, Résilience, Coopération internationale, Développement des capacités, etc.)

Étape 2. Décomposition en indicateurs mesurables

Chacun des 6 critères est décomposé en un ensemble d'**indicateurs spécifiques et mesurables**. Ces indicateurs permettent de granulariser l'évaluation et de rendre l'appréciation de chaque critère plus objective et détaillée. Chaque indicateur cible un aspect particulier du critère auquel il est rattaché. Si l'indicateur est par exemple "la posture de cyberdéfense" du pays, on peut pour le mesurer regarder l'existence d'une unité cyber militaire dédiée, budget alloué, participation à des exercices internationaux, etc.).

Étape 3. Évaluation détaillée au niveau de l'indicateur :

Pour chaque pays évalué et pour **chaque indicateur individuel**, une note est attribuée. Cette note n'est pas subjective mais est construite sur l'analyse de **trois facteurs d'évaluation** distincts :

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

- **Avancement (ou Matérialisation) :** Évalue le niveau de réalisation effective et concrète de l'indicateur. Qu'est-ce qui a déjà été mis en place ou accompli ? (Ex: Unité cyber bel et bien existante au sein de l'armée, loi votée et promulguée, etc.).

- **Intention (ou Volonté Politique) :** Évalue la manifestation de la volonté politique et la vision stratégique concernant l'indicateur. Qu'est-ce qui est prévu, désiré ou inscrit dans les documents officiels ? (Ex: Engagement clair du gouvernement, stratégie ambitieuse, plans / programmes futurs, etc.).

- **Capacité (ou Moyens d'Action) :** Évalue la disponibilité des ressources et des moyens nécessaires pour soutenir l'indicateur. Le pays a-t-il les moyens (humains, financiers, techniques, légaux, institutionnels) de concrétiser l'avancement et l'intention ? (Ex: Budget suffisant, experts disponibles, cadre légal adapté, etc.).

Le **score attribué à chaque indicateur** est donc calculé en faisant la **moyenne des notes obtenues pour les trois facteurs** (Avancement, Intention, Capacité) pour cet indicateur spécifique.

Étape 4. Agrégation au niveau du critère

Une fois que tous les indicateurs d'un critère donné ont été évalués et scorés (étape 3), le **score du critère** est calculé. Le score d'un critère est obtenu en faisant la **moyenne des scores de tous les indicateurs** qui sont rattachés à ce critère. Tous les indicateurs au sein d'un même critère ont un poids égal.

Étape 5. Normalisation des scores des critères

Avant de calculer le score final, les scores moyens obtenus pour chacun des 6 critères sont **normalisés sur une échelle commune, typiquement de 0 à 100**. Cette normalisation est essentielle pour garantir que les scores des critères, qui peuvent avoir des gammes de valeurs potentiellement différentes en

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

fonction du nombre et de la nature de leurs indicateurs, soient comparables et puissent être correctement agrégés via la pondération.

Étape 6. Calcul du score final de l'indice

Chacun des 6 critères se voit attribuer une **pondération spécifique**. Cette pondération reflète l'importance relative de chaque critère dans la détermination de la maturité cyberstratégique globale du pays selon le modèle de l'indice. La somme des pondérations des 6 critères devant donner un total de 100%. Le score final de l'ACSI pour un pays est calculé en effectuant la **somme pondérée des scores normalisés de chacun des 6 critères**.

Score Final ACSI = **Score linéaire → moyennes arithmétiques simples sur les facteurs AIC**	**Score Normalisé Critère 1 * Pondération Critère 1) + (Score Normalisé Critère 2 * Pondération Critère 2) + ... + (Score Normalisé Critère 6 * Pondération Critère 6)**

Étape 7. **Interprétation du score final**

Le score final obtenu sur l'ACSI représente le niveau global de maturité cyberstratégique du pays évalué. Un score élevé indique un pays ayant une stratégie cyber robuste, caractérisée par des réalisations concrètes (Avancement), une vision claire et affirmée (Intention) et les moyens nécessaires pour agir (Capacité), particulièrement dans les domaines (critères) considérés comme les plus importants (ceux ayant les pondérations les plus élevées). Les pays seront à la fin, classés par ordre croissant de score, le pays considéré le plus mature ayant le score global le plus élevé.

DOCUMENT DE TRAVAIL NE PAS DIFFUSER

Exemple fictif de calcul ACSI pour un pays

Eléments évalués :

- 6 critères (C1 à C6))
- Evaluation (entre 0 et 5) de chaque indicateur selon A, I, C
- Moyenne, normalisation, pondération

Critère	Nom	Nb ind	Pondé
C1	Souveraineté numérique	3	20%
C2	Gouvernance et cadre légal	4	20%
C3	Résilience et cyberdéfense	3	20%
C4	Coopération internationale	2	15%
C5	Développement des capacités humaines	3	15%
C6	Innovation et infrastructures	3	10%

Evaluation des indicateurs de chaque critère

Indicateur	A	I	C	Moyenne
Cloud souverain	3	4	2	3.0
Données critiques	4	5	4	4.3
Régulation locale	2	3	3	2.7
Score C1	**3.33**			

Indicateur	A	I	C	Moyenne
Loi cybersécurité	5	5	4	4.67
Autorité nationale	3	4	3	3.33
Stratégie nationale	4	5	3	4.0
Protection des données	4	5	3	4.0
Score C2	**4.00**			

C3 – Résilience et cyberdéfense

- Score $= (3.33 + 2.33 + 3.67)/3 = \mathbf{3.11}$

C4 – Coopération internationale

- Score $= (3.67 + 3.0)/2 = \mathbf{3.34}$

C5 – Capacités humaines

- Score $= (2.33 + 3.33 + 2.0)/3 = \mathbf{2.56}$

C6 – Innovation et infrastructures

- Score $= (2.33 + 1.33 + 2.67)/3 = \mathbf{2.11}$

Normalisation des scores

Formule : $(\text{score moyen}/5) \times 100$

Critère	Score moyen	Normalisé
C1	3.33	66.6
C2	4.00	80.0
C3	3.11	62.2
C4	3.34	66.8
C5	2.56	51.2
C6	2.11	42.2

Pondération et score final

Formule : $\text{ACSI} = \sum(\text{score normalisé} \times \text{pondération})$

Critère	Score	Poids	Contribution
C1	66.6	20%	13.32
C2	80.0	20%	16.00
C3	62.2	20%	12.44
C4	66.8	15%	10.02
C5	51.2	15%	7.68
C6	42.2	10%	4.22
Total			**63.68**

DOCUMENT ... AS DIFFUSER

Remerciements

L'équipe de l'ACSI exprime sa profonde gratitude aux experts qui ont généreusement consacré leur temps et partagé leur expertise dans l'analyse et l'amélioration de la grille d'évaluation. Leurs commentaires critiques et suggestions constructives ont été déterminants pour l'élaboration de cette version enrichie, et ont permis de renforcer la rigueur et la pertinence de l'indice.