MINISTÈRE DE L'INTÉRIEUR
ET DE LA SÉCURITÉ

MINISTÈRE DE LA TRANSITION NUMÉRIQUE
ET DE L'INNOVATION TECHNOLOGIQUE

Projet de Stratégie Nationale de CyberSécurité 'SNCS' 2026-2030

Table des matières

COPYRIGHT

Ce document a été rédigé par le Cabinet EXULTET CONSULTING, spécialisé en Stratégie du numérique sous la supervision de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), et la participation de l'écosystème du numérique, particulièrement des experts issus des secteurs public, privé et académique.

Ministère de la Transition Numérique et de l'Innovation Technologique

Adresse : 17 BP 1404 Abidjan 17

Tél : +225 2720347372

Mail : ministere@telecom.gouv.ci

Site Web : www.telecom.gouv.ci

1. INTRODUCTION

1.1. Contexte et justification

L'élaboration de la Stratégie Nationale de Cybersécurité (SNCS) 2026-2030 intervient à un tournant décisif du développement de la Côte d'Ivoire. Alors que le pays accélère sa transformation digitale et la modernisation de ses structures socio-économiques, l'émergence d'un cyberespace de confiance devient une condition absolue pour garantir la souveraineté numérique, la continuité des services de l'État, protéger les citoyens et attirer les investissements.

Cette nouvelle feuille de route s'aligne sur la vision nationale de bâtir « *Une Grande Côte d'Ivoire, Ambitieuse et Solidaire »,* qui place la transformation structurelle de l'économie et l'inclusion sociale au sommet des priorités étatiques.

Dans cette dynamique, le numérique n'est plus un simple secteur d'activité, mais le moteur transverse de la performance de l'administration publique, de la compétitivité du secteur privé et de l'amélioration de la vie de la population. Cependant, cette accélération digitale, portée plus que jamais par l'émergence de l'Intelligence Artificielle et la valorisation massive des données, s'accompagne de risques cyber de plus en plus sophistiqués. Dès lors, la sécurisation du cyberespace ivoirien dépasse le cadre technique pour devenir un enjeu de souveraineté nationale et un pilier du contrat social.

Prenant la pleine mesure de cette situation, l'Etat ivoirien dans un contexte économique difficile marqué par les effets persistants de la pandémie de covid-19, a mis en œuvre sa première Stratégie Nationale de Cybersécurité sur la période 2021 – 2025.

Au terme de cette période stratégique, on note que la Côte d'Ivoire a modernisé son cadre législatif, centralisé le cadre institutionnel de la cybersécurité autour de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et jeté les bases de la transformation de l'écosystème de la cybersécurité.

Désormais, le pays doit franchir une étape décisive vers la résilience opérationnelle et la souveraineté numérique. La présente SNCS 2026-2030 ne saurait être une simple reconduction des acquis. Son ambition est triple :

- capitaliser sur les acquis par le renforcement des dispositifs qui ont fait la preuve de leur efficacité durant le cycle précédent ;
- reconduire et achever les chantiers essentiels initiés entre 2021 et 2025 pour garantir une protection totale des infrastructures critiques ;
- anticiper sur les nouvelles menaces pour bâtir un espace numérique de confiance, moteur de croissance économique et garant de la sécurité nationale.

En effet, l'évolution rapide des menaces liées notamment à l'intelligence artificielle et à la sophistication des cyberattaques met en évidence la nécessité de passer d'une posture principalement réactive à une posture résolument proactive, fondée sur l'anticipation des risques, la veille stratégique et technique. Cette dynamique nécessite le renforcement des compétences en vue de constituer un vivier national où l'être humain n'est plus le maillon faible mais une force active de protection et bénéficiaire de la stratégie. Le maillon faible devient le maillon fort.

L'enjeu est d'éveiller la conscience de chaque usager, du dirigeant / chef d'entreprise au simple citoyen, en passant par le travailleur de l'administration publique ou le salarié de l'entreprise privée pour que nul ne soit une faille par ignorance, mais que chacun soit capable de détecter les risques. Grâce à cette dynamique du changement marquée par la culture nationale de cybersécurité, la sécurité numérique se transforme en une vigilance partagée. La cybersécurité devient ainsi l'affaire de tous.

Alignée d'une part, sur le cadre juridique en vigueur dont la loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information en Côte d'Ivoire, la loi n°2024-352 du 06 juin 2024 relative aux communications électroniques, et d'autre part, sur le Plan National de Développement (PND 2026-2030),à la Stratégie Nationale de la Gouvernance des Données (SNGD 2030) ainsi qu'à la Stratégie Nationale de l'intelligence artificielle (SNIA 2030), la SNCS 2026-2030 devient le socle transversal de la confiance numérique. Elle accompagne l'émergence de la "*Grande Côte d'Ivoire*" innovante, performante et souveraine.

Pour garantir la pertinence et l'efficacité de cette vision, la démarche adoptée se veut holistique et inclusive. Elle repose sur une analyse croisée de nos performances passées, de notre écosystème local et des standards internationaux les plus exigeants.

1.2. Méthodologie

La SNCS 2026-2030 constitue la réponse stratégique aux défis de l'économie numérique ivoirienne en pleine expansion. Pour y parvenir, la méthodologie adoptée repose sur une démarche structurée, rigoureuse et inclusive en quatre (4) étapes allant du diagnostic opérationnel à la définition de la vision et du plan d'actions opérationnel :

- **La première étape est le diagnostic opérationnel** ;
- **La seconde étape de la démarche est consacrée au cadrage stratégique et à la mise en cohérence transversale ;**
- **La troisième étape est la consultation des parties prenantes ;**
- **La quatrième et dernière étape est la synthèse et la définition de la vision, des piliers et des objectifs stratégiques.**

2. PAYSAGE DES MENACES

La transformation numérique de la Côte d'Ivoire s'est fortement accélérée au cours de la dernière décennie. Elle est portée par la digitalisation des services publics, l'essor du Mobile Money et l'augmentation des usages numériques. Si cette dynamique constitue un levier important de développement économique et social, elle s'accompagne également d'une exposition accrue aux risques et menaces cyber.

Le paysage des menaces ivoirien est aujourd'hui dominé par une cybercriminalité opportuniste à motivation financière, ciblant particulièrement les services financiers numériques, les opérateurs de télécommunications et les usagers du Mobile Money. Les campagnes de phishing, les escroqueries en ligne et l'ingénierie sociale figurent parmi les modes opératoires les plus fréquents.

Selon le rapport d'activités 2024 de l'ANSSI « *L'analyse des trois dernières années montre une hausse continue du nombre de plaintes. En effet, les plaintes sont passées de 6579 en 2022 à 8132 en 2023, puis à 12100 en 2024, soit une augmentation de 84% entre 2022 et 2024* ». Cette augmentation s'explique par la digitalisation croissante des usages, la transition de la délinquance classique vers le numérique et une plus grande confiance des citoyens dans le dépôt de plaintes.

En 2024, plus de 12 000 affaires de cybercriminalité ont été enregistrées. Les atteintes à la dignité humaine (23 %) et les escroqueries sur Internet (19 %) figurent parmi les infractions les plus fréquentes. Sur le plan financier, les escroqueries en ligne représentent à elles seules près de 2,36 milliards de FCFA de préjudices, contribuant à un total estimé à près de 7 milliards de FCFA de pertes liées aux infractions cyber.

En 2025, 14705 affaires de cybercriminalité ont été enregistrées. Les atteintes à la dignité humaine conservent toujours la première place du top 5 des infractions avec un chiffre en baisse 21,07% des affaires, suivie de près par l'escroquerie sur internet qui a augmenté pour passer à 20,25%. L'entrée du prêt à usure en ligne dans le Top 5, soit 14,7% traduit l'émergence de nouvelles formes de cybercriminalité exploitant la vulnérabilité économique des populations.

Au titre des infractions, les cinq principales infractions enregistrées en 2025 sont l'accès frauduleux à un système d'information 60,59 %, l'escroquerie sur Internet 13,52 %, l'atteinte à la dignité humaine 7,91 %, l'usurpation d'identité 5,47 %) et la fraude sur transaction électronique 5,23 %.

L'accès frauduleux à un système d'information représente à lui seul plus de la moitié des pertes financières totales, soit 13 889 060 398 FCFA. Cela souligne la nécessité de renforcer la sécurité des systèmes d'information critiques et des infrastructures numériques.

Au-delà de cette cybercriminalité de masse, les systèmes d'information de certaines infrastructures critiques telles que l'énergie, la santé, les transports et les télécommunications peuvent constituer des cibles d'attaques plus structurées visant l'interruption de services, l'exfiltration de données sensibles ou l'atteinte à la crédibilité des institutions.

Les modes opératoires observés reposent principalement sur l'exploitation de vulnérabilités non corrigées, la compromission d'identifiants, l'ingénierie sociale et les attaques par la chaîne d'approvisionnement. Par ailleurs, l'usage croissant de l'intelligence artificielle facilite la production de contenus frauduleux sophistiqués et renforce la nuisance des campagnes de désinformation.

Plusieurs facteurs structurels amplifient ces risques. La maturité en cybersécurité reste inégale au niveau des populations et au sein des organisations, notamment dans certaines administrations et entreprises. La culture de sécurité demeure insuffisamment diffusée auprès des usagers et des professionnels. La dépendance à certaines technologies et services numériques étrangers limite également la maîtrise souveraine de certains systèmes critiques.

Dans ce nouveau contrat social qui place le citoyen au centre de la stratégie, l'identification des cibles constitue un préalable essentiel à la définition des priorités nationales de cybersécurité.

3. ACQUIS DE LA SNCS 2021-2025

La SNCS 2021-2025 a permis à la Côte d'Ivoire de réaliser des progrès décisifs. Elle a renforcé le cadre légal et instauré un nouvel écosystème institutionnel centralisé autour de l'ANSSI. Cette architecture s'appuie sur des centres techniques de pointe et bénéficie de la synergie avec l'ensemble des organismes partenaires de la sécurité numérique.

3.1. Un cadre légal renforcé

Entre 2021 et 2025, le cadre légal s'est enrichi avec de nouveaux instruments juridiques nationaux et internationaux telles que les conventions internationales de Budapest et de Malabo pour :

- centraliser au plan national, le cadre de gouvernance ;
- consolider la résilience des acteurs, tout en créant un environnement plus ouvert à l'innovation ;
- s'adapter aux standards internationaux en matière de lutte contre la cybercriminalité et de coopération judiciaire ;
- renforcer la coopération internationale.

La SNCS 2021-2025 a renforcé le cadre juridique existant avant son adoption de façon progressive au fil des années.

En 2021

- loi n°2021-893 du 21 décembre 2021 renforçant les peines liées aux infractions numériques ;
- décret n°2021-464 du 8 septembre portant organisation du MENUTI ;
- décret n°2021-911 du 22 décembre 2021 portant adoption du cadre commun d'architecture de référentiel de données ;
- décret n°2021-912 du 22 décembre 2021 portant adoption du cadre commun d'urbanisation des systèmes d'information de l'Etat ;
- décret n°2021-913 du 22 décembre 2021 portant adoption du référentiel général d'interopérabilité des systèmes d'information ;
- décret n°2021-914 du 22 décembre 2021 fixant les règles pour la conception, la réalisation et la gouvernance des projets publics d'infrastructures, d'équipements, et de la plateforme de services numériques ;
- décret n°2021-915 du 22 décembre 2021 Portant adoption de la politique de sécurité des systèmes d'information de l'administration publique ;
- décret n°2021-916 du 22 décembre 2021 portant adoption du référentiel général de sécurité des systèmes d'information ;
- décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information ;

- décret n°2021-918 du 22 décembre 2021 instituant un département en charge des systèmes d'information au sein des ministères.

En 2023

- loi n°2023-593 du 7 Juin 2023 modifiant les articles 17, 33, 58, 60, 62, et 66 de la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- loi n°2023-901 du 23 novembre 2023 portant promotion des startups numériques.

En 2024

- loi n°2024-352 du 6 Juin 2024 sur les communications électroniques ;
- décret n°2024-799 du 05 Septembre 2024 fixant le montant, les conditions et modalités de paiement de diverses contributions financière et licences des activités de communications électroniques ;
- décret n°2024-958 du 30 Octobre 2024 portant création, attributions organisation et fonctionnement de l'Agence Nationale de la Sécurité des systèmes d'Information.

En 2025

- décret n°2025-180 du 12 mars 2025 fixant les attributions, l'organisation et le fonctionnement du Comité de labellisation des Startups Numériques

3.2. Un cadre institutionnel centralisé

Le cadre institutionnel de la cybersécurité est désormais centralisé autour de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), une entité spécialement créée à cet effet.

La création de l'ANSSI marque une avancée majeure en dotant la Côte d'Ivoire d'une entité centrale, spécialement dédiée à la cybersécurité et chargée de coordonner les actions de prévention, de protection et de réponse aux incidents cyber.

Elle incarne la volonté de l'Etat de Côte d'Ivoire de bâtir un espace numérique sûr, résilient et de confiance. Pour réaliser ses missions, l'ANSSI est dotée de centres techniques de pointe.

3.3. Des centres techniques de pointe

Pour accomplir efficacement ses missions, l'ANSSI s'appuie sur des centres techniques de pointe, notamment :

- **(i) Le Centre national de gestion des incidents de cybersécurité 'CI-CERT'**

C'est précisément le 29 janvier 2020 que le Gouvernement a officiellement créé le CI-CERT en tant que Point focal national en matière de cybersécurité par décret n°2020-128 du 29 Janvier 2020.

Initialement, le CI-CERT était logé au sein de l'ARTCI.
Depuis 2024, il est devenu un Département à part entière de l'ANSSI et assure :

- la gestion et la réponse aux incidents majeurs ou critiques de cybersécurité;
- la coordination nationale et sectorielle des réponses aux incidents ;
- l'analyse approfondie des incidents ;
- une réponse adaptée en fonction de la gravité des menaces.

Sur la période 2021-2025, le CI-CERT a enregistré et traité environ 7804 incidents de sécurité réparti comme suit :

Tableau n°1 : Nombre d'incidents traités par le CI-CERT

Année	2021	2022	2023	2024	2025
NB d'incidents traités par le CI- CERT	Non parvenu	2117	2080	3607	Non parvenu

Source : ANSSI

(ii) La Plateforme de Lutte contre la cybercriminalité 'PLCC'

La PLCC a pour mission principale, la lutte contre les diverses formes de cybercriminalité.

A ce titre, elle mène plusieurs actions :
la prévention et la sensibilisation ;
la détection et l'analyse des incidents ;
la répression et le suivi juridique ;
la collaboration internationale.

De 2021 à 2025, la PLCC a traité 46 818 réclamations réparties comme suit.

Tableau n°2 : Nombre d'affaires traitées par la PLCC

Année	2021	2022	2023	2024	2025
NB de réclamations traitées	5302	6579	8132	12100	14705

Source : ANSSI

(iii) Le Centre de Fusion et d'Analyse de Données (CFAD)

Le CFAD a pour rôle de mutualiser les capacités d'investigations cyber permettant de soutenir tant les affaires de cybercriminalité que celles d'ordre général nécessitant des recherches techniques (grand banditisme, trafics de drogue, crimes économiques, trouble à l'ordre public, etc.). Ce choix permet à la Côte d'Ivoire d'impacter positivement l'ensemble du secteur de la sécurité.

Les missions du CFAD sont :
- collecter et traiter les données ;
- analyser les informations ;
- produire des rapports au profit des services d'investigations : PLCC, Police, Gendarmerie, CENTIF, Parquet, Juges d'instruction, etc.

Depuis sa création, le CFAD a enregistré et traité environ **21210** réclamations réparties comme suit :

- ***Tableau n°3 : Nombre de réclamations traitées le CFAD***

Année	2021	2022	2023	2024	2025
NB de réclamations	-	4379	8018	8813	Non parvenu

- ***Source : ANSSI***

- **(iv) Le Centre Alertes 100**

Les missions du Centre Alertes 100 sont :

- surveiller le territoire national par les moyens technologiques (vidéo protection, centre d'appel et les patrouilles web sur les réseaux sociaux) en mesure d'alerter les services de sécurité ;
- assister les services de maintien de l'ordre par les capacités technologiques ;
- faire les remontées d'informations ou d'incidents en temps réel et les démentis des fake news.

Depuis sa création en 2024, le Centre Alerte 100 a enregistré et traité 38 007 évènements répartis comme suit :

- ***Tableau n°4 : Nombre de réclamations traitées le Centre Alerte 100***

Année	2021	2022	2023	2024	2025
NB de réclamations traitées	6795	4379	8018	8813	10002

Source : ANSSI

- **(iv) Le Laboratoire de Criminalistique Numérique 'LCN'**

Le Laboratoire de Criminalistique Numérique (LCN) a pour mission d'extraire les données des équipements numériques qu'il reçoit des enquêteurs. Ses requérants sont constitués de services de police judiciaire ainsi que l'administration pénitentiaire.

Depuis sa création, le LCN a enregistré et analysé 11 780 matériels répartis comme suit :

Tableau n°5 : Nombre de matériels analysés par le LCN

Année	2021	2022	2023	2024	2025
NB de matériels analysés	1480	5056	2568	1450	1226

Source ANSSI

3.4. Les organismes partenaires

Au-delà des deux principaux Ministères de tutelle que sont le Ministère de la Transition Numérique et de l'Innovation Technologique ainsi que le Ministère de l'Intérieur et de la sécurité, d'autres organismes et acteurs publics et privés interviennent dans la cybersécurité.

3.4.1 Les organismes et acteurs publics

(i) Les organismes publics

Les principaux organismes publics intervenant dans la sécurisation des systèmes d'information sont :

- l'Autorité de Régulation des Télécommunications/ TIC de Côte d'Ivoire (ARTCI) ;
- la Société Nationale de Développement Informatique (SNDI) ;
- l'Agence Nationale du Service Universel des Télécommunications/ TIC (ANSUT) ;
- l'Agence Ivoirienne de Gestion des Fréquences (AIGF) ;
- l'Ecole Supérieur Africaine des TIC (ESTIC).

Pour rappel, avant la création de l'ANSSI et ce, dès 2007, la Direction de l'Informatique et des Traces Technologiques (DITT) avait été créée afin de prendre en charge les enjeux liés aux technologies numériques et à la cybersécurité.

Complètement opérationnelle à partir de 2011, la DITT s'est vu confier plusieurs missions majeures, à savoir (1) la lutte contre la cybercriminalité, (2) le conseil et l'assistance en matière de cybersécurité, (3) le soutien aux enquêtes et aux opérations de sécurité, (4) la conduite de projets technologiques à destination du secteur sécuritaire.

(ii) Les autres acteurs publics

D'autres acteurs publics interviennent également dans la sécurisation des systèmes d'information. Ce sont notamment :

- les forces de sécurité dont la police nationale, la gendarmerie ;
- la justice avec les parquets d'instance, l'Agence de Gestion et de Recouvrement des Avoirs Criminels ;
- la Cellule Nationale de Traitement des Informations Financières (CENTIF).

3.4.2 Les acteurs privés

Les acteurs privés qui interviennent dans la sécurisation des systèmes d'informations sont listés dans le tableau ci-dessous.

Tableau n° 5 Types des prestataires privés

TYPES DE PRESTATAIRES	NOMBRE	OBSERVATIONS
Prestataire de service de certification électronique (PSCE)	4	_
Prestataire d'Audit des Systèmes d'information (PASSI)	_	En cours de recrutement

Prestataire de service cryptologie (PSCO)	_	_
Prestataires de Service d'Archivage Electronique (PSAE)	_	_
Prestataire de Développement de Sécurisé (PDS)	-	-
Intégrateurs	_	_

.

4. LES DEFIS DE LA SNCS 2021-2025

En 2020, la Côte d'Ivoire s'est placée au 75ième rang mondial et 11ième rang africain, sur les194 pays classés à l'indice Mondial de Cybersécurité (GCI)

Dans la 5e édition du Global Cybersecurity Index (GCI 2024) publiée par l'Union Internationale des Télécommunications (UIT), la méthodologie d'évaluation a évolué : l'UIT a abandonné le classement rang par rang strict au profit d'un système de classification par niveaux de maturité (Tiers), allant du Tier 1 (les pays modèles) au Tier 5 (les pays en construction).

Dans cette dernière édition (GCI 2024), la Côte d'Ivoire est classée en Tier 3 (Pays "Établis" / Establishing) avec un score entre 55 -85.

Pour rappel, la SNCS 2021-2025 avait pour vision : *« Sécuriser le cyberespace pour soutenir l'accélération de la transformation digitale et faire de la Côte d'Ivoire le leader africain en cybersécurité*. »[1]

Elle s'articulait autour de :

- six (6) objectifs stratégiques
- auxquels ont été assignés quatorze (14) objectifs spécifiques
- dans un plan de trente (30) actions,

qui constituent le cœur de ladite Stratégie, permettant la concrétisation de la vision de la Côte d'Ivoire d'être leader africain en cybersécurité.

En raison de ce démarrage tardif du bras opérationnel de l'État et des répercussions économiques et logistiques durables de la COVID-19, le bilan d'achèvement des projets s'établit à 30 %.

La période 2021-2025 a principalement permis de bâtir le socle juridique et de mettre en place l'écosystème institutionnel, marqué par la création de l'ANSSI en octobre 2024.

Le défi majeur de la feuille de route 2026-2030 réside désormais dans le franchissement d'un cap : passer de la mise en place des structures au déploiement accéléré et mesurable des grands projets de résilience.

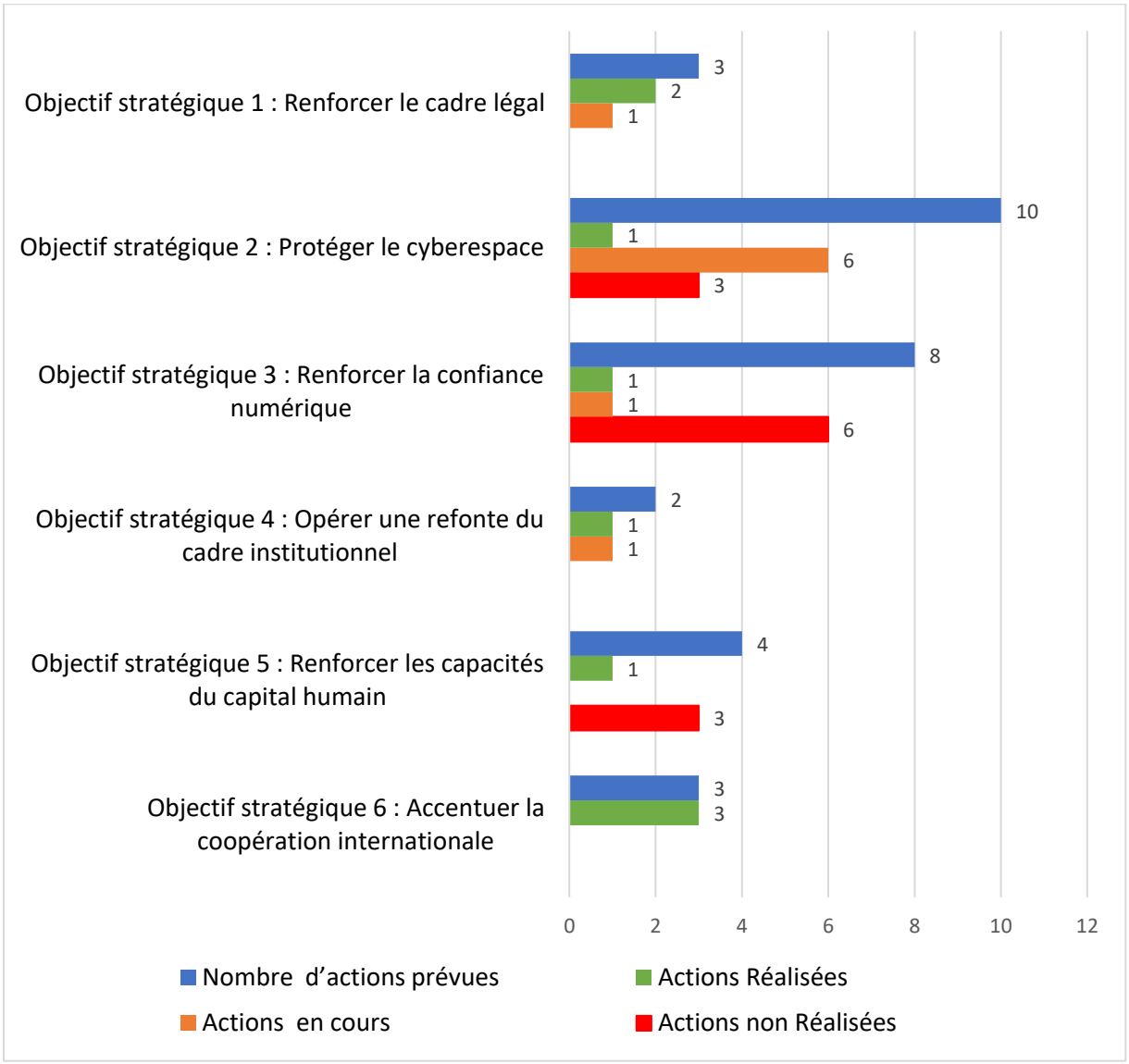
Tableau n°6 : Statuts des actions par catégorie

Catégorie de statut	Nombre d'actions	Pourcentage (sur 30)
Actions réalisées	9	30%
Actions non réalisées	12	40%
Actions en cours	9	30%
TOTAL	30	100%

[1] Source : SNCS 2021-2025

Résumé des actions par Objectif stratégique

Graphique : Niveau de réalisation des actions par objectif stratégique



5. VISION NATIONALE ET PRINCIPES DIRECTEURS

5.1 Enoncé de la Vision de la SNCS 2026-2030

« Promouvoir la confiance, l'éthique et l'excellence, afin de garantir pour chaque citoyen une transformation numérique souveraine et sécurisée en Côte d'Ivoire, à l'horizon 2030. »

5.2 Justification de la Vision 2026-2030

La transformation numérique de la Côte d'Ivoire s'est fortement accélérée au cours de la dernière décennie. Portée par la digitalisation progressive des services publics et l'appui dynamique du secteur privé, elle s'illustre par l'essor des services financiers et administratifs digitaux, la croissance du commerce électronique et la hausse des usages numériques dans la vie quotidienne des citoyens.

Cette évolution qui constitue une opportunité majeure pour le développement économique et social du pays, s'accompagne toutefois, d'une augmentation significative des risques liés à l'usage des services numériques. Les cyberattaques, notamment la fraude en ligne, l'usurpation d'identité et la désinformation, mettent à l'épreuve la résilience de nos infrastructures. Elles représentent désormais, un défi majeur pour la stabilité économique et la confiance numérique.

Dans ce contexte, la cybersécurité s'impose comme un enjeu stratégique majeur, au croisement de la souveraineté numérique, de la stabilité socio-économique et de la protection des citoyens. Garantir la continuité des services critiques et préserver la confiance dans l'économie numérique exigent un cadre solide, fondé sur le respect scrupuleux de nos valeurs pour un développement harmonieux et durable.

Pour répondre à ces exigences, l'État a d'abord structuré son action à travers la Stratégie Nationale de Cybersécurité (SNCS) 2021-2025, qui a permis de poser le cadre juridique avec un nouvel écosystème.

S'inscrivant dans le prolongement direct des orientations inclusives du Plan National de Développement (PND) 2026-2030, la nouvelle SNCS 2026-2030 franchit un cap décisif.

Elle place désormais le citoyen ivoirien au cœur du dispositif, sous le sceau des valeurs d'excellence, d'éthique et de redevabilité. Quelle que soit sa situation géographique sur l'ensemble du territoire, le citoyen devient ainsi l'acteur principal d'un cyberespace souverain et sécurisé, transformant le facteur humain en premier maillon de la résilience nationale.

En outre s'appuyant sur les derniers résultats officiels du Global Cybersecurity Index de l'UIT (GCI 2024) qui classent la Côte d'Ivoire au niveau Tier 3 (Maturité Établie), la SNCS 2026-2030 fixe pour cible l'accès au Tier 1 (Pays Modèle) lors des prochaines évaluations du GCI.

5.3 Valeurs

La SNCS 2026-2030 repose sur quatre (4) valeurs fondamentales qui intègrent les ODD, les Principes du Global Compact des Nations Unies et les orientations du PND 2026-2030 afin d'ancrer la cybersécurité au cœur grands enjeux humains.

À la différence de la stratégie antérieure, cette nouvelle feuille de route est résolument centrée sur le citoyen. Cette vision impose la culture de la cybersécurité et la conduite du changement comme impératifs absolus, portés par des valeurs fortes qui guident notre idéal commun dans la construction d'un cyberespace ivoirien hautement sécurisé et de confiance. Ces valeurs sont :

- **L'éthique**

L'éthique fournit le cadre moral et repose sur le respect des libertés, de la vie privée, la transparence et la dignité humaine. Les pouvoirs publics s'engagent à garantir la loyauté des services numériques, à protéger chaque citoyen contre toute forme de discrimination et à promouvoir un usage responsable des données[2].

- **La Souveraineté**

La souveraineté repose sur la maîtrise des infrastructures critiques et le développement d'une expertise nationale de pointe. A travers cette valeur, les pouvoirs publics s'engagent à bâtir un écosystème numérique autonome, garant d'une croissance économique pérenne et de la sécurité du patrimoine informationnel de la Nation I[3].

- **L'Excellence**

L'excellence constitue l'armure technique indispensable à la protection de notre cyberespace. Elle repose sur l'innovation de pointe, la haute qualification du capital humain et la performance durable. C'est pourquoi l'Etat s'engage à former une élite cyber aux standards mondiaux tout en inscrivant cette dynamique dans une démarche de sobriété énergétique et de respect strict de l'environnement[4].

- **La Confiance**

La réussite numérique repose sur la fiabilité des systèmes et l'intégrité absolue des échanges. Les pouvoirs publics s'engagent à auditer systématiquement les services

[2] ODD 16 Paix, Justice et Institutions efficaces et Global Compact : Principes 1 & 2 Protection des Droits de l'Homme) ;

[3] ODD 1 Pas de pauvreté ; ODD 8 Travail décent et croissance & ODD 9 Industrie, Innovation et Infrastructure et Global Compact : Principes 3, 4, 5 & 6 Respect des Normes du Travail et promotion des talents) PND 2026-2030 : Action 5.03.1.5.5 Sécuriser les infrastructures critiques et lutter contre la cybercriminalité et action 5.03.1.5.1 Renforcer les compétences en cybersécurité ;

[4] Cet engagement s'aligne sur l'ODD 4 Éducation de qualité, l'ODD 13 Lutte contre les changements climatiques, les Principes 7, 8 & 9 du Global Compact des Nations Unies Responsabilité environnementale et technologies propres, ainsi que l'Action 5.03.1.5.1 du PND 2026-2030 « Renforcer les compétences en cybersécurité » ;

publics et à lutter avec fermeté contre la corruption numérique pour sécuriser durablement le climat des affaires et les partenariats[5].

5.4 Principes directeurs

La mise en œuvre de la Stratégie Nationale de Cybersécurité 2026-2030 s'appuie sur un ensemble de principes directeurs qui vont orienter les actions et garantir la cohérence des projets en matière de protection du cyberespace ivoirien.

- **La transparence et la redevabilité**

Le principe de la transparence et de la redevabilité repose sur la responsabilisation des services publics en tant que véritables partenaires du citoyen qui est au cœur de la Stratégie. La SNCS 2026-2030 instaure un cadre où l'efficacité de la protection nationale est mesurable, auditée et communiquée de manière transparente aux parties prenantes « cyber-redevabilité ».

Il implique la réalisation d'audits réguliers et la publication de rapports sur l'état des menaces et les avancées de la SNCS, afin de maintenir la confiance des citoyens et des investisseurs.

- **La primauté du droit et le respect des droits de l'homme et des libertés fondamentales**

Ce principe garantit que les algorithmes et les traitements de données sont auditables et dépourvus de biais, assurant ainsi le respect scrupuleux des droits fondamentaux et de la vie privée[6], conformément aux lois nationales en vigueur et conventions internationales ratifiées par la Côte d'Ivoire.

Au demeurant, l'Etat reconnaît et affirme que l'accès à Internet et aux réseaux de communication électronique est un droit fondamental de l'Homme et un bien universel dont l'établissement, la préservation et la sécurisation restent des priorités nationales auxquelles toute personne physique ou morale doit concourir[7].

En outre, l'accent est mis sur la solidarité, la défense des plus vulnérables (la protection des enfants en ligne[8]) et la réduction de la fracture numérique. C'est la « cyber-solidarité ».

- **La responsabilité partagée et la coopération**

[5] ODD 17 (Partenariats pour la réalisation des objectifs) & ODD 16 (Transparence et Intégrité) et Global Compact : Principe 10 (Lutte contre la corruption sous toutes ses formes). PND 2026-2030 action 5.03.1.5.2 Certifier et qualifier des services de confiance numérique

[6] ODD 16 | Global Compact (Principes 1-2)

[7] Article 3 de la loi n°2017-803 du 07 décembre 2017 d'orientation de la société de l'information en CI

[8] ODD 17 (Partenariats pour la réalisation des objectifs) et Global Compact : Principe 10 (Intégrité et lutte contre la corruption par la transparence)

Ce principe traduit la volonté de toutes les parties prenantes à lutter contre la cybercriminalité aux côtés de l'Etat de Côte d'Ivoire, aussi bien sur le territoire national qu'au-delà de nos frontières. Loin d'être une contrainte, la cybersécurité est le bouclier qui protège les vies, les emplois, les investissements et la dignité des populations.

A cet effet, chaque utilisateur devient un acteur de la sécurité en mettant en œuvre les règles fondamentales d'hygiène numérique pour se préserver et protéger notre cyberespace commun. A travers ce principe, l'Etat s'engage à coopérer et à collaborer avec l'ensemble des parties prenantes issues du secteur public, privé et du monde académique sans oublier la population.

La sécurité numérique devient une responsabilité collective et nationale, posant ainsi les fondements de notre cyber partenariat, et à l'échelle international, de notre cyberdiplomatie.

- **Le développement de l'innovation numérique**

La cybersécurité n'est plus seulement un facteur de développement, elle devient un véritable outil de souveraineté, grâce au déploiement d'infrastructures critiques notamment le SOC national, le Cloud national sécurisé et le développement d'une intelligence artificielle de souveraineté ivoirienne.

L'État soutient la recherche et l'innovation locales ainsi que la promotion des start-ups spécialisées en cybersécurité « cyber-champions nationaux » et la création d'emplois qualifiés pour garantir une performance technologique durable et une autonomie stratégique[9].

[9] ODD 4 (Éducation de qualité) & ODD 9 (Industrie, Innovation et Infrastructure) et Global Compact : Principes 7, 8 & 9 (Responsabilité environnementale et technologies respectueuses du climat).

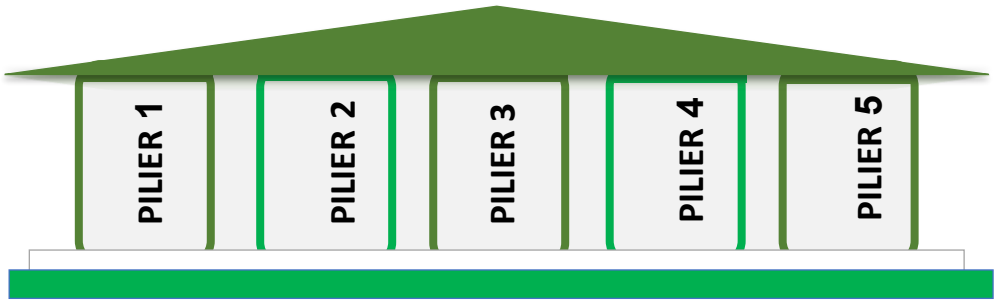
6. PILIERS DE LA SNCS 2026-2030

En faisant du numérique un pilier majeur de la transformation structurelle de l'économie national à l'horizon 2030, le PND 2026-2030 assigne au secteur une ambition d'attractivité et de croissance sans précédent.

Toutefois, l'expansion de cet écosystème numérique ne peut être pérenne sans un environnement d'affaires sécurisé et souverain. C'est à ce croisement stratégique que s'articule la nouvelle Stratégie Nationale de Cybersécurité (SNCS 2026-2030).

Elle constitue le socle de confiance indispensable garantissant la résilience des infrastructures critiques de l'État, la protection des données des citoyens et la crédibilité internationale du hub digital ivoirien.

A cet effet, la SNCS 2026-2030 s'appuie sur cinq (5) piliers qui sont les véritables fondations opérationnelles. Ces cinq (5) piliers sont :



- Pilier 1 : Gouvernance éthique et cadre légal
- Pilier 2 : Capital humain et innovation
- Pilier 3 : Protection des Infrastructures Critiques et Cyber résilience
- Pilier 4 : Capacités techniques et opérationnelles de l'État
- Pilier 5 : Coopération nationale et Rayonnement International

Dans chaque Pilier, le Gouvernement ivoirien s'emploiera à atteindre des objectifs stratégiques en réalisant des actions précises.

Pour chaque action, les livrables (preuves matérielles de la réalisation) sont indiqués et les indicateurs de Performance (KPI) permettant de mesurer l'efficacité réelle sont précisés.

Au total la SNCS 2026-2030 s'articule autour de :

L'Annexe 1 définit le cadre logique de la mise en œuvre de la SNCS 2026-2030.

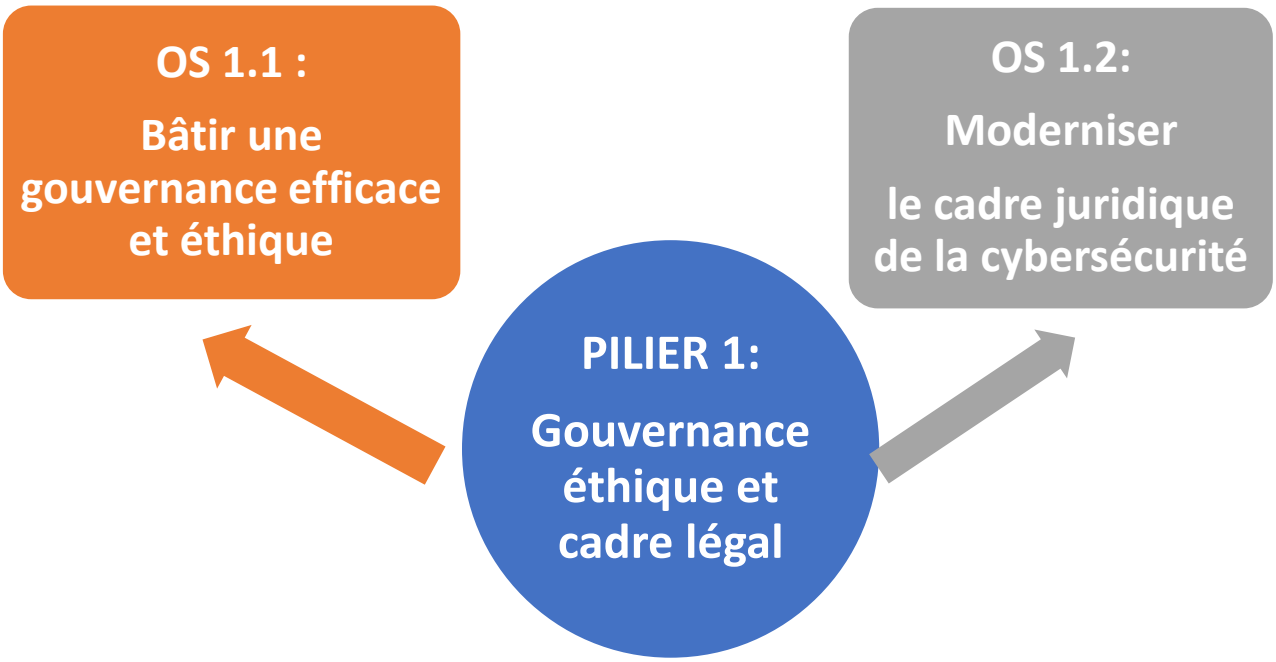
L'Annexe 3 présente de façon détaillée, le plan d'actions de la SNCS 2026-2030.

6.1 PILIER 1 : Gouvernance éthique et cadre légal

La gouvernance nationale de la cybersécurité s'organise autour d'un cadre institutionnel clarifié et d'un dispositif juridique modernisé. L'action publique gagne en cohérence, en efficacité et en transparence, tout en renforçant la coordination entre les acteurs et l'adaptation du cadre légal aux évolutions technologiques.

Le pilier 1 repose sur:

- deux (2) Objectifs Stratégiques (2 OS)
- et sept (7) Actions à réaliser .



OS 1.1 : Pilier 1 Objectif Stratégique 1

OS 1.2 : Pilier 1 Objectif Stratégique 2

Objectif Stratégique (OS 1.1) : Bâtir une gouvernance efficace et éthique

La SNCS 2021-2025 a ancré l'Agence Nationale de Sécurité des Systèmes d'Information 'ANSSI' dans le paysage institutionnel de la Cybersécurité en Côte d'Ivoire. La priorité est désormais de lever les zones d'ombre décisionnelles et les éventuels conflits de compétences, à travers la mise en place d'une gouvernance efficace et éthique.

Une gouvernance efficace repose sur une répartition claire des responsabilités pour éviter toute paralysie en cas de crise. Cette efficacité opérationnelle couplée de l'éthique garantit que chaque action de sécurité est menée avec transparence dans le respect rigoureux des droits fondamentaux de tous les acteurs, en particulier du citoyen et conformément aux procédures écrites.

Quatre (4) actions à réaliser :

- **OS 1.1. Action 1 : Impulser la montée en puissance de l'ANSSI sur l'ensemble des administrations publiques et les départements ministériels**

L'ANSSI exerce pleinement ses missions sur l'ensemble des administrations publiques, des départements ministériels, des entreprises publiques et des collectivités territoriales.

A cette fin, elle déploie des capacités nationales de cybersécurité à la hauteur des enjeux et apporte son expertise technique à la lutte contre la cybercriminalité au sein de l'État.

Son action repose sur une articulation étroite avec les ministères et les autorités sectorielles compétentes afin de coconstruire un cadre de coopération adapté aux spécificités de chaque entité et de chaque secteur dans la protection des systèmes d'informations publics.

Cette démarche va permettre d'assurer une protection appropriée aux risques auxquels chaque secteur devrait être approprié.

L'ANSSI veille au respect des exigences réglementaires notamment, au moyen de référentiels clairs, de lignes directrices, de procédures de suivi formalisées et d'audits par secteur d'activité, garantissant une montée en résilience globale de l'État, dans le strict respect de la transparence et de l'éthique administrative.

Pour piloter cette action, l'ANSSI disposera d'une feuille de route stratégique claire, adossée à des indicateurs de performance précis. Cet outil de pilotage permettra de prouver de manière structurée l'avancement de la résilience publique.

OS 1.1. Action 2 : Instaurer un cadre formel de concertation entre les acteurs publics et les Exploitants d'Infrastructures d'Information Critique (IIC)

La sécurité des infrastructures nationales repose sur une synergie étroite entre les acteurs publics et les Exploitants d'IIC. La mise en place d'un cadre national de gouvernance efficace et éthique permet le dialogue entre les acteurs et la coordination des différentes activités profitables à tous.

Cette approche partenariale permettra d'adapter les exigences de sécurité aux réalités métiers de chaque domaine économique, de renforcer leur résilience et leur capacité de reprise. Elle garantit ainsi aux Exploitants d'IIC, une protection optimale de leurs actifs critiques, dans le respect absolu du secret des affaires, des règles de déontologie et de la confiance mutuelle.

Dans le cadre cette action, l'ANSSI procédera à la signature de protocoles d'accord ou d'accords-cadres avec les différentes entités concernées afin de définir les responsabilités de chaque partie.

- **OS 1.1. Action 3 : Mettre en place un observatoire de confiance numérique au sein de l'ANSSI**

L'Observatoire de la confiance numérique est créé au sein de l'ANSSI. Il a pour mission de mesurer l'état de la menace cyber, d'évaluer le niveau de résilience des systèmes d'information et d'analyser l'impact des attaques sur la société.

Il veille à ce que le renforcement de la cybersécurité nationale s'accompagne d'une garantie absolue de sécurité et de confidentialité des données pour tous les acteurs, y compris les citoyens, les protégeant ainsi contre les cybermenaces et les usurpations numériques.

En accordant une attention particulière à la sécurisation des services publics aux personnes vulnérables, cette démarche donne à l'État, la légitimité nécessaire pour bâtir une confiance durable avec la population et garantir un espace numérique national résilient et sûr.

Dès le lancement de l'Observatoire**,** l'ANSSI rédigera la Charte d'éthique et de responsabilité numérique. C'est un référentiel qui définit les principes déontologiques applicables à la collecte de données, à la surveillance des réseaux publics et à la gestion des incidents, afin de garantir un équilibre strict entre impératifs de sécurité et respect des droits fondamentaux.

OS 1. 1. Action 4 : Mettre en place le Comité de suivi de la SNCS

Elaborer un mécanisme institutionnel de suivi, d'évaluation et de revue périodique de la SNCS en mettant en place le Comité de suivi de la SNCS.

L’organisation et le fonctionnement sont détaillés dans la suite de la présente SNCS.

Objectif Stratégique (OS 1.2) : Moderniser le cadre juridique de la cybersécurité

Cet objectif vise à procéder à la mise à jour régulière du cadre juridique de la cybersécurité afin de s’assurer de sa cohérence aux réalités du terrain et à l’évolution de l’écosystème, en étroite relation avec les parties prenantes concernées.

Cette modernisation du cadre juridique de la cybersécurité de façon concertée avec les différentes parties prenantes. Elle nécessite une veille sur les technologies numériques et le paysage de la cybersécurité.

Deux (2) actions à réaliser :

- **OS 1.2. Action 5 : Réviser et harmoniser le cadre juridique existant**

La pertinence du dispositif national de cybersécurité dépend directement de la capacité du cadre juridique à s’adapter au rythme des évolutions des cybermenaces, à travers la révision et le renforcement des textes existants. La création de l'ANSSI rend indispensable cette mise à jour.

Réviser les textes sectoriels existants notamment, les lois relatives à la cybercriminalité, aux transactions électroniques et aux communications électroniques ; ainsi que le décret sur le CI-CERT, les décrets n°2021-911 et suivants .

Cette révision consacrera formellement l'ANSSI comme l'entité nationale de référence en matière de cybersécurité. Elle permettra d'éliminer les chevauchements de compétences avec les régulateurs sectoriels, garantissant ainsi une gouvernance claire, cohérente et souveraine, tout en dotant l’ANSSI des prérogatives nécessaires pour sanctionner les manquements à la réglementation.

OS 1.2 Action 6 : Renforcer l’arsenal juridiques par de nouveaux textes

Renforcer le cadre juridique en s’appuyant sur une analyse préalable des lacunes et déficits des textes actuels, suivie de l’élaboration de nouveaux instruments juridiques structurant destinés à encadrer les nouveaux enjeux de la cybersécurité, notamment la loi sur la cybersécurité intégrant le régime juridique des CERT sectoriels tels que le CERT bancaire/financier et le CERT pour les télécommunications) interconnectés au CI-CERT national, la divulgation coordonnée des vulnérabilités, le partage d’information sur les cybermenaces Cette future loi et ses décrets d’application offrira la garantie d’une résilience adaptée aux réalités de chaque secteur critique et assura la protection des données transmises, du secret des affaires et du secret bancaire.

Ce renforcement continu repose sur la mise en place d'une cellule de veille stratégique et prospective au sein de l'ANSSI, chargée de suivre les évolutions réglementaires, les mutations technologiques et l'émergence des nouvelles cybermenaces.

- **OS 1.2. Action 7 : Mettre en place des mécanismes de révision des textes juridiques**

L’objectif est de procéder à la mise à jour régulière des textes **afin de les rendre** conformes à l’évolution des cybermenaces et aux pratiques internationales.

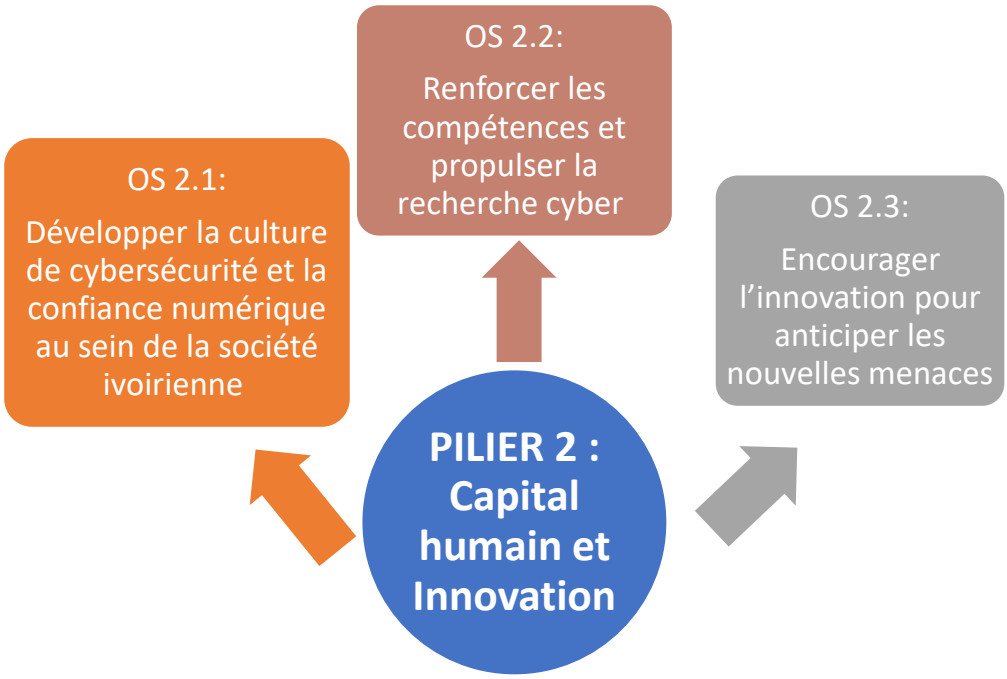
Cette activité sera réalisée en concertation avec les parties prenantes y compris la population.

6.2 PILIER 2 : Capital humain et Innovation

La montée en compétences et la structuration de l'innovation soutiennent l'autonomie nationale en cybersécurité. L'Etat de Côte d'Ivoire accorde une importance particulière au renforcement du capital humain à travers plusieurs initiatives de formation à l'endroit de l'ensemble de la population. Un intérêt particulier est accordé à l'innovation en cybersécurité.

Le pilier 2 repose sur :

- Trois (3) objectifs stratégiques (3 OS)
- et neuf (9) actions à réaliser.



OS 2.1 : Pilier 2 Objectif Stratégique 1

OS 2.2 : Pilier 2 Objectif Stratégique 2

OS 2.3 : Pilier 2 Objectif Stratégique 3

Objectif stratégique 2.1 : Développer la culture de cybersécurité et la confiance numérique au sein de la société ivoirienne

Dans le nouveau contrat social, l'Etat ivoirien change de paradigme en mettant le citoyen, souvent victime de cyberattaque par manque de connaissance ou ignorance, au cœur de la stratégie. Dans la SNCS 26-30, le citoyen devient le maillon fort et l'acteur principal de sa propre protection. Il ne subit plus la sécurité. Il l'incarne. L'Etat développe la confiance numérique chez ses citoyens.

Quatre (4) Actions à réaliser :

- **OS 2.1 Action 8 : Développer une culture cybersécurité des populations y compris des personnes vulnérables**

Former et éduquer les citoyens aux enjeux de la cybersécurité est la priorité de la nouvelle stratégie. Si le citoyen est formé, conscientisé et avertit des peines encourues en cas de réalisation d'actes de cybercriminalité, il est capable de d'éliminer les menaces avant même qu'elles n'atteignent les systèmes de l'Etat. Ce qui renforce directement la sécurité du cyberespace national et la résilience collective de notre société.

L'ANSSI initiera ou encouragera des campagnes périodiques de sensibilisation à la cybersécurité et à la protection des données sur les réseaux sociaux. Menées en partenariat avec la société civile, le secteur public et le secteur privé, ces actions cibleront l'ensemble de la population, avec une attention particulière portée aux personnes vulnérables, afin de promouvoir l'hygiène informatique et les bonnes pratiques numériques

Afin de toucher l'ensemble de la population sur toute l'étendue du territoire et réduire la fracture numérique, tous les canaux de communication devront être utilisés et les messages traduits en langues locales à travers les radios de proximité, (radios locales, langues nationales, leaders communautaires) et la télévision nationale.

L'ANSSI désignera et formera des ambassadeurs de la cybersécurité auprès des mairies, préfectures, commissariats pour relayer ses messages de formation. Les acteurs désignés seront chargés également de surveiller la mise en œuvre, évaluer les résultats de ces activités et recommander des changements, si nécessaire.

Pour les populations vulnérables :

- renforcer les sanctions pour les infractions commises contre elles ;
- simplifier les mécanismes de dénonciation (plateformes dédiées, numéros verts) pour que les victimes, même peu familières avec le droit, puissent obtenir réparation ;
- Imposer ou inciter fortement les plateformes et applications éducatives utilisées dans le cadre scolaire ou public à respecter des critères stricts de protection des mineurs.

OS 2.1 Action 9 : Organiser des campagnes de renforcement des compétences au bénéfice des professionnels des secteurs public et privé

L'ANSSI désignera une période de l'année pour réaliser des forums nationaux de de formation en cybersécurité regroupant les professionnels de l'Administration publique et des entreprises d'infrastructures critiques ainsi que ceux issus des Petites et Moyennes Entreprises avec pour objectif de se conformer à la règlementation en vigueur. Des formations spécifiques seront organisées à l'attention des experts en particulier du secteur public pour développer l'offre de professionnels qualifiés en cybersécurité.

OS 2.1 Action 10 : Encourager la formation des décideurs publics et des IIC

La Cybersécurité est l'affaire de l'ensemble du personnel y compris le top management, les membres des organes de direction, les décideurs publics et privés des exploitants d'importance critiques qui sont tenus de suivre une formation (au moins une formation dans l'année). Un membre du comité de Direction peut être désigné responsable cyber. Cette responsabilité fait partie intégrante de la fiche de poste du Directeur.

Dans leur rapport sur le déploiement de la cybersécurité, les services de l'Administration et les exploitants IIC informent l'ANSSI des programmes de formation suivi par leur Top management.

OS 2.1 Action 11 : Encourager le recours à l'expertise qualifiée locale pour réaliser des audits de sécurité ou des prestations de conseil et créer des emplois locaux.

Toutes les entités qualifiées de sensibles selon la démarche d'analyse de risque de l'ANSSI, devront disposer de ressources internes qualifiées pour réaliser les audits de sécurité des systèmes d'information.

L'ANSSI devra s'appuyer sur les parties prenantes pour mettre en place un planning de formation continue pour les professionnels de l'informatique en général et de la sécurité en particulier en service dans les administrations en vue de former des auditeurs.

Objectif Stratégique OS 2.2 : Renforcer les compétences en cybersécurité et propulser la recherche cyber

Le développement des compétences renforce l'autonomie nationale et améliore la capacité du pays à répondre aux menaces. La structuration d'un dispositif de formation et de recherche permet de disposer de ressources humaines qualifiées et de produire des connaissances adaptées aux réalités locales.

Trois (3) Actions à réaliser :

- **OS 2.2 Action 12 : Renforcer les capacités des centres publics de formation et encourager la promotion des carrières en cybersécurité**

Investir dans la formation en cybersécurité pour développer un vivier d'experts et consolider notre souveraineté numérique. À cet effet, des catalogues de formations, des parcours certifiants et des cursus diplômants seront élaborés en étroite collaboration entre l'ANSSI et nos universités et grandes écoles, notamment l'INPHB, l'ENSEA, l'ESATIC, l'Université Virtuelle, l'ENS, le CAFOP, l'UFR de criminologie des Universités, etc.

Ce catalogue de formation intégrera également des programmes spécialisés pour renforcer les capacités des forces de défenses et de sécurité telles que l'Ecole de Police, la Gendarmerie Nationale et assurer la mise à niveau agents publics en formation au Centre de Perfectionnement des Fonctionnaires et Agents de l'Etat (CPFA) ainsi que des hauts fonctionnaires en formation à l'Ecole Nationale d'Administration (ENA).

Le milieu académique en relation avec l'ANSSI procèdera à la révision des contenus de formation pour répondre aux besoins opérationnels du marché national Cette dynamique sera adossée à un programme national de stages et d'apprentissage en entreprise, facilitant le transfert de compétences pratiques et l'employabilité directe des jeunes diplômés.

- **OS 2.2 Action 13 : Mettre en place un programme national de sensibilisation en milieu scolaire**

En collaboration avec les ministères en charge de l'éducation, des modules adaptés seront intégrés au parcours scolaire (écoles et lycées) afin de sensibiliser les élèves et développer la culture cyber chez ces jeunes usagers.

Au-delà de cette première acculturation, la création d'un programme de bourses d'excellence permettra d'attirer et d'accompagner les meilleurs élèves vers les cursus spécialisés en cybersécurité.

- **OS 2.2 Action 14 : Déployer un programme national de certification en cybersécurité, encourager les recherches en cybersécurité**

Le renforcement des compétences et de la recherche améliore la capacité nationale d'analyse, réduit la dépendance aux solutions externes et favorise l'émergence d'expertises locales reconnues.

Le gouvernement ivoirien encouragera les recherches dans le secteur de la cybersécurité en relation avec le milieu académique. Il facilitera la création d'un cadre d'échange et de discussion entre les experts de la cybersécurité et les professeurs de l'enseignement supérieur de la Côte d'Ivoire ou en relation ceux de l'étranger pour encourager la recherche et le développement dans la cybersécurité.

Objectif stratégique 2.3 : Encourager l'innovation pour anticiper les nouvelles menaces

La capacité à anticiper les menaces repose sur l'émergence de solutions technologiques adaptées aux réalités nationales. L'innovation locale permet de concevoir des outils pertinents, de réduire les dépendances technologiques et d'accélérer les réponses face aux évolutions du cyberespace.

Les actions engagées soutiennent la création et la croissance de start-ups spécialisées, accompagnent les projets innovants et structurent les collaborations entre acteurs publics, privés et académiques. Un mécanisme de financement dédié à la cybersécurité permet d'assurer la continuité et la montée en puissance de ces initiatives pour contribuer à l'employabilité et insertion des jeunes.

Deux (2) Actions à réaliser :

- **OS 2.3 Action 15 : Mettre en place un programme de laboratoires communs public-privé (LabCom Cyber)**

Les actions engagées alignent les programmes académiques et professionnels sur les besoins du marché, renforcent les compétences des acteurs publics et privés et soutiennent les initiatives de recherche appliquée.

Il convient de mettre en place des Laboratoires Communs dédiés à la cybersécurité (LabCom Cyber) associant les institutions académiques, les centres de recherches, le secteur privé et les organismes de sécurité nationale.

Ces LabCom vise à :

- développer des technologies et méthodes souveraines pour répondre aux menaces émergentes et protéger les infrastructures critiques.
- encourager et accompagner le dépôt de brevets par les enseignants-chercheurs, doctorants et étudiants afin de valoriser la propriété intellectuelle nationale.
- accélérer le transfert de technologie et la création de startups innovantes en cybersécurité (Cybertechs).

- **OS 2.1 Action 16 : Organiser des concours de projets innovants**

Afin de pouvoir déceler de nouveaux talents et animer l'écosystème de cybersécurité, des concours de projets innovants et des compétitions de cybersécurité seront organisés de manière périodique.

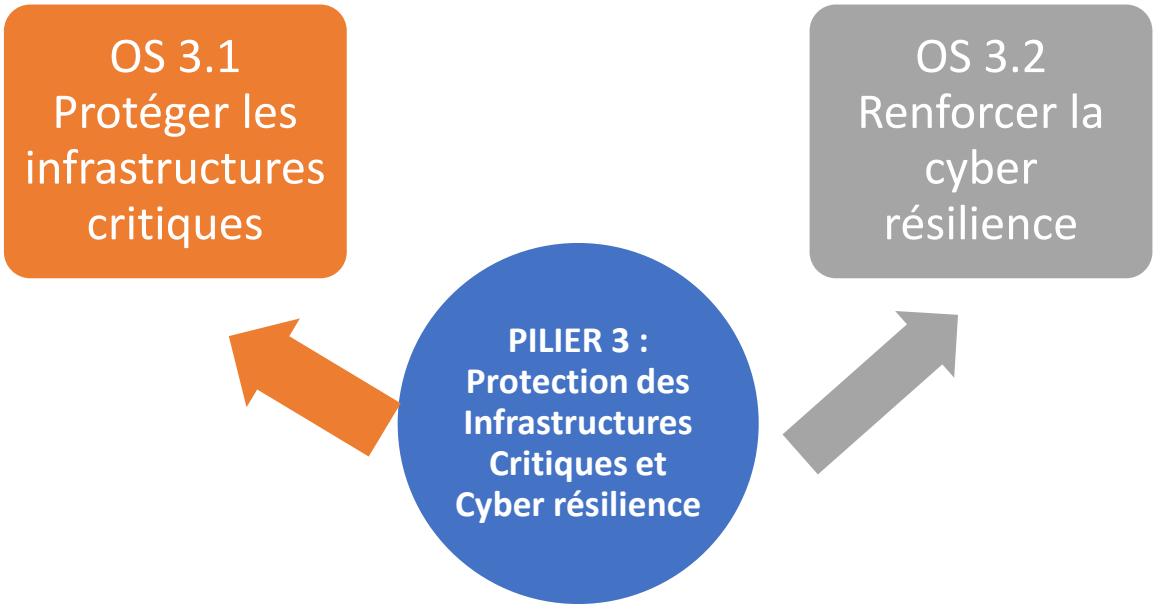
En lien avec le Ministère de la Jeunesse offrir des facilités aux jeunes sur les projets innovants en matière de cybersécurité.

6.3 PILIER 3 : Protection des Infrastructures Critiques et Cyber résilience

La sécurisation des infrastructures critiques et le renforcement de la résilience structurent la capacité de la Côte d'Ivoire à maintenir ses fonctions essentielles. L'exposition aux risques diminue, la continuité des services s'améliore et la gestion des incidents majeurs gagne en efficacité.

Le pilier 3 repose sur :

- deux (2) Objectifs Stratégiques (2 OS)
- et sept (7) Actions à réaliser.



OS 3.1 : Pilier 3 Objectif Stratégique 1

OS 3.2 : Pilier 3 Objectif Stratégique 2

Objectif Stratégique OS 3.1 : Protéger les infrastructures critiques

Cet objectif organise une démarche nationale de sécurisation fondée sur l'identification des infrastructures critiques, l'évaluation des risques et le déploiement des mesures de protection adaptées à partir du décret n°2021-916 du 22 décembre 2021 portant adoption du Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Critiques.

Deux (2) Actions à réaliser :

- **OS 3.1. Action 17 : Réaliser une étude nationale d'identification et d'évaluation des infrastructures critiques et non critiques**

Cette approche repose sur une connaissance précise et actualisée des infrastructures critiques et non critiques et de leurs systèmes d'information, permettant de prioriser les efforts de sécurisation et de réduire les surfaces d'exposition.

Elle intègre également l'alignement des prestataires de services numériques sur des standards de sécurité reconnus afin d'élever le niveau global de protection de l'écosystème.

- **OS 3.1. Action 18 : Mettre en œuvre le plan national de protection des infrastructures critiques**

Cette action consiste à mettre en œuvre le Plan de Protection des Infrastructures Critiques adoptés par le décret n°2021-916 du 22 décembre 2021.

Objectif stratégique 3.2 : Renforcer la cyber résilience

La continuité des services critiques dépend de la capacité des organisations à gérer efficacement les situations de crise. Cet objectif renforce la cyber résilience des institutions publiques et des opérateurs d'infrastructures critiques en structurant des mécanismes permettant d'anticiper, de résister, de se rétablir et de s'adapter aux incidents cyber.

Il s'appuie sur le déploiement de dispositifs de gestion de crise, de continuité et de reprise d'activité, ainsi que sur l'organisation d'exercices réguliers destinés à tester et améliorer les capacités de réponse. L'intégration de la résilience dans les processus organisationnels et techniques permet de limiter les impacts et de sécuriser la reprise des activités.

Sa mise en œuvre garantit la continuité des services essentiels, réduit les délais de rétablissement et renforce la capacité des acteurs à gérer des incidents majeurs.

Cinq (5) actions à réaliser :

- **OS 3.2. Action 19: Élaborer et mettre en œuvre un plan national de gestion des crises cyber**

Pour garantir une préparation efficace face aux crises cyber, l'ANSSI élaborera un plan national de gestion des crises et éventuellement des plans de gestion des crises, intégrant une connaissance approfondie du paysage des menaces.

Un comité de gestion de crise sera également mis en place pour superviser et coordonner les actions en cas d'urgence. Une plateforme d'échange d'information dédiée sera employée pour faciliter la coordination et la transmission des données critiques en temps réel. L'efficacité de ces dispositifs sera assurée par des tests périodiques, des plans relatifs au partage d'informations et à la gestion des incidents.

L'ANSSI organisera des exercices de cybersécurité de manière périodique, tant au niveau des équipes qu'à l'échelle nationale.

La mise en œuvre du plan national de gestion des crises cyber exige l'élaboration des procédures et une politique de communication de crise applicables également.

- **OS 3.2. Action 20 : Élaborer un catalogue national de services de cybersécurité adaptés aux besoins des collectivités territoriales**

L'ANSSI doit élaborer un catalogue national de services prenant en compte les différents secteurs critiques, tout en collaborant avec les collectivités territoriales qui en seront les relais naturels. Ce catalogue permettra d'offrir une réponse structurée et adaptée aux besoins de chaque entité, garantissant que la sécurité numérique ne reste pas centralisée.

Afin d'opérationnaliser ce maillage sur l'ensemble du territoire, des référents cybersécurité seront désignés au sein de chaque collectivité territoriale. Ils auront pour mission d'assurer la déclinaison locale des directives de l'ANSSI, de veiller à la sécurisation des systèmes d'information de ces collectivités et de faciliter la remontée rapide des incidents, renforçant ainsi la résilience globale de la Nation.

- **OS 3.2 Action 21: Auditer des institutions publiques et des collectivités territoriales aux référentiels et cadres techniques nationaux en vigueur**

Des institutions publiques et des collectivités territoriales mal protégées constituent des portes d'entrée pour attaquer l'État. En assurant leur mise en conformité au cadre technique en vigueur, on évite le "maillon faible" et on garantit que chaque entité publique applique les mêmes règles et dispose d'un bouclier minimum contre les cyberattaques.

A cet effet, l'ANSSI élaborera un guide d'évaluation adaptant les exigences du RGSSI pour évaluer le niveau de maturité cyber des institutions et des entreprises ivoiriennes.

- **OS 3.2. Action 22 : Mettre en place un cadre national de sécurité des systèmes d'information intégrant l'intelligence artificielle**

Il faut aller au-delà de la protection du matériel ou du système d'information pour s'assurer que l'intelligence artificielle qui le pilote est fiable, éthique et sécurisée, notamment par des audits algorithmiques réguliers, l'évaluation de la sécurité et conformité des systèmes IA et la création d'une certification spécifique pour garantir que les solutions respectent ces normes de sécurité intrinsèques et d'éthique, en lien avec l'Autorité nationale de supervision de l'IA.[10]

- **OS 3.2. Action 23 : Encourager la cyber-assurance dans la politique nationale de résilience des secteurs critique**

Renforcer la résilience des infrastructures d'information critiques (IIC) implique d'associer la sécurité technique à des mécanismes de gestion du risque résiduel. L'État souhaite ainsi intégrer la cyber-assurance comme levier d'incitation à l'hygiène numérique et de couverture des impacts majeurs.

Un diagnostic stratégique préalable permettra d'évaluer la maturité effective des Exploitants de IIC, de mesurer la capacité du marché de l'assurance face au risque systémique et de fixer la position sur le paiement des rançons.

Ce bilan servira de socle à la réglementation : l'accès aux garanties sera conditionné au respect de normes de sécurité obligatoires, adossé à des mécanismes de réassurance dans le respect des exigences du code CIMA.

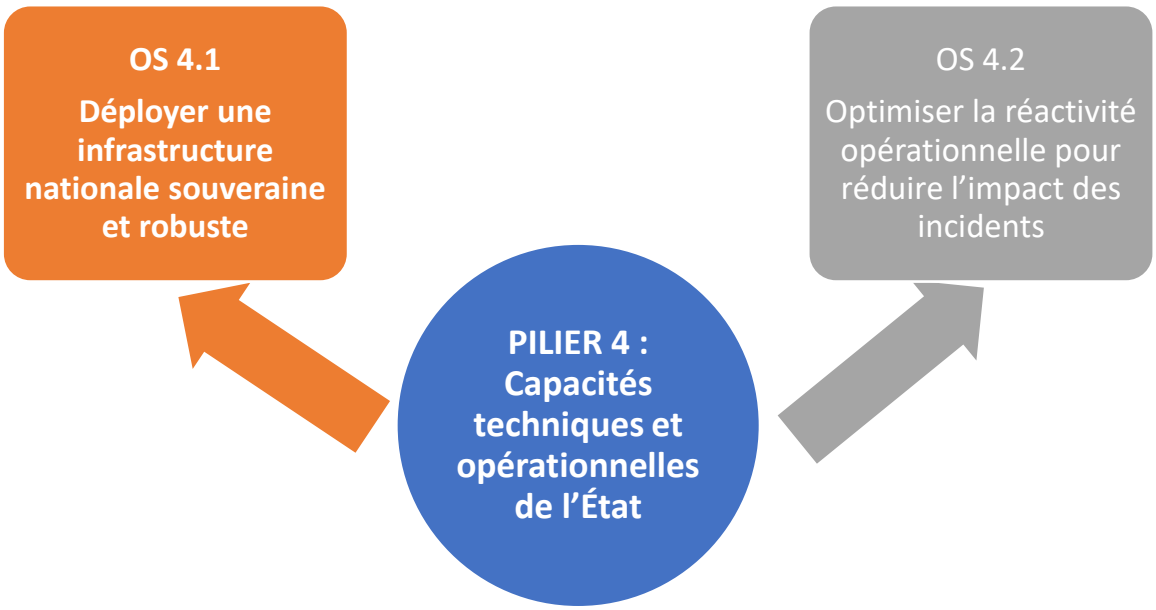
[10] Stratégie Nationale de l'Intelligence Artificielle

6.4 PILIER 4 : Capacités techniques et opérationnelles de l'État

Le développement de capacités techniques avancées renforce la maîtrise des systèmes critiques et améliore la gestion des incidents. La détection, l'analyse et la réponse gagnent en efficacité, garantissant la sécurité et la disponibilité des services numériques publics.

Le pilier 4 repose sur :

- Deux (2) objectifs stratégiques (2 OS)
- et neuf (10) actions à réaliser.



OS 4.1 : Pilier 4 Objectif Stratégique 1

OS 4.2 : Pilier 4 Objectif Stratégique 2

Objectif stratégique OS 4.1 : Développer les moyens de gestion des incidents

Le déploiement d'une infrastructure nationale souveraine confère à l'État la pleine-maîtrise ses données, de ses architectures critiques et ses capacités numériques. Une telle démarche structure les moyens techniques nécessaires pour assurer une surveillance continue, détecter les menaces et protéger les actifs stratégiques du pays.

Deux (2) Actions à réaliser :

- **OS 4.1 Action 24 : Mettre en place un centre national de Supervision des réseaux et services d'information critiques (SOC)**

L'architecture s'appuie sur des dispositifs centralisés et interconnectés capables de collecter, corréler et analyser les événements de sécurité à l'échelle nationale. Elle intègre notamment la mise en place d'un Centre Opérationnel de Sécurité (SOC) national, offrant une visibilité consolidée sur les incidents. Le SOC a pour mission de détecter, d'assurer le suivi et la supervision de la sécurité en temps réel 24h/7.

- **OS 4.1 Action 25 : Renforcer le laboratoire national de forensique pour les analyses numériques**

Le renforcement des capacités du laboratoire d'investigation forensique aidera la Côte d'Ivoire dans sa perspective d'améliorer ses activités d'acquisition et d'analyse scientifique des preuves numériques liées à des infractions pénales, ou des incidents nécessitant une expertise technique.

Cette amélioration impactera l'intégration des normes du domaine dans les processus opérationnels et la création d'une unité de recherche et développement ouvrant des perspectives d'autonomisation. Cela permettra au laboratoire de consolider sa position centrale dans le système judiciaire, en fournissant des preuves objectives pour éclairer les enquêtes et les procédures judiciaires.

Le renforcement du laboratoire d'investigation forensique aidera la Côte d'Ivoire dans sa perspective de développer des activités efficaces de veille pour la détection des menaces.

L'ANSSI apportera un appui technologique aux juridictions, aux forces de défenses et de sécurité ainsi que les services de renseignement.

Objectif stratégique OS 4.2 : Optimiser la réactivité opérationnelle pour réduire l'impact des incidents

L'amélioration de la réactivité opérationnelle repose sur une organisation capable de détecter rapidement les incidents, de contenir leur propagation, de limiter leurs impacts et à restaurer les services essentiels dans des délais maîtrisés.

Le dispositif s'appuie sur le renforcement des capacités du CI-CERT, la création de CERT sectoriels et la structuration des mécanismes de coordination entre équipes techniques, autorités compétentes et opérateurs de services essentiels.

Une réponse mieux organisée réduit les impacts opérationnels, améliore la gestion des incidents majeurs et renforce la capacité d'action collective face aux attaques.

Cinq (5) Actions à réaliser :

- **OS 4.2 Action 26 : Renforcer le CI-CERT et mettre en place des CERT sectoriels**

En rapprochant l'expertise de l'ANSSI du terrain vers des CERT sectoriels, il se crée un bouclier multisectoriel où chaque secteur protège ses pairs sans jamais compromettre le secret des affaires.

- CERT Telecom/Numérique : Opérateurs, FAI, datacenters. Focus sur les attaques DDoS, le détournement BGP et la sécurité des liaisons critiques
- CERT-Finance : Banques, assurances, microfinance, systèmes de paiement mobile. Focus sur le détournement de fonds, les ransomwares et la fraude transactionnelle.
- CERT-Énergie & Infrastructures : Électricité, eau, hydrocarbures. Focus sur la protection des systèmes SCADA/ICS et l'OT (Technologies Opérationnelles).
- CERT-Santé / Administration : Protections des données sensibles des citoyens (liées à la santé) et de la continuité des services publics.

Les échanges entre le CI-CERT et les CERT sectoriels se font sur des canaux chiffrés hors réseaux publics.

Garantie sur le secret des données : Les équipes d'investigation forensiques du CERT manipulent uniquement les artefacts techniques (fichiers journaux, empreintes mémoire, exécutables malveillants) et ne touchent jamais au contenu propre des données à caractère personnel ou médical des citoyens

- **OS 4.2 Action 27 : Consécration du poste de RSSI et opérationnalisation du réseau des RSSI des entités de l'Etat**

(i) **Consécration du poste de RSSI**

Pour renforcer la cybersécurité et garantir une protection unifiée des systèmes d'information, il est proposé de consacrer officiellement le poste de Responsable de la Sécurité des Systèmes d'Information (RSSI) dans chaque entité étatique, en définissant clairement son positionnement hiérarchique. Cette mesure visera à structurer et harmoniser la cybersécurité à l'échelle de l'État, en alignant les pratiques de sécurité avec les enjeux stratégiques.

Dans ce contexte, il sera nécessaire d'instituer une unité dédiée à la sécurité de l'information dans chaque entité de l'État. Ainsi, chaque entité aura une unité organisationnelle spécialisée, placée sous l'autorité du RSSI. Cette structure aura pour missions :

- de piloter la mise en œuvre des politiques de sécurité,

- d'intégrer la cybersécurité dans les processus métiers,
- de coordonner les actions de protection au sein de l'entité.

L'ensemble de ces dispositifs sera supervisé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui assurera :

- la cohérence globale des mesures de sécurité,
- le contrôle des activités du RSSI et de son unité,
- l'harmonisation des budgets et des rôles pour une approche unifiée.

Pour garantir les moyens nécessaires des ressources budgétaires devront être allouées :

- au RSSI, pour le pilotage stratégique et la coordination,
- à l'unité organisationnelle de sécurité de l'information, pour son fonctionnement et ses actions opérationnelles.

Au-delà de ces ressources budgétaires, un effort soutenu de renforcement des capacités devra être engagé, notamment à travers :

- la formation continue du RSSI et des membres de l'unité de sécurité,
- le développement des compétences techniques en cybersécurité,
- la sensibilisation régulière des agents et collaborateurs de l'entité,
- la veille technologique et réglementaire pour anticiper les nouvelles menaces,
- la montée en compétence collective, en cohérence avec les orientations et référentiels de l'ANSSI.

(ii) Opérationnalisation du réseau des RSSI des entités de l'Etat

Le réseau national des RSSI devrait être doté de ressources pour accompagner les projets structurants de la une transformation numérique des entités de l'État.

À court terme**,** les activités du réseau seront structurées autour de priorités visant à formaliser sa gouvernance interne en créant une instance de coordination permanente. A moyen et long terme, le réseau sera une force de proposition pour toutes les questions liées à la cybersécurité nationale.

- **OS 4.2 Action 28 : Déployer une plateforme nationale pour la conduite des cyberdrills**

Le déploiement de la plateforme nationale permet de vérifier la résilience des dispositifs de sécurité mis en place en les confrontant à des scénarios d'attaques réels. Elle garantit que tous les acteurs particulièrement, les exploitants IIC s'entraînent selon les mêmes normes. Il n'y a plus de maillon faible.

- **OS 4.2 Action 29 : Créer un label de sécurité (audit et certification) pour les plateformes fournissant des services de transaction en ligne ouverts au public**

L'économie ivoirienne devant de plus en plus dématérialisée, les plateformes sont les cibles privilégiées des cybercriminels. L'Etat agit comme un tiers de confiance pour protéger le citoyen, les entreprises en certifiant les plateformes.

- **OS 4.2 Action 30 : Mettre en œuvre la PKI racine et Intégrer les services clés de l'administration**

La modernisation des infrastructures techniques permet de supporter des usages de plus en plus complexes et massifs : généralisation et sécurisation des services de l'administration en ligne.

Centraliser ces services permet à l'État de garder le contrôle sur les clés de chiffrement et les certificats via la (PKI) nationale.

- **OS 4.2 Action 31 : Mettre en place un système national d'authentification unifié au service public numérique**

L'identité numérique nationale eiD-CI permet de bâtir une société numérique inclusive, transparente et résiliente avec une authentification très forte de l'usager.

Objectif stratégique OS 4.3 : Protéger les données des utilisateurs

La protection des données est un processus dynamique pour l'ensemble des usagers des services en ligne de l'Administration.

Avec le développement des services digitaux et des accès à internet pour les populations, des risques apparaissent pour les utilisateurs sur internet. Les enfants sont eux aussi exposés à des risques, notamment via les réseaux sociaux.

Face à ces défis, l'acquisition d'une véritable culture numérique est devenue indispensable pour permettre à tous ces usagers de naviguer en sécurité et de bâtir ainsi une confiance numérique durable et partagée avec l'État.

Deux (2) Actions à réaliser :

- **OS 4.3 Action 32 : Intégrer la protection des données dès le début des projets** pour collecter le strict minimum de données et réduire la surface d'attaque**.**

- **OS 4.3 Action 33 : Elaborer un guide de bonnes pratiques de la protection des données dans le cyberespace** pour la prise de conscience des usagers de l'internet sur les cybermenaces et maîtrise l'empreinte numérique.

Dans cette dynamique l’accent sera mis sur la loi contre la cybercriminalité pour l’adapter aux réalités de l’IA.

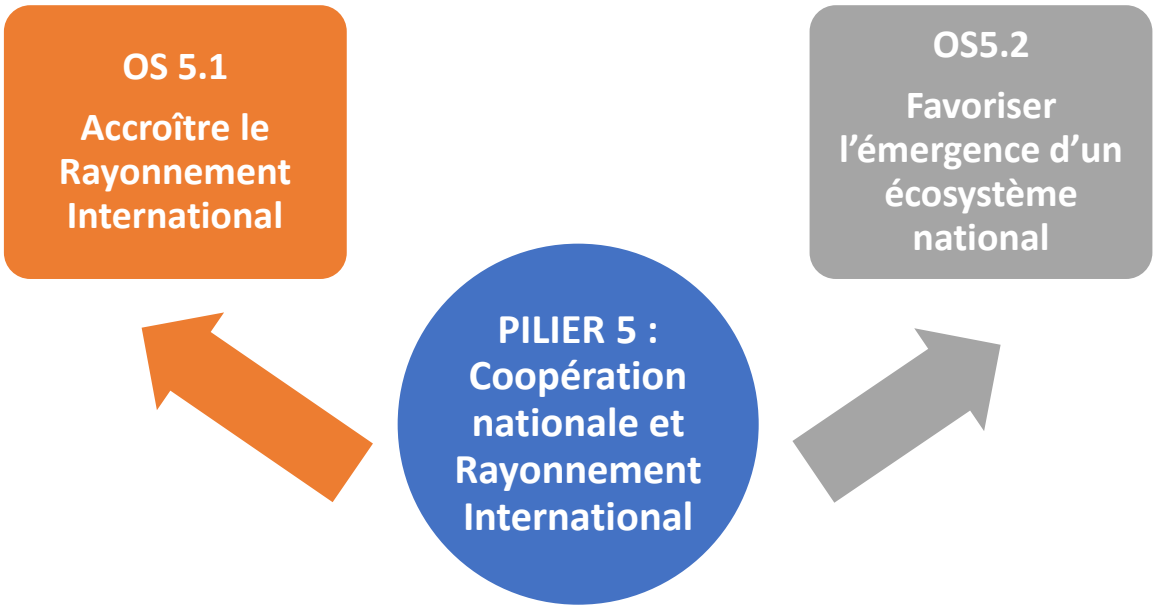
Au-delà du guide, il est essentiel de prendre une loi sur la cybersécurité qui va définir le cadre général de la cybersécurité, imposer des règles pour éviter que les cybers attaques ne réussissent. Il s’agira de transformer ces bonnes pratiques en règles, à court terme.

6.5 PILIER 5 : Coopération nationale et Rayonnement International

La coordination des acteurs nationaux et l'engagement international renforcent la position de la Côte d'Ivoire en cybersécurité. Les partenariats se structurent, les échanges s'intensifient et l'expertise nationale gagne en visibilité à l'échelle régionale et internationale.

Le pilier 5 repose sur :

- deux (2) objectifs stratégiques (2 OS)
- et quatre (4) actions à réaliser.



OS 5.1 : Pilier 5 Objectif Stratégique 1

OS 5.2 : Pilier 5 Objectif Stratégique 2

Objectif Stratégique OS 5.1 : Favoriser l'émergence d'un écosystème national

La coordination conditionne la cohérence et l'efficacité des actions en cybersécurité. La structuration d'un écosystème national repose sur l'organisation des relations entre l'État, le secteur privé, les universités et la société civile.

Les actions engagées formalisent les cadres de coopération, clarifient les rôles et responsabilités et renforcent les mécanismes de collaboration entre les parties prenantes. Elles facilitent le partage d'information, la mutualisation des ressources et la conduite d'initiatives communes.

Deux plateformes complémentaires vont se créer à travers les deux (2) Actions à réaliser :

- **OS 5.1 Action 34 : Créer et animer un forum d'échanges entre l'ANSSI, l'administration, les opérateurs du secteur public et privé pour la lutte contre les cyberattaques**

Une organisation intégrée améliore la synergie et renforce la capacité d'action collective tout en soutenant le développement d'un écosystème dynamique et performant. C'est une plateforme d'échanges qui offre un espace de dialogue direct où la coopération devient l'arme principale contre les menaces cyber.

- **OS 5.1 Action 35 : Mettre en place une plateforme nationale de partage et d'échange d'informations sur les menaces cyber (type MISP)**

L'ANSSI déploiera une plateforme nationale de partage d'informations (type MISP) avec les acteurs afin d'automatiser la diffusion des alertes cyber entre les opérateurs critiques. Ce dispositif technique permettra de mutualiser la connaissance des menaces en temps réel, garantissant qu'une attaque détectée par un acteur devienne immédiatement une protection pour tous.

Sur cette plateforme, on échange de manière réelle et anonymisée ou sous le sceau du secret partagé pour que l'ensemble de la communauté puisse se protéger sans que l'entreprise victime ne soit pénalisée. Il permet de réunir non seulement les techniciens (RSSI), mais aussi les décideurs.

Objectif Stratégique OS 5.2 : Accroître le Rayonnement International

Le positionnement international repose sur la capacité à contribuer activement aux initiatives en cybersécurité et à valoriser les compétences nationales au niveau régional et international. Une présence structurée dans les instances régionales et internationales renforce la crédibilité du pays et facilite l'accès aux partenariats stratégiques.

Les actions engagées développent les coopérations bilatérale, multilatérale en valorisant l'expertise ivoirienne. Elles favorisent également les échanges d'information et la coordination transfrontalière dans la prévention et la gestion des menaces.

Deux (2) actions à réaliser :

- **OS 5.2. Action 36 : Coordonner la participation active de la Côte d'Ivoire aux différents forums et activités internationales en matière de cybersécurité.**

Une implication renforcée améliore la visibilité du pays, soutient son positionnement comme hub régional et contribue à l'influence de la Côte d'Ivoire dans les dynamiques internationales de cybersécurité. La Côte d'Ivoire peut prendre l'initiative des directives dans l'espace UEMOA et régionales en matière de cybersécurité pour l'harmonisation de la réglementation

- **OS 5.2 Action 37 : Organiser des exercices de gestion de crises cyber régionaux (CEDEAO/UA)**

Dans la prévention et la gestion anticipées des risques, il est important d'organiser des simulations de cyberattaques visant les systèmes de paiement transfrontaliers.

Les partenariats du CI-CERT avec les réseaux régionaux et internationaux permettront d'améliorer la capacite à faire face aux crises et créer le réseau africain des CERT.

Cela permet de tester la rapidité de l'échange d'informations entre le CI-CERT et ses homologues des pays voisins.

7. MISE EN ŒUVRE DE LA STRATÉGIE

7.1 Plan d'actions de la SNCS

La Stratégie Nationale de Cybersécurité se décline en un plan d'actions quinquennal structuré par année et conçu pour permettre à chaque acteur de comprendre clairement les actions et les mesures à mettre en œuvre ainsi que les délais impartis pour les réaliser. Son exécution est annuelle.

Dès la signature, l'ANSSI notifie la SNCS signée à chaque administration, institution et agence concernée qui devient automatiquement et pleinement responsable de l'exécution des actions qui lui sont assignées. Cette responsabilité implique non seulement la mise en œuvre effective des mesures, mais également l'obligation de rendre compte dans les délais fixés.

Ainsi, la stratégie établit un cadre de redevabilité directe et immédiate, garantissant la transparence, l'efficacité, l'excellence et la coordination des efforts.

La réalisation des actions assignées et l'atteinte des objectifs seront récompensées pour encourager l'excellence. En revanche, la non-réalisation des actions sera consignée et rendue publique dans le rapport de suivi de la période, afin de garantir la transparence et la responsabilisation de tous les intervenants.

Le plan d'actions détaillé est joint en Annexe.

7.2 Entités opérationnelles

Cette section définit clairement les rôles et responsabilités des acteurs clés de la mise en en œuvre de la SNCS 2026-2030 qui sont les entités opérationnelles. L'ANSSI se positionne comme le chef d'orchestre.

Toutes les entités identifiées sont responsables de la mise en œuvre du plan d'actions de la SNCS 2026-2030 dans la limite de leurs champs de compétences respectifs, conformément aux dispositions légales en vigueur. Elles rendent compte à l'ANSSI dans le cadre de leurs missions de cybersécurité qui sont notamment, les suivantes :

- Réaliser les projets et actions dont elles ont la responsabilité ;
- Rendre compte de l'état d'avancement de la mise en œuvre des projets dont elles ont la responsabilité ;
- Contribuer pleinement à l'atteinte des objectifs stratégiques par la mise à disposition des ressources nécessaires à la réalisation des actions ;
- Proposer toutes mesures d'amélioration.

Les entités opérationnelles sont des structures identifiées parmi les entités étatiques, les organisations du secteur privé, la société civile ou toute autre entité impliquée dans la mise en œuvre de la stratégie. Ces entités sont :

- les autorités de réglementation,
- les ministères,
- les forces de police,
- les opérateurs d'infrastructures critiques,
- les fournisseurs de TIC,
- les universités,
- les grandes écoles et écoles de formation professionnelle
- les établissements scolaires : écoles primaires, collèges et lycées
- les instituts de recherche,
- la société civile,
- la population.

7.3 Réseau des points focaux de cybersécurité

Il sera créé au sein de chaque entité étatique un poste de Responsable de la Sécurité des Systèmes d'Information (RSSI) conformément au décret n°915-2021 portant Politique de Sécurité des Systèmes d'Information de l'Administration Publique.

Sous la supervision de l'ANSSI, le RSSI sera le point focal sur les questions de cybersécurité au sein de l'entité à laquelle il sera affecté. Il sera chargé de l'amélioration continue de la sécurité du système d'information de l'entité.

Placé sous la coordination stratégique de l'ANSSI, l'ensemble de ces RSSI constituera le **Réseau National des Points Focaux Cybersécurité** réunis au sein de cette communauté d'échange et d'alerte, les RSSI assureront la liaison opérationnelle dans leur administration et piloteront l'amélioration continue de la sécurité de leur système d'information.

7.4 Financement de la SNCS

Le risque cyber est partout, la richesse numérique est partagée, et la défense ne peut être qu'élargie. Cette nécessité d'une responsabilité collective trouve son fondement juridique dans l'article 33 de la loi de 2017 qui dispose que :

- Le développement et le maintien de la maturité numérique sont une priorité nationale ;
- La mise en œuvre de cette priorité est de la responsabilité de l'État ;
- L'État prend « toute disposition pour en assurer le financement », que ce soit par le budget national ou par différents partenariats.

Conséquence : La cybersécurité n'est plus une dépense "facultative", mais une ligne budgétaire imposée par la loi pour protéger la Nation.

En application de cette disposition, le financement de la SNCS 2026-2030 reposera sur une mobilisation multisectorielle impliquant divers acteurs et diverses sources. Un mécanisme de sécurisation garantira la pérennité du modèle, en privilégiant des ressources nationales pour préserver l'autonomie et la souveraineté de la SNCS.

Le tableau ci-dessous, présente les sources de financement identifiées.

SOURCES DE FINANCEMENT	PART DU BUDGET	ESTIMATION EN MILLIARDS FCFA	JUSTIFICATION STRATEGIQUE
ETAT (ligne dédiée dans le budget national et redevance cybersolidarité)	50%		Garantit la souveraineté et subventionne les plus vulnérables.
Partenariat avec les IIC (Banque, Assurance, Energie, Télécom)	30%		Reflète la responsabilité partagée. Les (IIC) financent la protection des infrastructures dont ils tirent leurs revenus.
Ressources des communications électroniques (Quote part des sanctions perçues dans le secteur du numérique et le fond de service universel)	5%		Réorienté une partie de ces fonds vers la sécurisation des infrastructures éducatives et de santé publique
ANSSI	5%		Marque le début de l'autonomisation de l'ANSSI : Labellisation et formations payantes
Coopération internationale (Coopération bilatérale et bailleurs de fonds)	10%		Assure l'accélération. Un apport limité pour éviter toute dépendance stratégique vis-à-vis des bailleurs étrangers.
TOTAL	**100%**		

7.5 Outils d'accompagnement obligatoire de la mise en œuvre de la SNCS 2026-2030

Pour que les obligations issues de la SNCS 2026-2030 ne restent pas sans suite, les outils d'accompagnement sont proposés à travers les investissements et la cyber assurance

(i) Les investissements obligatoires dans le secteur privé stratégique

Pour rendre les investissements obligatoires dans le secteur privé stratégique, la nouvelle stratégie SNCS 2026-2030 prévoit les deux (2) mécanismes ci-après :

- **Méthodologie de risque obligatoire : Désignation comme Infrastructure d'Information Critique (IIC)**

La stratégie recommande de rendre obligatoire l'usage d'une méthodologie nationale de gestion des risques pour toutes les Infrastructures d'Information Critique (IIC) relevant notamment des secteurs de l'énergie, l'eau, du numérique, de la santé, des finances, du transport, et de l'administration Civile.

En classant une entreprise privée comme "critique", l'État lui impose légalement de suivre le Plan National de Protection des Infrastructures Critiques (PPIC). Cela inclut l'obligation de réaliser des audits de sécurité annuels et de déclarer tout incident au CI-CERT sous peine de sanctions.

- **Le Modèle National de Maturité : Audits et Scoring**

Un modèle national de maturité sera déployé pour évaluer 100 % des administrations et des secteurs critiques, avec un "scoring" public. Un mauvais score ou un score insuffisant pourrait entraîner des restrictions d'activité ou des sanctions (amendes administratives ou des remises à niveau forcées). Un bon score améliorera la notoriété de l'entité concernée. Un classement annuel des entités sera rendu public.

(ii) La Cyber-Assurance Obligatoire

Lancer une étude sur l'opportunité d'instaurer l'obligation de cyber-assurance, incluant des dispositions contraignantes de déclaration d'incidents assorties de sanctions. L'Etat envisage d'imposer cette obligation à des secteurs privés ciblés, afin d'inciter ces acteurs à renforcer leurs dispositifs techniques pour satisfaire aux critères d'assurabilité.

7.6 Les mécanismes d'incitations

Dans la conduite de sa politique cyber, l'Etat devra prévoir des moyens et mécanismes d'incitation des PME à s'inscrire dans la stratégie de Cybersécurité, afin d'éviter de créer des maillons faibles qui pourraient fragiliser tout le dispositif.

Dans cette optique, la Stratégie prévoit des incitations fiscales et la mise en place d'un Fonds de Soutien Cyber. L'accès à ces mesures et mécanismes doit être basé sur des critères clairs et précis, suffisamment flexibles et accessibles à ces PME et startups.

8. SUIVI, ÉVALUATION ET RÉVISION

La SNCS 2026 -2030, élaborée avec la collaboration des parties prenantes est un instrument de planification et un cadre de référence et d'orientation des interventions en matière de Cybersécurité.

Le suivi permet de produire des informations sur le niveau de progression des Indicateurs Clé de Performance (KPI) formulés dans le cadre de la mesure du rendement. Ces indicateurs renseignent sur les évolutions réalisées dans la mise en œuvre et orientent sur les mesures correctives à envisager avant le terme des actions engagées. Il s'agit d'anticiper pour atteindre les résultats attendus.

Le suivi de la mise en œuvre de la SNCS est permanent sur toute la période 2026 -2030 et sera meublé des temps forts d'évaluation, en l'occurrence :

- le rapport annuel
- la revue à mi-parcours
- l'étude d'impact
- le bilan

8.1. Le rapport annuel

Le rapport annuel est produit chaque année de 2026 à 2030. Ce rapport rassemble les données collectées, traitées et constitue l'évaluation annuelle. Il propose entre autres des réajustements, s'il y a lieu, en fonction de l'atteinte des objectifs annuels. Il est disponible au plus tard le 31 mars de l'année. Il est destiné aux autorités politique, les acteurs du secteur dans le respect de la confidentialité des informations. Le premier rapport devra être disponible au plus tard le 31 mars 2027.

8.2. La revue à mi-parcours

Elle se tiendra à la fin du premier trimestre de l'année 2028, après le second rapport de 2027. Elle a vocation à identifier les facteurs de succès et d'échecs, les leçons, les lacunes en matière de programmation et de finances. Elle est l'occasion de partager, capitaliser les expériences et les bonnes pratiques et formuler des recommandations pertinentes pour la continuité de la mise œuvre du plan.

8.3. L’étude d’impact et le bilan

L’étude d’impact et le bilan seront rédigés en fin de période stratégique.

L’étude d’impact permettra de mesurer concrètement les effets à long terme de la SNCS sur la résilience nationale, l'économie numérique et la confiance des citoyens, fournissant ainsi des données terrain objectives.

Le rapport d’étude d’impact servira à l’élaboration du bilan final. Lequel bilan permettra d’identifier les écarts, les retards, les anomalies, les impacts, les nouveaux risques et de proposer des mesures correctives et des évolutions stratégiques adaptées afin de face aux nouvelles menaces qui pourraient peser sur la Côte d’Ivoire.

8.4. Mise en place du Comité de suivi

Le suivi constitue une phase d’importance capitale dans la réussite de la stratégie. En son absence, celle-ci risque d’être appliquée de manière discrétionnaire ou non conforme aux échéances par les acteurs.

La responsabilité du suivi incombe à l’ANSSI dont la mission est d’assurer la mise en œuvre des stratégies nationales de cybersécurité. Elle est assistée d’autres acteurs de l’écosystème pour constituer le Comité de suivi.

- **Composition du Comité de suivi**

- Un (1) représentant du Ministère qui en assurera la présidence ;
- Trois (3) représentants de l’ANSSI dont l’un assurera le secrétariat ;
- Des membres des faitières des acteurs clés du privé de la société civile, académique,
- et autres acteurs ayant contribué à l’élaboration de ladite SNCS (membres permanent).

- **Missions du Comité de suivi**

- Contrôler la mise en œuvre cohérente, rigoureuse et responsable de la stratégie ;
- Procéder à la révision de la SNCS et du plan d’actions le cas échéant pour tenir compte des résultats obtenus dans les rapports et bilan périodique ;
- Procéder à l’évaluation de la maturité de notre pays.
  Identifier et analyser les initiatives spontanées du terrain qui bien que non prévues par la stratégie s’avèrent bénéfiques pour celle-ci

- **Outils de suivi**

- Tableau de bord de suivi

- Rapports annuels
- Bilan à mi-parcours

- **Réunions**

- Une fois par trimestre pour examiner l’avancement du plan d’action ;
- Une fois par an afin d’analyser les résultats et établir un rapport ;
- À tout moment en cas de besoin.

8.5. Mécanisme de révision

Le changement perpétuel du numérique représente à la fois un risque à anticiper et une opportunité constante de mieux protéger et de toujours innover. À ce titre, notre stratégie se veut résolument pragmatique : elle s'adaptera aux évolutions du terrain sans jamais perdre de vue sa vision d'origine, qui demeure un socle inébranlable. Ainsi, elle pourra être révisée au rythme des évaluations du Comité de suivi ou face à toute mutation majeure de l’écosystème du numérique.

9. CONCLUSION

La Stratégie Nationale de Cybersécurité 2026-2030 ne constitue pas une simple mise à jour technique, mais un véritable pacte de confiance entre l'État, les acteurs de l'écosystème, tous les opérateurs économiques et les citoyens.

À l'heure où la transformation digitale devient le moteur principal de la croissance, de la Côte d'Ivoire, la sécurité de notre espace numérique s'affirme comme le socle de notre souveraineté nationale.

Durant ces cinq prochaines années, notre ambition sera de passer d'une posture de réaction à une véritable culture de la prévention. La SNCS 2026-2030 se veut opérationnelle, inclusive et proactive. En exécutant ce plan d'actions dans son intégralité, nous érigerons une barrière robuste contre les menaces émergentes, portée par une population avertie et un vivier de professionnels qualifiés. Notre objectif ultime est d'élever durablement le niveau de maturité de la Côte d'Ivoire en matière de cybersécurité.

La cybersécurité n'est plus une contrainte budgétaire, mais un avantage compétitif majeur qui positionnera notre pays comme un hub numérique sûr et attractif pour l'économie mondiale.

ANNEXES

Annexe 1 : Cadre logique de mise en œuvre de la SNCS 2026-2030

Annexe 2 : Rappel des principes du Global Compact et les ODD

Annex 3 : Projets structurants

Annexe 3 : Plan d’actions

Annexe 1 : Cadre logique de mise en œuvre de la SNCS 2026-2030

Cette annexe présente les principaux éléments nécessaires à la bonne compréhension du plan d'actions de la SNCS 2026-2030, son appropriation et mise en œuvre efficiente.

Pour chaque Pilier, il est essentiel de définir les Objectifs stratégiques, les Actions ou Projets à réaliser, les Livrables, les Indicateurs de Performance (KPI), le Porteur, l'Echéance, le niveau de Priorité, le Coût d'exécution et la Source de financement.

- **Les Piliers :**

Ce sont les grands axes stratégiques qui structurent la Stratégie. Ils regroupent un ensemble cohérent d'objectifs stratégiques et d'actions à réaliser pendant la période.

- **Les Objectifs stratégiques :**

Ce sont les résultats majeurs à atteindre dans le cadre de chaque pilier afin de concrétiser la vision de la stratégie.

- **Actions / Projets :**

Ce sont les activités ou initiatives concrètes à mettre en œuvre pour atteindre les objectifs stratégiques.

- **Livrable :**

C'est la preuve matérielle attendue à l'issue de la réalisation effective d'une action ou d'un projet.

- **Indicateurs de performance (KPI) :**

Ce sont des mesures permettant de suivre l'avancement et d'évaluer l'efficacité réelle des actions mises en œuvre.

- **Porteur :**

C'est l'Institution ou l'entité responsable de la mise en œuvre de l'action.

- **Échéance :**

C'est la période ou la date prévue pour la réalisation effective de l'action et la production du livrable.

- **Priorité :**

C'est le niveau d'importance de l'action dans la mise en œuvre globale de la stratégie.

- **Coût d'exécution :**

C'est l'estimation des ressources financières nécessaires à la réalisation de l'action.

- **Sources de financement :**

Ce sont les Origines des ressources financières mobilisées pour financer l'action.

Annexe 2 : Rappel des principes du Global Compact et des ODD

I) Rappel des dix (10) principes du Global Compact ou Pacte Mondial des Nations Unies

Droits de l'Homme

- **Principe 1** : Les entreprises sont invitées à promouvoir et à respecter la protection du droit international relatif aux Droits de l'Homme.
- **Principe 2** : Les entreprises sont invitées à veiller à ne pas se rendre complices de violations des Droits de l'Homme.

Normes internationales du travail

- **Principe 3** : Les entreprises sont invitées à respecter la liberté d'association et à reconnaître le droit de négociation collective.
- **Principe 4** : Les entreprises sont invitées à contribuer à l'élimination de toutes les formes de travail forcé ou obligatoire.
- **Principe 5** : Les entreprises sont invitées à contribuer à l'abolition effective du travail des enfants.
- **Principe 6** : Les entreprises sont invitées à contribuer à l'élimination de toute discrimination en matière d'emploi et de profession.

Environnement

- **Principe 7** : Les entreprises sont invitées à appliquer l'approche de précaution face aux problèmes touchant l'environnement.
- **Principe 8** : Les entreprises sont invitées à prendre des initiatives tendant à promouvoir une plus grande responsabilité en matière d'environnement.
- **Principe 9** : Les entreprises sont invitées à favoriser la mise au point et la diffusion de technologies respectueuses de l'environnement.

Lutte contre la corruption

- **Principe 10** : Les entreprises sont invitées à agir contre la corruption sous toutes ses formes, y compris l'extorsion de fonds et les pots-de-vin.

II) Les Objectifs de Développement Durable (ODD)

- **ODD 1** : Éliminer la pauvreté sous toutes ses formes et partout dans le monde
- **ODD 2** : Éliminer la faim, assurer la sécurité alimentaire, améliorer la nutrition et promouvoir l'agriculture durable
- **ODD 3** : Permettre à tous de vivre en bonne santé et promouvoir le bien-être de tous à tout âge
- **ODD 4** : Assurer l'accès de tous à une éducation de qualité, sur un pied d'égalité, et promouvoir les possibilités d'apprentissage tout au long de la vie
- **ODD 5** : Réaliser l'égalité de genre et autonomiser toutes les femmes et les filles
- **ODD 6** : Garantir l'accès de tous à l'eau et à l'assainissement et assurer une gestion durable des ressources en eau
- **ODD 7** : Garantir l'accès de tous à des services énergétiques fiables, durables et modernes, à un coût abordable
- **ODD 8** : Promouvoir une croissance économique soutenue, partagée et durable, le plein emploi productif et un travail décent pour tous
- **ODD 9** : Mettre en place une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation
- **ODD 10** : Réduire les inégalités entre les pays et en leur sein
- **ODD 11** : Faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables
- **ODD 12** : Adopter des modes de consommation durable et de production éco-responsable.
- **ODD 13** : Prendre d'urgence des mesures pour lutter contre les changements climatiques et leurs répercussions
- **ODD 14** : Conserver et exploiter de manière durable les océans, les mers et les ressources marines aux fins du développement durable
- **ODD 15** : Préserver et restaurer les écosystèmes terrestres, en veillant à les exploiter de façon durable, gérer durablement les forêts, lutter contre la désertification, enrayer et inverser le processus de dégradation des sols et mettre fin à l'appauvrissement de la biodiversité
- **ODD 16** : Promouvoir l'avènement de sociétés pacifiques et ouvertes à tous aux fins du développement durable, assurer l'accès de tous à la justice et mettre en place, à tous les niveaux, des institutions efficaces, responsables et ouvertes à tous
- **ODD 17** : Renforcer les moyens de mettre en œuvre le Partenariat mondial pour le développement durable et le revitaliser

Annexe 3 : Projets Structurants

Objectifs Stratégiques (OS)	#	Projets
OS 1.1 : Bâtir une gouvernance optimale	1	Instaurer un cadre formel de concertation es acteurs publics et les IIC du secteur numérique Instaurer un cadre formel de coordination entre
	2	Mettre en place un observatoire de confiance numérique au sein de l'ANSSI
	3	Dispositif de redevabilité de la SNCS
OS 1.2 : Moderniser le cadre légal	4	Loi sur la cybersécurité et ses décrets d'application
OS 2.2 : Renforcer les compétences et propulser la recherche cyber	5	Renforcer les capacités des centres publics de formation en cybersécurité
OS 3.1 : Protéger les infrastructures critiques	6	Mettre en œuvre le plan national de protection des infrastructures critiques
OS 3.2 : Renforcer la cyber résilience	7	Élaborer et mettre en œuvre un plan national de gestion des crises cyber
OS 4.1 : Déployer une infrastructure nationale souveraine et robuste	8	Renforcer le CI-CERT et Mettre en place des CERT sectoriels dans les secteurs bancaires et des télécommunications
		Mettre en place un centre national de Supervision des réseaux et services d'information critiques (SOC)
	9	Mettre en place une plateforme nationale de partage et d'échange d'informations sur les menaces cyber (type MISP)
	10	Déployer une plateforme nationale pour la conduite des cyberdrills
	11	Assurer la mise en conformité des institutions publiques et des collectivités territoriales aux référentiels et cadres techniques nationaux en vigueur
	12	Renforcer les capacités techniques de la PKI racine

Annexe 4 : Plan d'actions

#	Actions /Projets	Livrable	Indicateurs de performance	Porteur	Échéance	Priorité	Coût d'exécution	Sources de financement	Statut
Pilier 1 : Gouvernance éthique et cadre légal									
Objectif Stratégique OS 1.1 : Bâtir une gouvernance efficace et éthique									
Résultats attendus : • Synergie entre les institutions dans un cadre de collaboration clairement défini ; • Suppressions de lourdeurs administratives ; • Meilleure Coordination institutionnelle des activités de cybersécurité ; • Chaînes de décision plus rapide et plus lisible, permettant une réponse instantanée et efficace aux incidents de cybersécurité au bénéfice direct du citoyen.									
1	Impulser la montée en puissance de l'ANSSI sur l'ensemble des administrations publiques et des départements ministériels.	Feuille de route de l'ANSSI Référentiels, lignes directrices et procédures	100% des administrations et des autorités des secteurs stratégiques disposent d'un accord formel	Ministères ANSSI ARTCI BCEAO ANARE CI	T1-2027	P2			

		formalisées par secteur d'activité Déclinaison sectorielle de la SNCS à travers des feuilles de route par secteur d'activité Accords formels signés avec les départements ministériels et chaque autorité sectorielle (télécommunications, énergie, transport…)	signé avec l'ANSSI	…..					
2	Instaurer un cadre formel de concertation entre les acteurs publics et les Exploitants d'IIC	Procédures rédigées, communiquées à l'ensemble des acteurs Signature d'accord	100% des procédures validées et appliquées par les différents acteurs 100% des accords signés avec les IIC	ANSSI	T1-2027	P2			

3	Mettre en place un observatoire de confiance numérique au sein de l'ANSSI	Décision de création et installation de la de l'observatoire de confiance numérique Charte d'éthique et de la déontologie de la cybersécurité Rapport annuel sur l'état de la Confiance et la résilience cyber	2026 : 30% des agents de l'ANSSI formés à l'éthique 2027 : 70% des agents de l'ANSSI formés à l'éthique % des administrations et entreprises conformes aux référentiels ANSSI	ANSSI Administrations Entreprises publiques	T4-2027	P1			
4	Mise en place le Comité de Suivi de la SNCS	Document officiel de création Dispositif de redevabilité de la SNCS Rapport annuel de suivi de la mise en œuvre de la SNCS	Rapport publié annuellement (Oui/Non)	ANSSI	T4-2026	P1			
Objectif stratégique 1.2 : Moderniser le cadre juridique de la cybersécurité									

5	Réviser et harmoniser le cadre juridique existant	Textes existants en matière de cybersécurité révisés	Nombre des textes existants révisés	ANSSI et les parties prenantes	T2-2029	P1			
6	Renforcer l'arsenal juridique par de nouveaux textes	Nouveaux textes adoptés : Lois sur la cybersécurité et ses décrets d'application Mise en place d'une Cellule de Veille stratégique et prospective	Nombre de nouveaux textes Création de la Cellule de Veille Stratégique et Prospective	ANSSI et les parties prenantes	T2-2029				
7	Mettre en place des mécanismes de révision des textes juridiques	Mécanisme de révision continue des textes Mécanisme d'information de la population	100% des textes sont portés à la connaissance de la population sur les différents canaux de communications % des propositions de révisions de	ANSSI	T4-2028	P3			

			textes soumis au Réseau des RSSI % des propositions de révision de textes soumis à la Commission de						
Pilier 2 : Capital humain et innovation									
Objectif stratégique 2.1 : Développer la culture de cybersécurité et la confiance numérique au sein de la société									
Résultats : • Protection renforcée de l'ensemble de la population sur tout le territoire national en cybersécurité, avec une attention particulière portée aux personnes et groupes vulnérables ; • Réduction des risques liés aux usages numériques, notamment les fraudes et les atteintes aux données personnelles ; • Développement d'une conscience collective des enjeux de cybersécurité, favorisant des comportements numériques responsables									
8	Développer une culture cybersécurité des populations y compris des personnes vulnérables	Plan national de sensibilisation des populations Programmes de campagnes nationales aux risques cyber	Plan adopté (Oui/Non) Taux d'exécution du programme national de sensibilisation sur les abus en ligne	ANSSI	Elaboration du plan : 2026 Exécution du programme : Récurrent T1-2027	P2			

		Supports de sensibilisation grand public Guide de sensibilisation des personnes vulnérables (enfants, femmes, personnes âgées) Plateforme et applications éducatives pour mineurs	Réduction du taux d'abus en ligne de 50 % par rapport au taux actuel Nombre d'ambassadeurs de la cybersécurité désignés et formés						
9	Organiser des campagnes de renforcement des compétences au bénéfice des professionnels des secteurs public et privé	Programme de formation des professionnels des secteur public et privé	Nombre de professionnels formés	ANSSI	T1-2027				
10	Encourager la formation des décideurs publics et des IIC	Programme de formation suivi par le top management de	Nombre de décideurs formés	IIC ANSSI	T4-2026				

		l'Administration et des IIC							
11	Encourager le recours à l'expertise qualifiée locale pour réaliser des audits de sécurité ou des prestations de conseil et créer des emplois locaux.	Plan de formation des auditeurs	Nombre d'auditeurs formés	ANSSI	T3-2026				
Objectif stratégique 2.2 : Renforcer les compétences en cybersécurité et propulser la recherche cyber									
Résultats : • Co-construction des programmes de formation sur la cybersécurité avec les universités, les centres de formation spécialisés ; • Programmes de formation académique et professionnelle actualisés, alignés sur les besoins réels du marché et les menaces émergentes ; • Formation d'experts en cybersécurité (environ 10 0000) ; • Montée en compétences des acteurs publics et privés, renforçant l'autonomie nationale en matière de cybersécurité ; • Solutions de cybersécurité nationales développées via la recherche et le développement (R&D) ; • Fonds National de la Cybersécurité (FNCS).									
12	Renforcer les capacités des centres publics de formation et encourager la promotion des	Catalogues de formations et parcours certifiants et diplômants	Nombre de conventions de partenariat signés	ANSSI INPHB, ENA	T3-2027	P2			

	carrières en cybersécurité	Conventions de partenariat signées Rapport d'activité des centres de formation	Nombre de centres de formation opérationnels Taux d'insertion professionnelle des bénéficiaires Nombre de certifications / diplômes délivrés Nombre d'agents publics et fonctionnaires formés Plan de stages	Ecole de gendarmerie Nationale Ecole de Police Nationale ENSEA ESATIC CPFA					
13	Mettre en place un plan national de sensibilisation en milieu scolaire	Programme de formation en cybersécurité dans les écoles et universités	Nombre d'écoles ayant intégré le module cybersécurité dans leurs cursus	ANSSI ET CENTRES DE FORMATION	T4-2029				

		Partenariats signés entre le Ministère de l'Enseignement Technique, le Ministère de l'Education Nationale, secteur privé et les universités	Nombre d'élèves formés Nombre de bourses accordées aux élèves Cadre d'échanges entre les experts de la cybersécurité et les professeurs						
14	Déployer un programme national de certification en cybersécurité, encourager les recherches en cybersécurité	LIVRABLE SUPPRIME Convention avec les organismes certificateurs Mécanisme de financement (fonds dédié ou ligne budgétaire annuelle)	Pourcentage d'enseignants certifiés dans les filières ciblées (cible : 50–70 % à 5 ans) Nombre annuel de certifications internationales obtenues RGSSI	ANSSI ENS CAFOP	T1-2028	P3			

		Référentiel national des certifications prioritaires	Taux de réussite national (>65 % cible progressive) Ratio investissement public / certifications obtenues (efficience) Contribution du programme à l'amélioration du capital humain cyber national						
Objectif stratégique 2.3 : Encourager l'innovation pour anticiper les nouvelles menaces									
Résultats : • Financement structuré de la recherche en cybersécurité (FNCS) et soutien actif à l'innovation locale ; • Promotion de start-ups spécialisées en cybersécurité (« cyber-champions »), contribuant à l'émergence d'un écosystème national compétitif et créateur de valeur ; • Expertise ivoirienne reconnue, contribuant au rayonnement et à l'excellence national ; • Développer la cyber intelligence									
15	Mettre en place un programme de			Ministère de la transition	T4-2027	P2			

	laboratoires communs public-privé (LabCom Cyber)	LIVRABLE SUPPRIME Cadre juridique des laboratoires communs public–privé (LabCom Cyber) Comité de gouvernance multi-acteurs (État, universités, secteur privé) Appels à projets annuels (innovation, R&D appliquée, souveraineté) Dispositif de suivi financier et d'audit	Nombre de laboratoires communs opérationnels Nombre de solutions développées et testées Taux de transfert des solutions vers l'industrie ou l'administration Nombre de solutions cyber nationales déployées Nombre d'emplois créés dans l'écosystème cyber local	numérique et de la digitalisation (MTND) Institutions académiques Centre de recherches Centres de recherches Organisme de sécurité nationale					

16	Organiser des concours de projet innovants	Dispositif de concours mis en place	Nombre de concours organisés	ANSSI, MTNIT MEJ MTND	T4-2027				
Pilier 3 : Protection des Infrastructures Critiques et Cyber résilience									
Objectif stratégique 3.1 : Protéger les infrastructures critiques									
Résultats : • Etat des lieux des infrastructures critiques et des systèmes d'information ; • Plan de protection des Infrastructures mis en œuvre ; • Alignement des prestataires de services numériques sur des standards professionnels, renforçant la fiabilité globale de l'écosystème numérique ivoirien ; • Réponse proactive en cas d'incidents									
17	Réaliser une étude nationale d'identification et d'évaluation des infrastructures critiques et non critiques	Rapport d'inventaire des IIC Rapport d'étude d'évaluation des IIC Tableau des prestataires de services numériques Rapport sur l'alignement des	Rapports réalisés et validés (Oui/Non)	ANSSI	T4-2026	P1			

		prestataires de services numériques							
18	Mettre en œuvre le plan national de protection des infrastructures critiques (PPIC)	PPIC (déjà adopté) Plan de mise en œuvre et de contrôle du PPIC Rapport de suivi de la mise en œuvre du PPIC Rapport de conformité des IIC par rapport aux exigences légales du plan	Pourcentage d'IIC conformes aux exigences du plan (cible : 2026 : 20% 2027 : 50% 2028 : 75% 2029 : 100%) 100% du taux de réalisation du plan d'audits annuel Réduction du nombre d'incidents majeurs affectant les IIC	ANSSI	T4-2026	P1			
Objectif stratégique 3.2 : Renforcer la cyber résilience									
Résultats : • Plan de gestion de crise mis en œuvre ;									

• Renforcement de la continuité d'activité des services publics et privés critiques									
19	Élaborer et mettre en œuvre un plan national de gestion des crises cyber	Plan national de gestion de crise cyber Rapports d'exercices et simulations de crise Calendrier de formation des parties prenantes au plan national de gestion de crises Mise en place d'une plateforme d'échange d'information Mise en place du Comité de gestion des crises Elaboration de procédures de gestion des crises et	Nombre d'exercice organisés annuellement (par équipe et à l'échelle internationale) et % des participants formés par rapport aux effectifs cibles Disponibilité et utilisation de la plateforme d'échange d'information (taux d'uptime de la plateforme et volume de données/ informations partagées en temps réel des exercices) Charte fonctionnement	ANSSI	T1-2027	P2			

		politique de communications	du comité de gestion de crise Nombre de plans (nationaux, sectoriels) élaborés validés et testés par rapport aux objectifs fixés (ex 100% des plan prévus finalisés d'ici 2027) Plan validé et opérationnel (Oui/Non) Taux de réalisation du planning des exercices de crise (cible 100%)						

			100% Taux de participation aux formations						
20	Élaborer un catalogue national de services de cybersécurité adapté aux besoins des collectivités territoriales	Cartographie des besoins de services Cyber Catalogue de services cyber Référents cyber désignés	2026 : 10 % des collectivités embarquées dans des activités cyber avec l'ANSSI 2027 : 30 % des collectivités embarquées dans des activités cyber avec l'ANSSI 2028 : 50 % des collectivités embarquées dans des activités cyber avec l'ANSSI 2029 : 75 % des collectivités embarquées dans des activités	ANSSI UVICOCI Collectivités territoriales	T4-2030	P1			

			cyber avec l'ANSSI 2030 : 90 % des collectivités embarquées dans des activités cyber avec l'ANSSI						
21	Auditer les institutions publiques et des collectivités territoriales aux référentiels et cadre technique nationaux en vigueur	Rapports d'audits de sécurité Plan de mise en conformité	Pourcentage d'organismes audités (cible : 2027 : 30% 2028 : 50% 2029 : 100%) Nombre d'audits réalisés Cible 6 (1 par bimestre) Nombre d'institution publique et collectivité territoriale	ANSSI		P3			

			conforme à la Politique de Sécurité des Systèmes d'Information (PSSI)						
22	Mettre en place un cadre national de sécurité des systèmes d'information intégrant l'intelligence artificielle	Méthodologie nationale d'audit cybersécurité des systèmes d'IA. Référentiel de contrôle cyber IA (checklists techniques). Plan d'audit annuel Rapports d'audit type pour systèmes IA critiques.	Taux d'exécution du plan d'audits (évaluation) des systèmes embarquant l'IA dans les secteurs sensibles (cible 100%)	ANSSI	T4-2030	P3			
23	Encourager la cyber-assurance dans la politique nationale de résilience des secteurs critiques	Diagnostic stratégic Liste des IIC assurées	% IIC couvertes par assurance cyber	ANSSI	T4-2028	P3			

Pilier 4 : Capacités techniques et opérationnelles de l'État									
Objectif stratégique 4.1 : Déployer une infrastructure nationale souveraine et robuste									
Résultats : • Création du SOC national pour renforcer la surveillance et la détection des incidents cyber ; • Réduction mesurable des délais de détection, d'analyse et de traitement des incidents de cybersécurité ; • Amélioration tangible de la confiance des citoyens et des acteurs économiques dans les services numériques de l'État									
24	Mettre en place un centre national de Supervision des réseaux et services d'information critiques (SOC)	Décret de création, organisation et de fonctionnement du SOC national Rapport annuel de fonctionnement du SOC national Procédures de supervision et d'escalade Rapports de surveillance et d'alertes	SOC opérationnel (24/7) (Oui/Non) Nombre d'événements de sécurité corrélés	ANSSI	T2-2027	P1			

25	Renforcer le laboratoire national de Forensique pour les analyses numériques	Équipements et outils d'analyse certifiés Procédures de fonctionnement du Laboratoire Rapports d'analyses numériques judiciaires	Nombre d'analyses forensiques réalisées par an Nombre d'affaires judiciaires appuyées	ANSSI	T2-2027	P3			
Objectif stratégique 4.2 : Optimiser la réactivité opérationnelle pour réduire l'impact des incidents									
Résultats : • Préparation opérationnelle des acteurs renforcée face aux incidents cyber ; • Niveau de conformité des institutions publiques renforcé ; • Infrastructure nationale de confiance numérique robuste et disponible ; • Coordination renforcée entre les équipes techniques, les autorités compétentes et les opérateurs de services critiques ; • Consécration du poste des RSSI et opérationnalisation du réseau des RSSI des entités de l'Etat									
26	Renforcer le CI-CERT et mettre en place des CERT sectoriels	CERT Télécom/Numérique opérationnel CERT Bancaire/Finance opérationnel	Opérationnalisation des CERT sectoriels Nombre d'incidents traités/	ANSSI	T4-2026 : renforcement du CI-CERT T4-2027 : Mise en place des	P1			

		CERT-Énergie & Infrastructures Opérationnel CERT-Santé / Administration Opérationnel Décrets / arrêtés de création et de rattachement Procédures de coordination entre le CI-CERT et les CERT sectoriels Playbooks d'intervention et SLA de réponse aux incidents Renforcement du capital humain et spécialisation des équipes du CI-CERT	Nombre d'incidents déclarés par CERT et par secteur Délai de réaction prévu par le SLA pour les Entreprises Taux de satisfaction des secteurs couverts (cible 70%) Plan de recrutement des Experts du CI-CERT Programme de formation préparatoire à la Certification internationale Niveau de maturité organisationnelle atteint		CERT sectoriels				
27	Consécration du poste des RSSI et opérationnalisation	Création d'unité dédiée à la sécurité	Le répertoire des CSI	ANSSI	T4-2028	P 3			

	du réseau des RSSI des entités de l'Etat	de l'information dans chaque entité de l'État (CSI)	Répertoire des RSSI Positionnement et formation du RSSI						
28	Déployer une plateforme nationale pour la conduite des cyberdrills	Protocole national de cyberdrills Calendrier annuel d'organisation des cyberdrills Rapports des travaux d'organisation des cyberdrills	Protocole national de cyberdrills Calendrier annuel d'organisation des cyberdrills % de participation des opérateurs IIC Rapports des travaux d'organisation des cyberdrills	ANSSI	T3-2026	P2			

			% des vulnérabilités corrigées						
29	Créer un label de sécurité (audit et certification) pour les plateformes fournissant des services de transaction en ligne ouverts au public	Procédure validée d'audit et de certification Document décrivant les exigences ou les conditions de certification au label Registre public des plateformes labellisées Tableau de l'ordre des expert auditeur des PASSI	Label créé et adopté (Oui/Non) Nombre d'audit de labélisation réalisé (cible >= 3) Nombre de prestataire d'audit (PASSI et expert auditeur) ayant l'agrément par an (cible >=3)	ANSSI, ARTCI et CODINORM	T3- 2027	P2			

30	Mettre en œuvre la PKI racine et y intégrer les services clés de l'administration	Rapport de mise en œuvre de la PKI racine Guides d'utilisation pour l'administration Copie de document signé électroniquement (1 ou 2)	PKI conforme aux standards internationaux (Oui/Non) Nombre de certificats émis/révoqués Taux de disponibilité de la PKI (cible > 99,99 %) La scalabilité assurée Nombre de service de l'Administration intégrés à la plateforme	ANSSI	T2-2027	P2			
31	Mettre en place un système national d'authentification unifié au service public numérique	Système d'identité numérique nationale opérationnel Cadre juridique et technique de l'eID	eID opérationnelle (Oui/Non) Nombre d'utilisateurs enregistrés (cible	ANSSI ONECI ARTCI	T1-2030	P3			

		Rapport d'Intégration avec les services publics	30% de la population recensée) Nombre de services publics intégrés						
Objectif stratégique 4.3 : Protéger les données des utilisateurs									
Résultats : Développer la Confiance numérique des usagers									
32	Intégrer la protection des données dès le début des projets	Registre de protection des données	% des projets ayant intégré la protection des données	~~ANSSI~~, ARTCI	T4 -2026	P1			
33	Elaborer un guide de bonnes pratiques de la protection des données dans le cyberespace	Guides de bonnes pratiques de protection des données dans le cyberespace Campagne de communication	Taux de pénétration (% des personnes ayant lu et mis en œuvre ces bonnes pratiques)	Ministères ARTCI ANSSI ACTEURS	T2-2027	P2			
Pilier 5 : Coopération nationale et Rayonnement International									
Objectif stratégique 5.1 : Favoriser l'émergence d'un écosystème national									
Résultats :									

• Mise en œuvre de conventions nationales de coopération clarifiant les rôles, responsabilités et engagements des différents acteurs ; • Renforcement des synergies entre institutions publiques, entreprises et centres de recherche.									
34	Créer et animer un forum d'échanges entre l'ANSSI, l'administration, les opérateurs du secteur publique et privé pour la lutte contre les cyberattaques	Termes de référence du cadre d'échange Cadre formel de concertation public-privé : document de création d'organisation et de formation Procédures de travail Règlement intérieur Comptes rendus et plans d'actions issus des réunions	Réunions planifiées (cible> 80%) -Taux de participation des acteurs ciblés (cible >80%) -Taux de prise en compte des recommandations issue du cadre d'échange -Nombre de conventions et ententes de coopération entre le public et le privé	ANSSI	T1-2027 : Mise en œuvre du cadre T2-2027-T4-2030 : animation des rencontres planifiées	P2 P4			
35	Mettre en place une plateforme nationale de partage et d'échange d'informations sur	Termes de référence du cadre d'échange Cadre formel de concertation public-privé : document de	Réunions planifiées (cible> 80%) Taux de participation des	ANSSI	T1-2027 : Mise en œuvre du cadre	~~P1~~			

	les menaces cyber (type MISP)	création d'organisation et de formation Procédures de travail Règlement intérieur Comptes rendus et plans d'actions issus des réunions Mise en place du dispositif technique	acteurs ciblés (cible >80%) Taux de prise en compte des recommandations issue du cadre d'échange Nombre de conventions et ententes de coopération entre le public et le privé		T2-2027-T4-2030 : animation des rencontres planifiées				
Objectif stratégique 5.2 : Accroître le Rayonnement International									
Résultats : • Positionnement renforcé de la Côte d'Ivoire comme hub digital et cyber de référence dans la sous-région ouest-africaine ; • Participation active et reconnue aux travaux des organisations régionales et internationales compétentes en matière de cybersécurité ; • Renforcement de la coopération transfrontalière pour la prévention et la gestion des menaces cyber									
36	Coordonner la participation active de la Côte d'Ivoire aux différents forums et activités internationales en	Liste officielle des organisations dont la Côte d'ivoire est Membre	Taux de participation aux réunions et activités internationales (cible 100%)	ANSSI	T4-2026	P1			

	matière de cybersécurité	Courriers d'adhésion aux réseaux et initiatives internationales Rapports de participation aux réunions, exercices et initiatives internationales Initiatives de textes régionaux (Directives régionales sur la cybersécurité°	Taux de présence de la Côte d'ivoire dans les instances internationales (cible > 70%)						
37	Organiser des exercices de gestion de crises cyber régionaux (CEDEAO/UA)	Rapports d'exercices régionaux (fiche RETEX) Planning d'exercices régionaux Catalogue de scénario d'exercice	Taux d'exécution du planning (cible 100%) Nombre de pays participants (cible > 8) Nombre de scénario exécuté (cible 3)	ANSSI	T4-2028	P2			