RÉPUBLIQUE DE CÔTE D'IVOIRE
Union - Discipline - Travail

MINISTÈRE DE L'ÉCONOMIE NUMÉRIQUE, DES TÉLÉCOMMUNICATIONS ET DE L'INNOVATION

STRATÉGIE NATIONALE DE CYBERSECURITE 2021-2025

v. 4.0 – 16 Novembre 2021

TABLE DES MATIÈRES

LISTE DES ACRONYMES

ANSUT : Agence nationale du service universel des télécommunications

ARTCI : Autorité de Régulation des Télécommunications de Côte d'Ivoire

CERT : Computer Emergency Response Team

CI-CERT : Côte d'Ivoire Computer Emergency Response Team

DGPN : Direction générale de la police nationale

DITT : Direction de l'Information et des Traces Technologiques

ESATIC : Ecole supérieure Africaines des Technologies de l'Information et de la Communication

FIRST : Forum of Incident Response and Security Team

IIC : Infrastructures d'Informations Critiques

INPHB : Institut national polytechnique Houphouët Boigny

LABTIC : Laboratoire des nouvelles Technologies de l'Information et de la Communication

MENUTI : Ministère de l'Economie Numérique, des Télécommunications et de l'Innovation

OCWAR-C : Organised Crime : West African Response on Cybersecurity and fight against Cybercrime (Réponse de l'Afrique de l'Ouest sur la Cybersécurité et la lutte contre la Cybercriminalité)

OIC-CERT : Organization of Islamic Cooperation Computer Emergency Response Team**PLCC :** Plateforme de Lutte Contre la Cybercriminalité

PSSI : Politique de Sécurité du Système d'Information

RGSSI : Référentiel Général de Sécurité des Systèmes d'Information

RSSI : Responsable Sécurité des Systèmes d'information

SNC : Stratégie Nationale de Cybersécurité

SNDI : Société nationale de développement informatique

TIC : Technologie de l'Information et de la Communication

UA : Union africaine

UIT : Union Internationale des Télécommunications

1. INTRODUCTION

1.1. Contexte

L'utilisation des technologies du numérique en Côte d'Ivoire a évolué de manière exponentielle ces dernières années, au point d'avoir acquis une très grande importance pour notre société. Outre les organisations du secteur public de façon générale, l'on distingue singulièrement les infrastructures dites critiques, telles que les réseaux de transport, de distribution d'eau et d'électricité, les organismes de santé, et les organisations du secteur financier. Tous ces secteurs clés et vitaux pour la santé économique et sociale de notre nation, se trouvent fortement liés à l'usage des technologies de l'information et de la communication. Cette dépendance au numérique a été exacerbée par le fait que leur usage améliore incontestablement la qualité des services fournis, favorise un accroissement de la productivité dans les organisations et contribue au renforcement de l'économie, impactant par ricochet la qualité de la vie du citoyen de manière générale. En effet, presque toutes les activités des organismes des secteurs public et privé sont majoritairement soutenues par les TIC, du site internet, aux systèmes d'information en passant par les moyens de stockage de données numériques (base de données, archivage électronique), etc. De ce fait, les organisations ne sauraient se départir de l'intégration de stratégies numériques efficaces, dans un marché économique mondial de plus en plus connecté.

Cependant, la multiplication des services associés et l'interconnexion des systèmes et outils technologiques ont entrainé une hausse des risques de sécurité liés à l'usage des TIC. Ainsi, les incidents de sécurité informatique de nature malveillante ou accidentelle connaissent une augmentation considérable dans notre cyberespace.

La cybercriminalité et les menaces de cybersécurité constituent donc le revers de la médaille de cette percée technologique. La possibilité pour un utilisateur malveillant de s'introduire frauduleusement dans un système d'information, d'y voler des données numériques confidentielles et même de perturber ou entraver le fonctionnement du système d'information d'opérateurs à infrastructures critiques, peut entrainer des graves conséquences, tant sur le plan économique que sur le plan humain, voire mettre à mal la sécurité intérieure et la stabilité de l'Etat.

1.2. Justification

Au vu de l'importance que le numérique a acquise pour la vie de notre nation et tous les enjeux sécuritaires y associés, il apparait plus qu'impérieux de mettre en place des moyens adaptés aux enjeux, afin de garantir la sécurisation des infrastructures technologiques et numériques hébergées ou utilisées sur le territoire national.

En effet, le cyberespace ivoirien n'échappe pas à l'explosion mondiale des cybercrimes et autres cybermenaces, telles que le cyberterrorisme, le cyber espionnage, etc. Le développement de l'infrastructure Internet d'une part et du e-commerce d'autre part, favorisent la montée en puissance de ces nouvelles formes de menaces. De surcroit, la relative facilité d'accès aux ressources (logiciels, forums,

formations, etc.) des marchés illicites en ligne accroissent les risques d'attaques informatiques et l'étendue des dégâts éventuels causés par de tels actes.

Pour faire face à ces menaces et assurer l'éclosion d'un environnement numérique propice à l'innovation technologique et qui soit porteur de développement, l'Etat Ivoirien a initié l'élaboration d'une stratégie nationale de cybersécurité 2021 - 2025. Cette stratégie vise à définir de façon claire et précise, les objectifs de sécurité ainsi que les moyens et l'organisation nécessaire à mettre en place au plan national. Elle est applicable à l'ensemble des infrastructures publiques et privées.

Les organismes des secteurs public et privé, la société civile et toutes les institutions étatiques sont appelés à prendre une part active à la mise en œuvre de la stratégie nationale de cybersécurité, dans la limite des prérogatives et rôles qui seront assignés à chaque acteur.

1.3. Définitions

Au sens de la présente stratégie, on entend par :

Cyberespace : le réseau interdépendant des infrastructures utilisant les technologies de l'information, comprenant notamment l'Internet, les réseaux de télécommunications, les systèmes d'information et les objets connectés ;

Cybersécurité : l'ensemble des mesures et des actions destinées à protéger le cyberespace des menaces associées à ses réseaux et à son infrastructure informatique ou susceptibles de leur porter atteinte. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues ; on parle alors de la triade CID (confidentialité, intégrité et disponibilité), à laquelle l'on peut ajouter comme quatrième élément la traçabilité ;

Cybercriminalité : les activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme, soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon, usurpation d'identité ….) facilites par l'usage du numérique, les délits liés au contenu (fichiers pédopornographiques, incitation à la haine raciale ...) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service, logiciel malveillant …).

1.4. Références et limitation du périmètre

L'élaboration de cette stratégie s'est appuyée sur :

- le Guide pour l'élaboration d'une stratégie nationale de cybersécurité de l'Union Internationale des Télécommunications (UIT) ;
- la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO.

- La politique régionale pour la protection des infrastructures critiques de la CEDEAO

La présente stratégie ne traite pas des aspects liés à la Défense ni à la Sécurité nationale. Ces aspects devront faire l'objet d'une démarche spécifique avec les Ministères en charge.

2. DIAGNOSTIC DE LA CYBERSECURITE EN CÔTE D'IVOIRE

En 2020, la Côte d'Ivoire s'est placée au 75ème rang mondial et au 11ème rang africain, sur les 194 pays classés à l'Indice Mondial de Cybersécurité (GCI). Cet indice, lancé en 2015 par l'Union Internationale des Télécommunications (UIT) pour mesurer l'engagement des États dans le domaine de la cybersécurité, permet de réaliser un diagnostic fiable et objectif, d'identifier les lacunes et les domaines d'amélioration, et d'encourager les Gouvernements à prendre les mesures idoines pour améliorer leur posture de cybersécurité.

Les résultats du GCI, qui sont basés sur 82 questions et 20 indicateurs, montrent une amélioration de onze places au niveau global, mais un recul de deux places au niveau africain entre 2018 et 2020. Ainsi, la Côte d'Ivoire a été surpassée par le Ghana et la Zambie en deux ans.

Le diagnostic présenté repose principalement sur l'étude du GCI, et aussi sur le rapport établi au 31 décembre 2020 par l'équipe du projet régional de l'Union Européenne et de la CEDEAO sur la Cybersécurité et la lutte contre la Cybercriminalité (OCWAR-C).

Ce rapport présente la situation de préparation de la CI en matière de cybersécurité et de lutte contre la cybercriminalité au 31 décembre 2020, notamment sur les aspects de stratégie et d'institutions, de cadre légal et règlementaire, de protection des infrastructures critiques, de capital humain, d'infrastructures et de coopération.

2.1. Etat des lieux

La situation est présentée suivant les cinq axes suivants :

- Le cadre légal ;
- Le cadre technique ;
- Le cadre organisationnel ;
- Le capital humain ;
- Les mesures de coopération.

2.1.1. Cadre légal

La Côte d'Ivoire dispose depuis 2013 d'un cadre juridique riche en matière de cybersécurité.

Ainsi, l'on note l'existence de :

- l'Ordonnance n° 2012-293 du 21 mars 2012 relative aux télécommunications et aux TIC (titre IX, chapitre 3), obligeant les opérateurs et fournisseurs de services à garantir le secret des communications (article 162) et à prendre les

mesures propres à assurer la protection, l'intégrité et la confidentialité des données à caractère personnel (article 164), ainsi que la sécurité des communications (article 167) ;
- la Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- la Loi n° 2013-451 du 19 Juin 2013relative à la lutte contre la cybercriminalité[1] ;
- la Loi n° 2013-546 du 30 Juillet 2013 relative aux transactions électroniques ;
- La loi n° 2017-803 du 7 décembre 2017 d'orientation de la Société de l'information en Côte d'Ivoire stipule que :
    - La législation et la réglementation en matière de télécommunication/TIC doivent garantir la sécurité et la redondance des réseaux de communication électronique (article 7), et assurer dans les meilleures conditions possibles la sécurité des réseaux et systèmes d'information (article 8),
    - Les responsables de réseaux et systèmes d'information doivent prendre toutes les mesures utiles pour en assurer la sécurité (article 8),
    - L'État met en place une politique nationale de sécurité des infrastructures et services TIC (article 18) ;
- l'Ordonnance n° 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui prévoit la mise en place, par décret, d'un ensemble de référentiels portant notamment sur la sécurité des données échangées par voie électronique;
- le décret n° 2014-105 du 12 Mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;
- le Décret n° 2014-106 du 12 Mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- le décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;
- le décret n° 2020-128 du 29 Janvier 2020 portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique (CI-CERT).

Tandis que ces lois ont très peu évolué depuis 2013, les menaces de cybersécurité ont, elles, fortement évolué.

Un Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) a été approuvé par décision n° 2019-494 du Conseil de Régulation de l'ARTCI le 6 mai 2019; un projet de plan de protection des infrastructures critiques et un projet de Politique de Sécurité des Systèmes d'Information (PSSI) ont été élaborés. Ces instruments devront être adoptés par décret, conformément aux Ordonnances 2017-500 et 2017-803.

2.1.2. Cadre technique

La prévention des attaques reste la meilleure approche. Cependant, peu de moyens techniques ont été mis en place à cet effet au sein des structures publiques, qui gèrent

[1] Le Conseil des Ministres a adopté, le 8 septembre 2021, un projet de loi modifiant les articles 17, 33, 58, 60, 62 et 66 de cette loi, afin de durcir la répression des actes de cybercriminalité.

elles-mêmes, chacune à son niveau, la sécurisation de leur infrastructure, de même que l'acquisition et l'usage de logiciels.

Aucune étude n'a pour l'instant été réalisée pour dresser l'état des lieux du niveau de sécurité du cyberespace ivoirien en général. Cependant, les nombreux incidents qui surviennent de manière récurrente (détournements de fonds, attaques de type ransomware, pertes de données, inaccessibilité des services, etc.) présagent d'un état des lieux technique peu satisfaisant.

Il existe, au sein de l'ARTCI, un Centre de Veille et de Réponse aux Incidents de Sécurité Informatique (CI-CERT) est membre de plusieurs réseaux régionaux et internationaux de structures de veille. L'existence du centre a été officialisée par décret en 2020.

Le CI-CERT dispose aujourd'hui d'un staff technique opérationnel pour les services de base, cependant ses procédures et processus d'organisation sont toujours en cours d'élaboration. Par ailleurs, le CI-CERT n'assure pas le monitoring et la supervision de la sécurité des infrastructures nationales, vu qu'il n'est pas doté d'un centre de supervision des opérations de sécurité (SOC). Il n'effectue pas non plus l'analyse avancée des codes et logiciels malveillants.

La Cote d'Ivoire ne dispose pas aujourd'hui de ses propres moyens techniques au niveau national pour assurer la surveillance continue des incidents de cybersécurité sur les infrastructures, réseaux et données, y compris ceux considérés comme critiques.

2.1.3. Cadre institutionnel

Les activités de cybersécurité et de la lutte contre la cybercriminalité ont jusqu'à présent été menées de façon disjointe entre plusieurs structures. Ainsi, les structures que sont l'ARTCI à travers sa Direction de la Confiance Numérique et de la Sécurité des Réseaux (DCNS) et sa Direction de la Protection des Données Personnelles (DPDP), le CI-CERT, l'ANSUT, la SNDI et la PLCC agissent dans le domaine.

La PLCC est aujourd'hui sans ambiguïté le point focal en matière de lutte contre la cybercriminalité.

Il n'existe pas de point focal sur les questions de cybersécurité au sein des Ministères ou des Institutions gouvernementales. Les structures qui agissent dans le domaine de la cybersécurité pour le compte de l'Etat n'ont donc pas de référant officiel qualifié dans les entités étatiques.

Le manque de cohésion et la fragmentation des initiatives nuit au rendement des ressources humaines, techniques et financières mobilisées par les différents acteurs.

Pourtant, la nature transversale de la cybersécurité soulève des défis en termes de structures organisationnelles, d'établissement des priorités, d'orientation des efforts à fournir en matière de renforcement des capacités, d'allocation de ressources de tous types, et de financement public et privé.

L'absence de coordination des actions a été jusqu'ici une des faiblesses majeures de la cybersécurité en Cote d'Ivoire.

Récemment, le décret numéro n° 2021-464 du 08 septembre 2021 portant organisation du MENUTI a créé une Direction de la Cybersécurité (DCS). Cette nouvelle Direction est désormais chargée, notamment, de :

- définir et proposer les stratégies, orientations et objectifs ;
- développer des plans et programmes relatifs à la sécurité des systèmes d'information et des réseaux dans les secteurs public et privé, et en suivre l'exécution ;
- assurer la coordination entre les divers intervenants ;
- assurer la veille technologique ;
- piloter les processus de prévention, de protection, de protection, de surveillance, de détection, de réponse aux incidents ;
- coordonner la gestion de crise en cas de cyberattaque.

2.1.4. Capital humain

Malgré l'existence d'une école d'ingénieurs locale, l'ESATIC, classée Centre d'Excellence en matière de cybersécurité par l'UIT, et la présence d'autres grandes écoles telles que l'INPHB, l'on déplore le manque de compétences nationales spécialisées en nombre suffisant, capables d'accompagner l'Etat ou les entreprises dans la sécurisation de leurs systèmes d'information.

En outre, il n'existe pas de cursus local de formation continue en cybersécurité pour les autres professionnels tels que ceux des domaines administratif, juridique et judiciaire, ou les forces de sécurité qui pourraient pourtant en bénéficier.

Des actions de sensibilisation des utilisateurs en général et des décideurs en particulier existent, mais sont en nombre insuffisant et manquent de coordination.

2.1.5. Coopération

La nécessité d'une coordination et d'une coopération, tant sur le plan national entre tous les acteurs impliqués que sur le plan international, découle du caractère supranational des réseaux de communication. Le but de cette coopération est d'aboutir à un échange d'informations et à une entraide entre les services compétents des différents pays, et au sein des instances internationales, ainsi qu'à la création d'approches et de solutions communes.

Il est dès lors impératif de disposer d'un tissu de collaboration actif avec la communauté internationale, en particulier au niveau des CERT et des forces de l'ordre. Aujourd'hui, à travers le CI-CERT, la Côte d'Ivoire bénéficie de l'appui technique de plusieurs réseaux régionaux et internationaux de structures de veille cybersécuritaire. En effet, le CI-CERT a déjà adhéré à plusieurs réseaux de centres de veille tels que le FIRST, et l'OIC-CERT.

Au niveau de la CEDEAO, la Côte d'Ivoire participe pleinement à l'initiative dénommée « Crime Organisé: la Réponse de la CEDEAO/Mauritanie sur la Cybersécurité et la Lutte contre la Cybercriminalité » (OCWAR-C). Cette initiative a permis l'adoption, par

le Groupe Régional Technique dont fait partie le MENUTI, d'une stratégie régionale de cybersécurité et de lutte contre la cybercriminalité, et d'une politique régionale de protection des infrastructures critiques.

Au niveau de l'Alliance Smart Africa, la Côte d'Ivoire est le pays phare du projet en cours visant l'élaboration de plans directeurs de la cybersécurité pour les Etats membres de l'Alliance. A ce titre, la Côte d'Ivoire travaille en étroite collaboration avec Smart Africa afin de produire un plan directeur continental de cybersécurité, puis le déployer dans des pays pilotes.

Au titre des conventions internationales sur la cybersécurité et la lutte contre la cybercriminalité, la Côte d'Ivoire n'a pas encore ratifié les deux conventions les plus importantes, à savoir la Convention de Budapest et la Convention de Malabo.

Concernant la première, le Gouvernement avait donné son accord pour l'adhésion de la Côte d'Ivoire à la Convention de Budapest le 12 juin 2019, mais la procédure est toujours en cours.

Pour ce qui est de la convention de Malabo, le processus d'adhésion et de ratification par la Côte d'Ivoire sera prochainement lancé.

L'ARTCI a signé des conventions avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, et avec l' Agence nationale de certification électronique (ANCE) en Tunisie.

2.2. Forces, faiblesses et opportunités

L'état des lieux de la cybersécurité en Côte d'Ivoire permet de relever les forces principales, les faiblesses et obstacles principaux et les opportunités et recommandations dans le tableau ci-dessous.

Forces principales	**Faiblesses et obstacles principaux**	**Opportunités et recommandations**
• Affirmation de l'ambition du Gouvernement d'accélérer la transformation numérique pour faire de la Côte d'Ivoire le hub digital de l'Afrique de l'Ouest, d'où la nécessité de sécuriser le cyberespace ; • Existence de plusieurs lois, ordonnances, décrets et décisions ; • Existence d'un centre de veille (CI-CERT) ; • Création d'une Direction de la Cybersécurité au sein du MENUTI en septembre 2021 ;	• Absence d'une stratégie nationale de cybersécurité ; • Absence d'une agence dédiée à la cybersécurité ; • Absence de coordination des actions ; • Insuffisance de ressources humaines formées en cybersécurité ; • Insuffisance de l'offre de formation en matière de cybersécurité ;	• Environnement favorable à la cybersécurité et à la lutte contre la cybercriminalité ; • Développement de programmes de formation en matière de cybersécurité ; • Existence de programme de formation régionale en matière de cybersécurité ; • Possibilités d'adhésion aux instances

• Existence du Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) (en cours de validation); • Existence d'un plan de protection des infrastructures critiques (en cours de validation) ; • Existence d'une école classée centre d'excellence en matière de cybersécurité (ESATIC) ; • Existence de la Stratégie Régionale de la Cybersécurité de la CECEAO • Compétence et expérience acquises par la DITT, notamment en matière de lutte contre la cybercriminalité et d'analyse forensique.	• Indisponibilité de ressources financières pour la formation et la sensibilisation en matière de cybersécurité ; • Non formalisation du réseau de point focaux de cybersécurité dans l'administration publique ; • Absence de PKI nationale • Absence de politique nationale de sécurité des systèmes d'information (PSSI) • Absence d'un observatoire de données statistiques sur la cybersécurité • Absence de CERTs sectoriels.	mondiales de cybersécurité ; • Ratification des conventions internationales relatives à la cybersécurité et à la lutte contre la cybercriminalité ; • Adoption d'une PSSI nationale ; • Vulgarisation du RGSSI ; • Adoption d'un cadre règlementaire des audits ; • Mise en place de l'identité numérique ; • Mise en place d'un observatoire des métiers de la cybersécurité.

3. ORIENTATIONS DE LA STRATEGIE DE CYBERSECURITE

Au regard du diagnostic établi ci-dessus, il apparait indispensable d'adopter une stratégie nationale pour répondre aux attentes du Gouvernement ivoirien relatives à la sécurisation du cyberespace et soutenir ainsi la réalisation de l'objectif de faire de la Côte d'Ivoire le hub digital de l'Afrique de l'Ouest.

La stratégie nationale de cybersécurité définie à cet effet identifie les enjeux, les principes, la vision, les objectifs stratégiques, ainsi que les axes stratégiques et les chantiers qui seront mis en œuvre.

3.1. Les enjeux

Les enjeux majeurs qui sous-tendent l'élaboration de la stratégie nationale de cybersécurité ont été identifiés et se déclinent comme suit :

(1) Définir une stratégie nationale en adéquation avec les objectifs fixés par le Gouvernement dans le Plan National de Développement pour la période 2021-2025, et conformément aux priorités sectorielles ;

(2) Elaborer une stratégie inclusive qui prenne en compte les préoccupations de l'ensemble des acteurs, incluant ceux du secteur privé ;

(3) Restructurer et rationaliser le cadre institutionnel existant pour une gestion plus efficace et performante de la cybersécurité et de la lutte contre la cybercriminalité ;

(4) Etablir une agence dédiée à la cybersécurité qui permettra à la Côte d'Ivoire d'améliorer sa posture de sécurité et de rentabiliser ses investissements visant à sécuriser son cyberespace ;

(5) Développer et mettre en œuvre un mécanisme de financement durable de la cybersécurité en Côte d'Ivoire.

3.2. La vision

Avec l'ambition de faire de la Cote d'Ivoire le hub digital de l'Afrique de l'Ouest, la vision est formulée comme suit :

« Sécuriser le cyberespace pour soutenir l'accélération de la transformation digitale et faire de la Côte d'Ivoire le leader africain en cybersécurité»

3.3. Les principes

La stratégie nationale de cybersécurité a pris en compte les principes clés suivants dans l'atteinte de ces objectifs :

- **La responsabilité partagée** : Tous les utilisateurs des services liés à la technologie des systèmes d'information (Acteurs privés, acteurs publics) devront mettre en œuvre les bonnes pratiques de sécurité afin de protéger leur information et garantir leur résilience.

- **Le développement de l'innovation numérique** : Le développement du numérique et de l'innovation étant un moteur que veut activer et amplifier le gouvernement ivoirien, la stratégie nationale cybersécurité est un facteur de développement..

- **La primauté du droit et le respect des droits de l'homme et des libertés fondamentales** : La stratégie nationale de cybersécurité sera mise en œuvre en conformité avec le cadre légal existant en Côte d'Ivoire, et avec les conventions internationales ratifiées par l'Etat. Elle est définie dans le respect des droits de l'homme et des libertés fondamentales des populations, avec une attention particulière donnée à la protection des données à caractère personnel et à la protection des enfants en ligne.

- **La coopération et la collaboration** : L'Etat s'engage à coopérer et à collaborer avec l'ensemble des parties prenantes du secteur de la cybersécurité, au niveau national et international.

- **L'amélioration continue** : La stratégie nationale de cybersécurité s'appuie sur une démarche d'amélioration continue afin de garantir la protection des infrastructures, des services, des données et des citoyens face à des risques en constante évolution.

- **L'approche basée sur les risques** : La stratégie va s'appuyer sur une approche basée sur les risques dans l'évolution, le suivi des menaces et dans la réponse aux incidents relatifs à la cybersécurité. L'Etat engage tous les intervenants à adopter une approche basée sur les risques. Les organisations publiques et les organisations critiques de l'Etat devront adopter la méthodologie d'analyse de risques de l'Etat.

Ces principes clés devront être respectés dans la mise en œuvre de la stratégie.

4. OBJECTIFS STRATEGIQUES ET OBJECTIFS SPECIFIQUES

En s'appuyant sur le diagnostic, la vision, les enjeux et les principes, des objectifs stratégiques, déclinés chacun en plusieurs objectifs spécifiques se présentent comme suit :

(1) Objectif stratégique 1 : Renforcer le cadre légal

Objectif spécifique 1.1 : Optimiser le cadre légal
Objectif spécifique 1.2 : Opérationnaliser le cadre légal

(2) Objectif stratégique 2 : Protéger le cyberespace

Objectif spécifique 2.1 : Mettre en place les moyens de détection des incidents
Objectif spécifique 2.2 : Elaborer et opérationnaliser un plan de gestion des crises
Objectif spécifique 2.3 : Protéger les systèmes d'information de l'Etat et les infrastructures critiques

(3) Objectif stratégique 3 : Renforcer la confiance numérique

Objectif spécifique 3.1 : Protéger les données des utilisateurs
Objectif spécifique 3.2 : Améliorer la sécurité des services en ligne

(4) Objectif stratégique 4 : Opérer une refonte du cadre institutionnel

Objectif spécifique 4.1 : Instituer un cadre de gouvernance optimal
Objectif spécifique 4.2 : Adopter et opérationnaliser les normes de sécurité

(5) Objectif stratégique 5 : Renforcer les capacités du capital humain

Objectif spécifique 5.1 : Accentuer les formations en cybersécurité
Objectif spécifique 5.2 : Réaliser une action permanente de sensibilisation
Objectif spécifique 5.3 : Encourager la recherche et le développement

(6) Objectif stratégique 6 : Accentuer la coopération internationale

Objectif spécifique 6.1 : Poursuivre la participation aux initiatives régionales et internationales
Objectif spécifique 6.2 : Ratifier les Conventions internationales

4.1. Objectif stratégique 1 : RENFORCER LE CADRE LEGAL

4.1.1. Objectif spécifique 1.1 : Optimiser le cadre légal

La Côte d'Ivoire devra procéder à la création d'un cadre de révision et d'amélioration du dispositif légal existant sur la cybersécurité.

Dans ce cadre de révision, elle définira, notamment, un cadre règlementaire :

- pour la souveraineté des données ;
- sur la déclaration des incidents de sécurité, afin de rendre celle-ci obligatoire.

La Loi n° 2016-412 du 15 juin 2016 relative à la consommation a prévu des dispositions génériques très larges et prend donc en compte les nouvelles exigences liées à la cybersécurité. Il faudrait modifier les dispositions du décret précisant les attributions, la composition, l'organisation, la composition et le fonctionnement de la commission de sécurité des consommateurs, afin d'y intégrer des spécialistes de la cybersécurité.

4.1.2. Objectif spécifique 1.2 : Opérationnaliser le cadre légal

La Côte d'Ivoire devra mettre en place des mécanismes d'information de la population sur le cadre légal existant, ainsi que des mesures d'incitation pour le respect de la règlementation sur la cybersécurité.

Les décrets d'application devront être pris pour permettre l'application effective de tous les textes existants, notamment la loi n° 2017-803 du 7 décembre 2017 d'orientation de la Société de l'information en Côte d'Ivoire, et l'Ordonnance 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Les modalités d'application des obligations de cybersécurité au secteur privé devront être précisées.

4.2. Objectif stratégique 2 : PROTEGER LE CYBERESPACE

4.2.1. Objectif spécifique 2.1 : Mettre en place les moyens de détection des incidents

La capacité de détecter les incidents de sécurité est un élément essentiel pour atteindre l'objectif de protection des infrastructures.
C'est pourquoi la mise en place d'un centre opérationnel de sécurité (SOC national) capable d'assurer le monitoring et la supervision de la sécurité en temps réel 24 heures sur 24 est nécessaire et urgente.

La mise en place d'un laboratoire d'investigation forensique permettra d'aider la Cote d'Ivoire dans sa perspective de développer des activités efficaces de veille et d'intelligence pour la détection des menaces.

L'Autorité en charge de la cybersécurité devra identifier les ressources pour la mise en œuvre du centre de supervision et du laboratoire, ainsi que leur gestion.

Les activités et services du centre de supervision et du laboratoire seront sous la responsabilité de l'Autorité en charge de la cybersécurité.

4.2.2. Objectif spécifique 2.2 : Elaborer et opérationnaliser un plan de gestion des crises

Dans une démarche de gestion de crise, à la suite de la détection d'incident de sécurité vient la phase de réponse à l'incident, qui nécessite l'élaboration et la mise en œuvre d'un plan de gestion des crises. L'Autorité en charge de la cybersécurité mettra en place un plan de gestion de crise.

Les capacités techniques, organisationnelles et humaines du CI-CERT devront être améliorées, et les CERT sectoriels prévus devront être mis en place, notamment dans le secteur bancaire. Les partenariats du CI-CERT avec les réseaux régionaux et internationaux permettra d'améliorer la capacite à faire face aux crises.

Le Gouvernement mettra en place un accord de partenariat entre les entreprises du secteur public et privé pour la lutte contre les cyberattaques. Cet accord permettra d'accentuer la collaboration entre les acteurs et réduire les risques sur les organisations. Le cadre de collaboration constitue un des leviers d'action pour améliorer la capacité de réponse aux incidents : la collaboration avec d'autres pays, avec d'autres CERT et avec des opérateurs privés. Une relation forte avec les opérateurs des télécoms permettra à l'Autorité nationale en charge de la cybersécurité de limiter les opérations en provenance de sources malveillantes.

Une plateforme de communication, d'alerte et d'échanges de données relatives aux menaces et aux attaques observées sera mise en place au profit des parties prenantes.

Outre les dispositions techniques mises en place par l'Etat, une importante mesure organisationnelle doit être prise afin de mieux orchestrer la gestion des incidents :

l'obligation de déclaration des incidents de sécurité pour tous les opérateurs. L'Etat a mis en place des dispositions spécifiques dans le cadre du décret de création du CI-CERT, de sorte à rendre obligatoire la déclaration des incidents de sécurité au CI-CERT. Celui-ci pourra ainsi diffuser les mesures de sécurité à prendre pour éviter que ces incidents ne se reproduisent dans les autres organismes du pays,, de façon anonyme, aux entreprises du secteur privé et public, pour prévenir les risques de sécurité informatique. Cette disposition est à mettre en œuvre de manière effective et rigoureuse.

Les entreprises du secteur public et les opérateurs d'infrastructures critiques auront donc l'obligation de communiquer tous leurs incidents de sécurité, ce qui constitue un élément clé de l'organisation de la défense des infrastructures.

4.2.3. Objectif spécifique 2.3 : Protéger les systèmes d'information de l'Etat et les infrastructures critiques

La Loi n° 2013-546 du 30 Juillet 2013, relative aux transactions électroniques, définit comme infrastructures critiques : « les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique et social des citoyens, ou encore le fonctionnement continu des services de l'Etat ».

Dans l'approche basée sur la gestion des risques, les infrastructures critiques seront les premières à être supervisées en temps réel dans le cadre de la mise en œuvre du plan de protection des infrastructures critiques, qui est en cours de validation. Vu que la grande majorité de ces infrastructures critiques (plus de 90%) appartiennent à des entités privées, leur protection nécessitera une forte collaboration public-privé.

C'est pourquoi, l'Autorité en charge de la Cybersécurité procèdera également à la création d'un cadre de collaboration sur les infrastructures critiques pour un partage d'expérience sur les risques et les incidents auxquels ils sont exposés au quotidien. Ce cadre de collaboration, outre les fins statistiques, permettra d'identifier les menaces pesant sur les organisations clés de l'économie ivoirienne et d'organiser une défense appropriée.

Il permettra à l'Autorité en charge de la Cybersécurité de faire des recommandations sur les moyens techniques, humains et organisationnels à mettre en place pour améliorer le niveau de sécurité des installations.

Le référentiel général de sécurité des systèmes d'information, en cours de validation, constitue le niveau minimal de sécurité à respecter par les organisations en charge des infrastructures critiques de l'Etat. L'Autorité en charge de la cybersécurité veillera au respect des exigences définies dans le Référentiel Général de Sécurité des Systèmes d'Information (RGSSI). Ce référentiel servira de socle pour l'ensemble des organisations en Côte d'Ivoire. Il sera obligatoire pour toutes organisations en charge de la gestion des infrastructures critiques d'en respecter les dispositions. Les audits et contrôles de sécurité se baseront sur la conformité au référentiel général de sécurité.

L'Autorité en charge de la cybersécurité définira une méthodologie nationale d'analyse des risques afin de mettre à la disposition des organisations un cadre de référence. Ce cadre de référence sera utilisé par l'Autorité et par les organisations mandatées par celle-ci pour évaluer les risques pesant sur les infrastructures critiques et les

administrations publiques. Cette méthodologie permettra d'évaluer de manière cohérente les risques pesant sur les organisations et de définir un niveau d'alerte commun en fonction de la sensibilité des actifs et du secteur.

Cette méthodologie commune d'analyse de risques sera obligatoire, pour l'ensemble des infrastructures critiques et pour le secteur public.

4.3. Objectif stratégique 3 : RENFORCER LA CONFIANCE NUMERIQUE

4.3.1. Objectif spécifique 3.1 : Protéger les données des utilisateurs

La protection des citoyens, des entreprises et de leurs données représente un enjeu clé pour développer la confiance numérique en Côte d'Ivoire.
Dans cette dynamique, la Côte d'Ivoire a promulgué depuis 2013 une loi relative à la protection des données à caractère personnel (Loi 2013-450 du 19 Juin 2013). Cependant cette loi reste peu connue par les citoyens.

Afin de permettre au plus grand nombre de mieux comprendre les risques liés aux données à caractère personnel et les droits de chaque citoyen, le Gouvernement devra vulgariser, pour le grand public, les éléments clés de la loi sur la protection des données à caractère personnel.

De plus, l'Autorité en charge de la Cybersécurité devra élaborer un guide de bonnes pratiques de la protection des données sur les réseaux sociaux, pour la prise de conscience des usagers de l'internet sur les cybermenaces.

Aussi, pour améliorer le niveau de sécurité des citoyens, le gouvernement ivoirien procédera à la revue de sa loi sur la protection des consommateurs en y intégrant les aspects liés à la Cybersécurité.

La protection des enfants en ligne constitue un enjeu important. 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.

Des actions de sensibilisation ont été initiées avec la mise en place d'un site internet de sensibilisation (jemeprotegeenligne.ci).

La problématique de la protection en ligne des personnes en situation de handicap devra elle aussi être traitée en raison des risques particuliers auxquels ces personnes sont exposés, notamment lors de l'utilisation des services numériques. Ainsi, un plan de protection en ligne sera élaboré.

En somme, il s'agira d'accentuer les actions de sensibilisation à destination du grand public face aux risques de divulgation des données à caractère personnel en général,

et mettre en place des plans de protection en ligne pour les personnes vulnérables en particulier.

4.3.2. Objectif spécifique 3.2 : Améliorer la sécurité des services en ligne

La Côte d'Ivoire a développé plusieurs services en ligne dans le cadre de sa démarche de dématérialisation. Ces services digitaux sont en phase avec l'ambition de modernisation de l'Etat et de développement du numérique en général.

Pour obtenir l'adhésion massive du public à ces services, il faudra améliorer les mesures de sécurité des portails de e-services proposés par l'Etat et par les entreprises privées.

Pour ce faire, une infrastructure à clés publiques (PKI) devra être opérationnalisée à l'échelle nationale pour garantir la confidentialité des échanges de données, l'authentification des utilisateurs, l'intégrité des données lors des transactions, et la non-répudiation des transactions. Cette action viendra renforcer les exigences de la loi sur les transactions électroniques.

Avant la mise en place de cette PKI, l'usage de certificats électroniques (disponibles dans le commerce) devra être promu, pour sécuriser au plus tôt les services en ligne, notamment les plus sensibles, et pour faciliter l'adoption par ces sites des certificats nationaux lorsqu'ils seront disponibles.

Au vu du fort développement des transactions électroniques et du commerce en ligne, l'Autorité en charge de la cybersécurité travaillera en impliquant la société civile au renforcement de la confiance des citoyens dans les transactions électroniques en général, et dans le commerce électronique en particulier, par la mise en place d'un label des sites marchands.

Un renforcement de la sécurité des moyens de paiement en ligne et mobiles sera mis en place ainsi que l'appui aux établissements financiers à se conformer aux standards de sécurité en vigueur. Ce renforcement de la sécurité cible aussi bien les services financiers classiques (banques) que les services financiers innovants (monnaie électronique) très répandus en Côte d'Ivoire.

Une assistance aux organisations sera portée par l'Autorité en charge de la cybersécurité afin de d'aider au renforcement de la sécurité des services en ligne et mobiles. Cette assistance pourra se matérialiser par la publication de bonnes pratiques de sécurité en matière de développement, ou par la réalisation d'audit de sécurité.

4.4. Objectif stratégique 4 : OPERER UNE REFONTE DU CADRE INSTITUTIONNEL

Cet axe stratégique vise à mettre en place les structures qui permettront d'assurer une gestion optimale de la cybersécurité.

4.4.1. Objectif spécifique 4.1 : Instituer un cadre de gouvernance optimal

Le processus d'élaboration et de mise en œuvre de la stratégie nationale de cybersécurité implique l'intervention de divers acteurs étatiques, non-étatiques et de

la société civile. La diversité de ces acteurs, les besoins en coordination et la capacité de mobiliser les ressources nécessaires sont des facteurs clé aussi bien dans l'élaboration de la stratégie nationale de cybersécurité que dans sa mise en œuvre.

Un nouveau modèle de gouvernance est proposé. Il sera constitué d'une Agence Nationale de la Cybersécurité, d'entités opérationnelles, et d'un réseau de points focaux de cybersécurité déployés dans les entités étatiques.

1) L'Agence Nationale de la Cybersécurité

La Stratégie régionale de cybersécurité de la CEDEAO prévoit que chaque État Membre établisse et désigne une autorité nationale de cybersécurité, disposant des pouvoirs et des moyens nécessaires pour assurer les fonctions suivantes, soit directement, soit par délégation d'une autorité gouvernementale (si possible interministérielle) :

- la gouvernance globale du dispositif national de cybersécurité (définition de la politique nationale et des politiques sectorielles de cybersécurité, élaboration de la stratégie nationale et des stratégies sectorielles, suivi des plans d'action, élaboration des textes législatifs et règlementaires, coordination des tâches liées à la cybersécurité, pilotage des dispositifs de prévention et de réaction, animation des échanges avec les parties prenantes publiques et privées, etc.) ;
- l'animation du dispositif national de cybersécurité, notamment au travers du centre de veille national ;
- la coordination avec les autorités en charge de la lutte contre la cybercriminalité ;
- la transposition des actes communautaires en matière de cybersécurité dans les textes nationaux ;
- le contrôle de la bonne application des Conventions internationales, des actes communautaires, de la présente Stratégie régionale et des dispositions législatives et réglementaires nationales en matière de cybersécurité ;
- le rôle de point de contact principal pour la coopération régionale et internationale.

L'autorité nationale de cybersécurité devra pouvoir exercer sa mission sur l'ensemble des secteurs d'activité (services de l'État, télécommunications, énergie, santé, transports, banques …), en liaison avec les autorités sectorielles compétentes et sans préjudice des pouvoirs dévolus à ces autorités.

L'Agence Nationale de la Cybersécurité devra donc être créée et pourra être placée sous la tutelle de la Primature, ou celle de la Présidence.

L'Agence Nationale de la Cybersécurité aura la charge de piloter la mise en œuvre des réformes et projets identifiés dans le cadre de la stratégie nationale de cybersécurité.
Les indicateurs de performance élaborés par l'Agence permettront un suivi et un contrôle réguliers de cette stratégie, ainsi que tous les projets qui en découlent.

Les attributions, l'organisation, le fonctionnement et le mode de financement de l'Agence Nationale de la Cybersécurité seront définis par décret pris en conseil des Ministres.

2) Les entités opérationnelles

Constituées d'entités du secteur public et du secteur privé qui seront chargées de la mise en œuvre d'un ou plusieurs volets du plan d'actions de la stratégie. Ces entités sont les agences d'Etat, les différents ministères, toute autre entité impliquée dans la mise en œuvre de la stratégie, ou encore toute entité créée, en tenant compte des besoins.

Toutes les entités ayant par décret ou par le biais de la loi des prérogatives en matière de cybersécurité sont d'office intégrées parmi les entités opérationnelles du modèle de gouvernance de la stratégie.

Elles sont responsables de la mise en œuvre du plan d'actions de la stratégie nationale dans leurs champs de compétences respectifs, conformément aux dispositions légales en vigueur.
Elles rendent compte à l' Agence Nationale de la Cybersécurité dans le cadre des leurs mission de cybersécurité qui sont les suivantes :

- Réaliser les projets et actions dont elles ont la responsabilité ;
- Rapporter à la demande de l'Agence Nationale de la Cybersécurité 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 à l'Agence Nationale de la Cybersécurité.

Les entités opérationnelles sont des structures identifiées parmi :

- Les entités étatiques ;
- Les organisations du secteur privé ;
- La structures de la société civile ;

3) Le réseau des points focaux de cybersécurité

Il sera créé au sein de chaque entité étatique un poste de Responsable de la Sécurité du Système d'Information (RSSI).
Sous la supervision de l'Agence Nationale de la Cybersécurité, le RSSI sera le point focal sur les questions de cybersécurité au sein de l'entité à laquelle il/elle sera affecté(e). Il/elle sera chargé(e) de l'amélioration continue de la sécurité du système d'information de l'entité.

A ce titre, au sein de l'entité, le RSSI aura pour missions :

- la définition, la diffusion, le suivi et le contrôle de la mise en œuvre par les parties prenantes de la Politique de Sécurité du Système d'Information ;
- la proposition et la mise en place de mesures et de procédures permettant d'améliorer le niveau de sécurité du système d'information ;
- l'analyse des risques de la sécurité des systèmes d'information ;
- le suivi des incidents de sécurité ;
- la sensibilisation, la formation et le conseil aux utilisateurs, y compris les décideurs, sur les enjeux de la sécurité des systèmes d'information;
- la veille technologique et règlementaire;
- alerter la hiérarchie sur l'existence de vulnérabilités critiques au regard du dispositif de sécurité informatique mis en place ;
- l'élaboration de rapports périodiques sur les vulnérabilités et les incidents.

4.4.2. Objectif spécifique 4.2 : Adopter et opérationnaliser les normes de sécurité

Plusieurs outils tels que le Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) et la Politique de Sécurité des Systèmes d'Information de l'Administration publique de l'Administration publique (PSSI) sont en cours d'adoption ou de validation. Ils devront être opérationnalisés afin de servir de base à l'adoption de bonnes pratiques par les utilisateurs du cyberespace.

L'Autorité en charge de la cybersécurité se dotera de moyens pour encourager, faciliter et contrôler l'adoption effective des normes de sécurité.

4.5. Objectif stratégique 5 : RENFORCER LES CAPACITES DU CAPITAL HUMAIN

Le capital humain est un des principaux facteurs limitants en matière de cybersécurité. Il s'agira non seulement de promouvoir la culture de la cybersécurité, mais également disposer de compétences et talents techniques capables d'implémenter des outils et mesures de cybersécurité.

4.5.1. Objectif spécifique 5.1 : Accentuer les formations en cybersécurité

Le développement d'une culture de la cybersécurité et le renforcement des compétences nationales en la matière sont des priorités pour la Côte d'Ivoire. Des actions seront menées non seulement pour les formations initiales, mais aussi pour la formation continue.

Ainsi, une des actions principales de l'Agence Nationale de la Cybersécurité sera d'œuvrer pour intégrer la formation à la cybersécurité et à la lutte contre la cybercriminalité dans les programmes de l'Education Nationale, de l'Enseignement Technique et de l'Enseignement Supérieur. Ainsi, des programmes de formation sur les cyber risques seront inscrits au sein du programme scolaire dès le primaire et le secondaire. Cette action visera également la formation des enseignants.

L'Etat ivoirien mettra en place dans le cursus de formation universitaire et des Grandes Ecoles, des contenus en sécurité informatique qui seront des formations diplômantes en cybersécurité. L'ESATIC, qui possède déjà cette filière verra ses capacités d'accueil augmentées, de sorte à accroitre le nombre de diplômés en cybersécurité produits chaque année.

De plus, l'Agence Nationale de la Cybersécurité 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 l'administration.

Les acteurs de l'administration publique et particulièrement les acteurs de l'environnement judiciaire (Magistrats, ENA, Police, Gendarmerie, etc.) devront bénéficier de formations en cybersécurité afin de mieux appréhender les nouveaux défis de leur métier traditionnel.

Le gouvernement ivoirien devra élaborer un partenariat avec les institutions internationales de formation et de certification pour renforcer les compétences de ses ressources dans le domaine de la cybersécurité.

L'Agence de cybersécurité développera par la même occasion, un programme de formation spécifique afin de constituer un corps d'auditeurs certifiés par elle-même. Cette création d'un corps d'auditeurs s'adresse à la fois aux personnes physiques par l'obtention d'un certificat qu'aux personnes morales par l'obtention d'une homologation comme prestataire d'audit de sécurité qualifié.

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

4.5.2. Objectif spécifique 5.2 : Réaliser une action permanente de sensibilisation

L'Agence Nationale de la Cybersécurité initiera des campagnes périodiques de sensibilisation de la population sur la cybersécurité en partenariat avec la société civile, le secteur public et le secteur privé en s'appuyant sur les professionnels de la communication.

Afin de toucher le plus grand nombre d'acteurs possible, les canaux et les messages de communication devront être adaptés à l'ensemble des couches de la population ivoirienne.

L'Agence mettra un accent sur la sensibilisation des hauts décideurs. Il est important qu'au plus haut niveau de management de l'Etat, l'importance de la stratégie et l' implication des décideurs dans le choix et l'exécution des actions à mener soient une réalité.

La mise en place d'un forum national annuel de sécurité pour les professionnels, aidera à promouvoir et à appuyer les évènements et les entreprises de sécurité. L'Agence Nationale de la Cybersécurité portera des actions de communication et de sensibilisation durant les forums spécialisés de la cybersécurité.

Elle désignera une période de l'année pour mener une campagne de sensibilisation nationale à l'échelle des entreprises et aussi au niveau des organismes de formations.

4.5.3. Objectif spécifique 5.3 : Encourager la recherche et le développement

Le gouvernement Ivoirien, avec l'appui du laboratoire de l'ESATIC et du laboratoire des TIC (LABTIC) de l'Institut National Polytechnique Houphouët Boigny (INPHB) organisera les recherches menées dans le domaine de la cybersécurité.

L'Etat étendra ses recherches sur la cybersécurité au niveau national à travers la création de plateformes d'échanges pour les opérateurs du secteur privé ; il favorisera la mise en place d'incubateurs pour le développement d'entreprises ivoiriennes dans le domaine de la cybersécurité.

La collaboration avec des partenaires privés nationaux ou étrangers, spécialisés dans la cybersécurité, constituera un accélérateur de la construction d'un écosystème de cybersécurité.
Afin d'atteindre l'objectif de devenir l'acteur de référence en matière de cybersécurité à l'échelle de l'Afrique, l'Agence Nationale de la Cybersécurité devra renforcer les capacités de l'ESATIC, centre d'excellence en cybersécurité. A ce titre, l'ESATIC devra être accessible à toutes les personnes désireuses de se former et de travailler dans le domaine de la cybersécurité, et se projeter comme un centre régional de compétences, de recherche et de développement sur la cybersécurité.

L'Agence Nationale de la Cybersécurité mettra en place un cadre de discussions avec le Ministère en charge de la recherche scientifique, afin de développer la recherche nationale dans le domaine de la cybersécurité et favoriser l'émergence de compétences dans ce domaine.

Le cadre d'échange et de discussions entre les professionnels de la cybersécurité et les professeurs de l'enseignement supérieur permettra de développer la recherche en alliant les approches théoriques et les pratiques existantes.

Afin de pouvoir découvrir de nouveaux talents et animer l'écosystème cybersécurité, la Cote d'Ivoire organisera de manière périodique des compétitions de cybersécurité à l'échelle nationale et régionale.

4.6. Objectif stratégique 6 : ACCENTUER LA COOPERATION INTERNATIONALE

4.6.1. Objectif spécifique 6.1 : Poursuivre la participation aux initiatives régionales et internationales

La coopération sur le plan international ne doit pas se limiter à l'échange d'informations opérationnelles. Elle doit aussi porter sur les aspects méthodologiques et les outils dans le domaine de la gestion d'incidents, sur les systèmes de détection d'anomalies, les systèmes d'alerte rapide, la gestion des risques, les politiques de sécurité, la sensibilisation et l'éducation.

La Côte d'Ivoire, en mettant en place un forum national et international sur la cybersécurité, créera un cadre d'échange favorable à la collaboration avec l'international. Ce forum devra être organisé chaque année.

Le gouvernement ivoirien démontrera son implication en participant activement aux évènements internationaux et régionaux sur la cybersécurité.

L'Agence Nationale de la Cybersécurité devra continuer la démarche d'adhésion du CI-CERT à des réseaux de collaboration internationaux et régionaux. Le CI-CERT a déjà adhéré aux organismes tels que le FIRST, et l'OIC-CERT. Il renforcera les relations bilatérales avec d'autres pays pour profiter non seulement des bonnes pratiques méthodologiques mais aussi des outils. Cette collaboration permettra à la Côte d'Ivoire de monter en compétence rapidement sur les sujets de cybersécurité.

La participation de la Côte d'Ivoire à l'initiative dénommée « Crime Organisé: la Réponse de la CEDEAO/Mauritanie sur la Cybersécurité et la Lutte contre la Cybercriminalité » (OCWAR-C) devra se poursuivre jusqu'à la fin du projet, prévue en 2023.

Au niveau de l'Alliance Smart Africa, la Côte d'Ivoire, qui est le pays phare du projet en cours visant l'élaboration du plan directeur de la cybersécurité pour les Etats membres de l'Alliance devra se donner les moyens de poursuivre sa participation à cet important projet, et de se positionner comme pays-pilote lors des phases de mise en œuvre prévues pour 2022.

4.6.2. Objectif spécifique 6.2 : Ratifier les Conventions internationales

La Côte d'Ivoire devra ratifier les conventions internationales en matière de cybersécurité et de lutte contre la cybercriminalité (Convention de Malabo et Convention de Budapest) pour non seulement accélérer la collaboration avec les autres pays , mais aussi favoriser l'amélioration de la confiance que les autres pays ont dans nos services numériques.

5. DISPOSITIF DE PILOTAGE ET DE SUIVI-ÉVALUATION

La présente stratégie définit les objectifs à atteindre dans les cinq (5) prochaines années en matière de cybersécurité. L'implémentation de la stratégie sera réalisée par l'Agence Nationale de la Cybersécurité. Un plan d'actions de cette stratégie est annexé au présent document.

Des objectifs de performances mesurables et réalisables seront définis pour chaque projet du plan d'actions de mise en œuvre de la stratégie. Ces objectifs de performances seront assignés aux parties prenantes en charge de la mise en œuvre des actions.

Des examens périodiques seront réalisés dans le cadre du suivi-évaluation de la stratégie de manière à garantir l'atteinte des objectifs fixés et à déclencher des alertes

en cas de dérive des projets. Un examen annuel sera réalisé sur l'avancement des projets. Une revue à mi-parcours de la stratégie et des risques sera réalisée à la fin de la 3ème année.

La stratégie nationale Cybersécurité doit être mise à jour tous les 5 ans à la suite du bilan de la précédente stratégie.

Un suivi-évaluation de la stratégie effectué de manière périodique permettra d'identifier les écarts, les retards, les anomalies, les nouveaux risques et de proposer des nouvelles mesures et des évolutions de la stratégie cybersécurité afin de faire face aux nouvelles menaces qui pourraient peser sur la Côte d'Ivoire.

6. ANNEXES

6.1. Plan d'actions

6.1.1. Réformes

#	Réformes	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Statut de l'activité
1.	Élaborer une stratégie nationale de cybersécurité	Obtenir une feuille de route pour réaliser la vision qui est de sécuriser le cyberespace pour soutenir l'accélération de la transformation digitale et faire de la Côte d'Ivoire le leader africain en cybersécurité	6 mois	2021-T2	P1	E1/P4/AN1	En cours
2.	Réaliser une étude d'optimisation du cadre légal	Optimiser le cadre légal	3 mois	2022-T1	P1	E1/P4/AN1	Non démarré
3.	Adopter et mettre en œuvre un plan national de protection des infrastructures critiques	Protéger le cyberespace, les systèmes d'information nationaux et les infrastructures critiques	6 mois	2021-T4	P2	E1/P4/AN1	En cours
4.	Développer et mettre en œuvre un plan national de gestion des crises		6 mois	2022-T1	P2	E1/P4/AN1	Non Démarré
5.	Adopter les textes sur la politique, les normes, les procédures et le contrôle de la cybersécurité		6 mois	2021-T4	P1	E1/P4/AN1	En cours
6.	Elaborer une stratégie de protection des données		6 mois	2022-T3	P2	E1/P4/AN1	Non démarré
7.	Elaborer un plan de protection des personnes vulnérables en ligne		6 mois	2022-T4	P2	E1/P4/AN1	Non démarré
8.	Réaliser une étude nationale d'identification et d'évaluation des infrastructures critiques		6 mois	2022-T1	P1	E1/P4/AN1	Non Démarré
9.	Mettre en place l'agence dédiée responsable des activités de cybersécurité	Optimiser le cadre de gouvernance	12 mois	2022-T1	P1	E1/P4/AN1	Non Démarré

10.	Formaliser et opérationnaliser le réseau des points focaux cybersécurité (RSSI) de l'administration publique		36 mois	2022-T1	P2	E1/P4/AN1	Non Démarré
11.	Créer et animer un cadre permanent d'échanges et de travail sur la protection des infrastructures critiques		6 mois	2022-T2	P2	E1/P4/AN1	Non Démarré
12.	Adhérer et/ou ratifier les conventions de Budapest et Malabo sur la cybersécurité	Renforcer la coopération internationale en matière de cybersécurité	12 mois	2021-T3	P1	E1/P4/AN1	En cours

6.1.2. Projets

#	Projets	Résultats attendus	Durée	Date début	Priorité	Lien PND 21-25	Statut de l'activité
Objectif stratégique 2 : Protéger le cyberespace							
13.	Mettre en place un CERT gouvernemental et créer 2 CERT sectoriels dans le secteur bancaire et les télécommunications	Renforcer les capacités techniques et opérationnelles du CI-CERT et des structures annexes	12 mois	2022-T3	P3	E1/P4/ AN2	Non Démarré
14.	Mettre en place un centre national de supervision des réseaux et services d'information critiques (SOC)	Renforcer les capacités de détection des incidents	12 mois	2022-T4	P2	E1/P4/ AN2	Non Démarré
15.	Construire un laboratoire national de forensique pour les analyses numériques	Acquérir les capacités opérationnelles pour les autopsies numériques	12 mois	2023-T1	P1	E1/P4/AN3/ AT1	Non Démarré
16.	Renforcer la protection des infrastructures critiques	Anticiper et prévenir les cyberattaques	24 mois	2022-T1	P1	E1/P4/ AN2/ AT3	Non Démarré
17.	Mettre en place une plateforme numérique pour le déroulement des cyberdrills nationaux	Évaluer les capacités d'interventions en cas d'attaque	Récurrent	2022-T1	P1	E1/P4/AN2/ AT4	Non Démarré

Objectif stratégique 3 : Renforcer la confiance numérique							
18.	Créer une plateforme nationale des services d'horodatage	Renforcer la sécurité des services informatiques	24 mois	2022-T1	P1	E1/P4/ AN2	Non Démarré
19.	Renforcer les capacités techniques de la PKI racine		24 mois	2023-T1	P3	E1/P4/ AN2/ AT2	Non Démarré
20.	Sécuriser les sites Internet en adoptant le protocole HTTPS		48 mois	2022-T1	P1	E1/P4/ AN2/ AT2	Non démarré
21.	Tenir une conférence annuelle sur la cybersécurité (secteurs public et privé, la société civile et les milieux académiques)	Renforcer le cadre collaboratif des acteurs de la cyber sécurité pour partager les expériences	Récurrent	2022-T2	P1	E1/P4/ AN2	Non Démarré
22.	Créer un label de sécurité (audit et certification) pour les plateformes fournissant des services de transaction en ligne ouverts au public	Mettre en place les infrastructures et les procédures permettant d'accroître la sécurité des systèmes d'information	12 mois	2022-T3	P2	E1/P4/ AN3/AT3	Non Démarré
23.	Mettre en place l'identité numérique nationale (eID-CI)		36 mois	2023-T1	P2		Non Démarré
24.	Intégrer les services clés de l'administration à une plateforme centralisée de signature électronique		12 mois	2022-T3	P3	E1/P4/ AN3/AT3	Non Démarré
Objectif stratégique 5 : Renforcer les capacités du capital humain							
25.	Organiser des campagnes pour développer la culture de cybersécurité des populations	Former les populations à un usage responsables des outils numériques	Récurrent	2021-T3	P2	E1/P4/AN2/ AT7	En cours
26.	Intégrer des modules d'éducation à la cybersécurité dans les cursus dès le primaire		12 mois	2023-T1	P2	E1/P1/AN1/ AT7	Non démarré
27.	Intégrer la cybersécurité dans la formation des fonctionnaires (Gendarmerie, Police, ENA, Magistrats, etc.)	Accroître la confiance numérique et l'employabilité par la formation, dans les nouveaux métiers et les domaines critiques	12 mois	2023-T1	P2	E1/P1/AN1/ AT7	Non démarré

28.	Créer des centres pour former à la cybersécurité dans tous les secteurs prioritaires de l'économie nationale	du secteur de l'économie numérique en Côte d'Ivoire	36 mois	2024-T1	P3	E1/P4/AN2	Non démarré
Objectif stratégique 6 : Renforcer la coopération internationale							
29.	Signer un MoU avec les autres Autorités nationales de cybersécurité (Autorités prévues par la Stratégie régionale de cybersécurité de la CEDEAO)	Promouvoir les partages d'expérience en matière de cybersécurité entre les acteurs	12 mois	2023-T3	P2	E1/P4/AN1	Non Démarré
30.	Mettre en place une plateforme de partage d'informations et renseignement opérationnels de sécurité (MISP)		12 mois	2023-T3	P2	E1/P4/AN1	Non Démarré

6.2. Financement de la SNCS2025

La mise en œuvre du plan d'action résultant de la SNCS2025 et l'opérationnalisation de l'Agence Nationale de la Cybersécurité nécessitent des financements significatifs, souvent au-delà des efforts financiers que peuvent consentir les autorités gouvernementales dans l'immédiat.

C'est pourquoi il est important d'identifier les sources et les stratégies de financement des investissements, et des sources de revenus réguliers pour couvrir les besoins de fonctionnement et les opérations courantes de l'Agence.

1. Les partenaires financiers Internationaux

Plusieurs bailleurs de fonds multilatéraux peuvent être sollicités pour apporter leur concours financier à la mise en œuvre du plan d'action stratégique de cybersécurité. Il s'agit notamment de :

- La Banque Mondiale, à travers son initiative D4A consacrée au développement de l'économie numérique. Dans ce cadre, les projets contributifs à la création d'un cadre favorable au développement de l'économie numérique pourraient être éligibles au financement.
- L'IUT dans le cadre de son projet de soutient à la mise en œuvre de centre de coordination de la réponse aux incidents de sécurité
- Etc.

Le principal avantage de ce mécanisme est la disponibilité plus ou moins immédiate des fonds qui peuvent être intégrés aux programmes de coopérations en cours d'exécution sous la forme de prêts concessionnels ou de dons.

2. Budget de l'Etat

Le programme peut être financé par le budget de l'état à travers :

- L'allocation de ressources nouvelles ;
- La centralisation de toutes les lignes budgétaires précédemment allouées aux structures ministérielles aux agences et structures publiques dans le cadre d'initiatives de cybersécurité qui rentreraient dans le cadre des activités inscrites dans la SNCS2025 ;
- La mobilisation de ressources auprès des entreprises d'Etat pour la mise en œuvre du volet du programme national de cybersécurité consacré à la sécurisation des systèmes d'information de l'Etat ;

Le principal avantage de cette approche est la maitrise du planning d'exécution de la Stratégie Nationale de Cybersécurité. Par ailleurs, la centralisation des lignes budgétaires consacrées aux investissements liés à la cybersécurité contribuera à la rationalisation des dépenses liées à ce secteur.

La principale limite du financement de la Stratégie Nationale de la Cybersécurité par le budget de l'Etat pourrait être l'incertitude liée à la mise à disposition des ressources financières.

3. Financement par le secteur privé

Les grandes entreprises installées en Côte d'Ivoire sont appelées à investir dans la protection de leurs activités vis-à-vis du risque du cybersécurité. Il est donc important de canaliser ces investissements dans le cadre de l'exécution de la stratégie Nationale

de Cybersécurité. Ceci pourrait concerner notamment les organismes détenteurs d'infrastructures critiques de communication, pour lesquels, un référentiel de protection et un niveau d'investissement minimal, individuel et collectif sera requis.

4. Le Partenariat Public / Privé

La Stratégie Nationale de Cybersécurité peut être financée par un partenariat public/privé, avec un(des) partenaire(s) privé(s) qui apporterai(en)t tout ou partie des capitaux nécessaires aux investissements sous la forme de prêts concessionnels. Le remboursement pourrait se faire sur la base des revenus propres de l'Agence avec une garantie de l'Etat. Par ailleurs, il serait envisageable que les remboursements soient directement pris en charge par le budget de l'Etat.

Le principal avantage d'une telle approche est la visibilité et la maitrise du risque lié au défaut de financement. Cela permettrait notamment à l'Agence d'être opérationnelle dans les plus brefs délais et de se positionner comme une structure efficiente et productive aux yeux de l'ensemble des parties prenantes.

Ce mode de financement permettra aussi à l'Agence de disposer rapidement de sources de revenus propres à travers de la prestation de service pour les secteurs public et privé.

5. Autres sources

Le Tableau ci-après présente diverses autres sources potentielles de financement de la stratégie :

Partenaires	Mécanismes de mobilisation
Coopération internationale	Au travers des instruments de soutien aux TIC des institutions financières et organismes internationaux, entre autres UA, UE, UIT, INTERPOL, SMART AFRICA, et de la coopération bilatérale et multilatérale
Les multinationales des TICs	Au travers d'accords de partenariats stratégiques avec les équipementiers, éditeurs de logiciels, etc.
Les organisations de la société civile (ONG, associations, …)	Au travers d'accords de partenariats spécifiques.