11/12/2020

Stratégie Nationale de Cybersécurité du Sénégal – SNC2022

Analyse de la mise en œuvre de 2018 à 2020

El Hadji Daouda DIAGNE

Spécialiste en cybersécurité

Tel : 221775254129

Email : computechnos@gmail.com

SOMMAIRE

I. Introduction

Ambitionnant de se mettre sur la rampe d'un développement assuré, le Sénégal a adopté le Plan Sénégal Emergent (PSE), stratégie nationale traçant l'orientation du Sénégal vers une nouvelle dynamique de développement économique et social.

En parfaite harmonie avec la transformation digitale, soupape de la globalisation, la vision claire du PSE « Un Sénégal émergent en 2035 » motive le fait que le pays compte s'appuyer sur le numérique comme moteur clé de la transformation structurelle de l'économie pour réussir le défi de son développement.

Par ailleurs, l'accélération de la diffusion des TIC est devenue aujourd'hui une réalité au Sénégal confortée par la multiplicité d'offres autour du haut débit, l'amélioration de la qualité des infrastructures, des services et la réduction des coûts. Etant conscient de ces atouts, le Sénégal a élaboré et adopté sa stratégie nationale de transformation en une société numérique « Sénégal numérique 2025 » (SN2025).

Le troisième pré-requis de la (SN2025) qui est « la confiance numérique » sous-tend la protection des infrastructures, des systèmes d'information, des utilisateurs et du cyberespace dans sa globalité. Ce qui est une nécessité avérée dans l'échiquier du numérique.

Pour garantir cette confiance numérique, le Sénégal devra se munir de tout élément approprié pour prendre en charge sa cybersécurité et prévenir les actes de cybercriminalité, voire même y remédier ou les réprimer. Fort de cela, le Sénégal a rajouté dans son dispositif un cadre stratégique, la « Stratégie Nationale de Cybersécurité 2022 » (SNC2022) ayant pour vision **« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ».**

Nous essayerons d'abord de faire un condensé de la Stratégie Nationale de Cybersécurité (SNC2022) pour ensuite analyser des progrès réalisés depuis sa validation. Ce qui conduira bien entendu à analyser les défis à relever pour la dernière ligne droite à savoir la période 2021 à 2022. Les atteintes aux droits numériques lors de la mise en œuvre de cette stratégie méritent un coup d'œil d'où leur prise en compte dans ce document. Nous terminerons par des recommandations à l'endroit des parties prenantes, particulièrement Etat et Société Civile, chacun en ce qui le concerne pour la prise en compte du respect des droits de l'homme dans la mise en œuvre.

II. Présentation de la Stratégie Nationale de Cybersécurité (SNC2022) du Sénégal

Développée en 2017, la « Stratégie Nationale de Cybersécurité 2022 » (SNC2022) articule la vision et les objectifs stratégiques à atteindre par le Sénégal en matière de cybersécurité.

Ce document proposé au Gouvernement par le Ministère des Postes et des Télécommunications (actuel Ministère de l'Economie Numérique et des Télécommunications) vient renforcer les priorités et les objectifs de la SN2025. Il traite des points suivants :

- L'évaluation du contexte stratégique de la cybersécurité au Sénégal
- L'approche du Gouvernement sur la cybersécurité et les objectifs à atteindre
- Les principes généraux de gestion et de suivi de l'exécution comprenant les rôles et responsabilités, l'évaluation
- Le cadre logique pour sa mise en œuvre ainsi que les projets prioritaires

Elle repose sur cinq objectifs stratégiques que le Gouvernement du Sénégal s'emploiera à atteindre.

- ✓ **Objectif stratégique 1** : renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal
- ✓ **Objectif stratégique 2** : protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal
- ✓ **Objectif stratégique 3** : promouvoir une culture de la cybersécurité au Sénégal
- ✓ **Objectif stratégique 4** : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs
- ✓ **Objectif stratégique 5** : participer aux efforts régionaux et internationaux de cybersécurité

Ces objectifs devront permettre de produire vingt-cinq (25) résultats à partir de quarante-neuf (49) actions à mener suite au déploiement de douze (12) projets prioritaires pour un budget de trois milliards cent quatre-vingt-dix-huit (3 198 000 000) francs CFA, soutenus par un mécanisme de suivi et d'évaluation.

Le Gouvernement s'emploiera à appliquer les principes relatifs à la gouvernance de la cybersécurité tout en mettant en place une structure nationale qui sera chargée de piloter la mise en œuvre assurant la coordination des initiatives liées à la cybersécurité.

Pour rappel, la stratégie a fait l'objet d'un point en conseil des ministres du mercredi 11 avril 2018 lors duquel le Chef de l'Etat a rappelé sa mise en place en plus de la politique de sécurité des systèmes d'information de l'Etat du Sénégal (PSSI-ES) comme un des dispositifs qui permettra d'assurer véritablement une gouvernance de la sécurité. Ce qui traduit ainsi sa volonté de diriger et de piloter la sécurité pour dominer les risques liés au numérique dans le respect des lois et règlements en vigueur. Après deux années d'existence, il semble opportun de faire un état des lieux.

III. Etude et analyse des progrès réalisés dans la mise en œuvre de la Stratégie Nationale de Cybersécurité de 2018 à 2020

Certes des avancées ont été notées avec la réalisation d'actions pas forcément coordonnées, n'empêche, nous essaierons d'avoir une vue plus rapprochée à travers l'étude comparative ci-dessous. Nous porterons notre analyse sur la base des actions qui ont été retenues à travers les objectifs stratégiques et spécifiques définis précisément en terme de ce qui a pu être réalisé, en cours de réalisation ou pas encore réalisé.

Objectif stratégique 1 : Renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal

- ✓ **Renforcer le cadre juridique de la cybersécurité**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Effectuer une analyse des déficits du cadre législatif et réglementaire des TIC, et élaborer des instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité	Un cadre législatif et réglementaire des TIC existe Le code pénal et le code de procédures pénales sont renforcés		
Souscrire aux conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité	Adhésion à la Convention de Budapest Adhésion à la Convention de l'Union africaine sur la Cybersécurité et la Protection des Données à caractère personnel (Malabo) Adoption des directives de la CEDEAO sur la cybercriminalité Adhésion à la convention 108 de l'UE		
Examiner et améliorer les dispositions législatives et règlementaires sur les pouvoirs de procédure en matière d'investigations d'actes de cybercriminalité pour prévenir, réagir et poursuivre les auteurs de ces actes plus efficacement.			✓
Renforcer le cadre législatif et réglementaire en matière de protection des données et l'aligner aux normes internationales		Un avant-projet de loi sur la protection des données personnelles abrogeant la loi de 2008 sur la protection des données	

- ✓ **Renforcer le cadre institutionnel pour assurer une gouvernance efficace de la cybersécurité**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Mettre en place une structure nationale de cybersécurité, laquelle mènera la mise en œuvre de la SNC2022 et sera responsable du développement et de la coordination des activités nationales relatives à la cybersécurité.			✓
Mettre en place le CERT/ CSIRT national sous forme d'unité au sein de la structure nationale de cybersécurité, avec des fonctions et responsabilités précises, y compris la réponse aux incidents.			✓
Identifier les institutions pertinentes des secteurs public et privé et en constituer un comité consultatif sur la cybersécurité dont le but sera de fournir des conseils stratégiques à la structure nationale de la cybersécurité			✓
Mettre en place un centre de commandement et de contrôle pour la cyberdéfense			✓
Renforcer le pouvoir des forces de défense et de sécurité, ainsi que leurs ressources en matière de lutte contre la cybercriminalité, notamment dans l'usage effectif d'outils d'investigation et d'établissement de preuves en cas de crimes ou délits commis à partir d'instruments numériques ou de réseaux informatiques		✓	
Élaborer une stratégie de cyberdéfense qui décrit l'approche nationale face aux cybermenaces envers la sécurité nationale			✓

- ✓ **Etablir des normes de cybersécurité, des lignes directrices et un cadre opérationnel et technique**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Edicter un ensemble de normes sur la cybersécurité, prenant en compte les normes internationales et adaptées au niveau national, entre autres pour les logiciels et le développement de leur code source.			✓
Mettre en place un cadre opérationnel et technique chargé d'édicter les normes de cybersécurité et du suivi de leur application			✓
Promouvoir la sensibilisation et la mise en œuvre des normes dans les secteurs public et privé, surtout pour les PME			✓

Objectif stratégique 2 : renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal

- ✓ **Assurer la protection des infrastructures d'information critiques et sécuriser les systèmes d'information du Sénégal**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Etablir un répertoire des IIC et des systèmes d'information du Sénégal			✓
Définir les cadres, les procédures et les processus nécessaires en matière de cybersécurité pour toute institution possédant ou gérant des IIC et les systèmes d'information du Sénégal			✓
Etablir un cadre de gestion des vulnérabilités des IIC et des systèmes d'information de l'Etat afin d'en promouvoir un suivi régulier			✓
Effectuer des tests et autres activités de surveillance réguliers des IIC et des systèmes d'information du Sénégal			✓
Définir des exigences minimales en matière de sécurité des IIC et des systèmes d'information du Sénégal.		✓	

✓ **Maintenir un suivi permanent des cybermenaces et une gestion des risques**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Définir des exigences minimales dans la tenue de répertoires d'incidents nécessaires à leur analyse			✓
Surveiller, analyser, gérer en continu les menaces et les risques, atténuer, préparer, intervenir et faire le retour d'incidents.			✓
Mettre en place un registre national des risques, les réglementations et les directives nationales afin de promouvoir l'évaluation et la gestion des risques			✓
Créer et continuellement actualiser un répertoire des incidents cybernétiques, évaluer ces incidents et proposer des solutions.			✓
Mettre en place des procédures de protection des informations et des procédures de gestion des risques.		✓	
Concevoir et mettre en œuvre des scénarii et programmes de simulation d'incidents de cybersécurité à utiliser lors des exercices nationaux			✓
Mettre en place des mesures nationales de gestion des crises, effectuer des tests périodiques au moyen d'exercices de cyberattaques et évaluer les enseignements tirés de ces exercices afin d'améliorer ces mesures			✓
Créer et continuellement actualiser un plan d'urgence de cybersécurité qui décrit les rôles et les responsabilités de la structure nationale de cybersécurité, des forces de défense et de sécurité en cas de cyberattaques.			✓

Objectif stratégique 3 : promouvoir une culture de la cybersécurité au Sénégal

- ✓ **Sensibiliser tous les groupes concernés ainsi que le grand public sur les risques de sécurité dans le cyberespace**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Effectuer une étude nationale pour déterminer le niveau de sensibilisation à la cybersécurité sur tous les pans de la société et mettre en place un programme national de sensibilisation pour couvrir les différents groupes-cibles			✓
Vulgariser les bonnes pratiques en matière de cybersécurité,		✓	
Mener des formations obligatoires en matière de cybersécurité pour les hauts fonctionnaires et les membres de conseils d'administration du secteur privé afin d'améliorer leur compréhension des risques et menaces et comment atténuer ceux-ci		✓	

- ✓ **Mettre en place un environnement de confiance fiable pour la fourniture des services gouvernementaux en ligne et des transactions électroniques**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Encourager l'utilisation des fonctions de sécurité de l'IGC, et notamment la confidentialité, l'authentification et l'intégrité pour créer des environnements fiables et sécurisés pour les services gouvernementaux en ligne et les transactions électroniques.			✓
Mener à bien la transition du protocole IPv4 au protocole IPv6.			✓
Assurer la prééminence des exigences de sécurité minimales dans le développement des services gouvernementaux en ligne et des transactions électroniques pour promouvoir la confiance numérique.		✓	

- ✓ **Promouvoir l'usage des services gouvernementaux en ligne et des transactions électroniques**

Actions	Etat des lieux		
	Réalisé	En cours de réalisation	Pas encore réalisé
Mettre en place les points de contact nationaux pour la cybersécurité dont le rôle sera, entre autres, la collecte d'informations sur les préoccupations des usagers des services gouvernementaux en ligne et des transactions électroniques, d'apporter des réponses à ces préoccupations et de promouvoir l'utilisation de ces services			✓
Informer le public sur les mesures de cybersécurité mises en place pour les services gouvernementaux en ligne et les transactions électroniques			✓

Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs

- ✓ **Renforcer les capacités et les connaissances techniques en matière de cybersécurité**

Actions	Etat des lieux		
	Réalisé	En cours de réalisation	Pas encore réalisé
Évaluer régulièrement les capacités et les connaissances techniques du CERT/ CSIRT national et des institutions étatiques afin de traiter les faiblesses identifiées.			✓
Former et orienter régulièrement le personnel du CERT/CSIRT national afin qu'il puisse faire face aux cyberattaques les plus sophistiquées			✓
Former et orienter périodiquement le personnel des institutions étatiques afin qu'il ait la capacité et les connaissances pour préparer, protéger, intervenir et effectuer les retours d'incidents		✓	
Établir des exigences de base en ce qui concerne la formation sur la cybersécurité pour les secteurs privé et public.			✓

- ✓ **Renforcer les capacités et les connaissances techniques nécessaires à l'application effective des textes législatifs et réglementaires**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Former et orienter en continu le personnel des services de sécurité et les autorités judiciaires afin de renforcer leurs capacités et leurs connaissances techniques pour traiter des cas de cybercriminalité.		✓	
Mettre en place les formations obligatoires liées aux investigations numériques et à la manipulation des preuves pour le personnel des services de sécurité, des autorités judiciaires et autres organisme œuvrant dans la détection et la poursuite d'actes de cybercriminalité.		✓	

- ✓ **Assurer une bonne adéquation formation/emploi en cybersécurité**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Élaborer un programme coordonné au niveau national sur l'éducation et la formation en cybersécurité, qui comporte un volet secondaire et universitaire sous la responsabilité des ministères concernés			✓
Promouvoir les carrières en cybersécurité.			✓
Évaluer et actualiser les programmes et la documentation pour les niveaux préscolaire, primaire, secondaire et universitaire pour y intégrer les notions de cybersécurité sous la responsabilité des ministères en charge de l'enseignement.			✓
Elaborer des conventions de partenariat entre les universités et grandes écoles nationales et/ou étrangères, le secteur public et le secteur privé pour mettre au point des programmes d'études, de recherche et de stages en cybersécurité.		✓	

- ✓ **Promouvoir le développement du secteur de la cybersécurité au Sénégal**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Promouvoir les investissements locaux et étrangers dans le secteur de la cybersécurité au Sénégal et proposer des mesures d'incitation.			✓
Réaliser des études sur l'impact de la cybercriminalité sur l'économie sénégalaise			✓
Soutenir les entreprises locales spécialisées dans le développement et la fourniture de solutions de cybersécurité.			✓

Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité

- ✓ **Renforcer la coopération internationale sur les questions liées à la cybersécurité**

Actions	Etat des lieux		
	Réalisé	**En cours de réalisation**	**Pas encore réalisé**
Coordonner la participation du Sénégal et renforcer sa collaboration avec les autres États et partenaires régionaux et internationaux sur la cybersécurité, notamment dans la lutte contre la cybercriminalité		✓	
Participer activement aux activités régionales et internationales de cybersécurité notamment dans la lutte contre la cybercriminalité.		✓	

Le tableau ci-dessous donne en valeur l'état des actions retenues dans le plan stratégique

Objectif stratégique	Intitulé	Objectifs spécifiques	Actions	Réalisé	En cours	Non Réalisé
1	Renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal	03	13	02	02	09
2	Protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal	02	13	00	02	11
3	Promouvoir une culture de la cybersécurité au Sénégal	03	08	00	03	05
4	Renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs	04	13	00	04	09
5	Participer aux efforts régionaux et internationaux de **cybersécurité**	01	02	00	02	00
	TOTAUX	**13**	**49**	**02**	**13**	**34**
	%			**4,1%**	**26,5%**	**69,4%**

Il ressort de cette analyse que seulement 4,1% des actions retenues dans la stratégie sont réalisées.

IV. Analyse des défis à relever dans la mise en œuvre pour la période 2021 à 2022

Certes, face à des délais très courts pour siffler la fin de vie de la stratégie, il convient de relever un certain nombre de défis. Ces derniers sont d'ordre organisationnel, technique, humain, juridique et financier.

Etant donné un déroulement très timide, il revient aux différents acteurs surtout à l'Etat du Sénégal de relever ces défis afin de ne pas rater le dernier virage.

Le premier défi qui est organisationnel est le socle de la structure et à ce niveau il est important de commencer par une prise en charge effective du pilotage et d'assurer le leadership. De facto, il n'est pas clair que la stratégie soit adoptée par le Gouvernement du Sénégal. C'est ce qui fait certainement qu'il n'y ait pas de politique qui en découle et qui fait défaut. Bien que l'existence de la politique de sécurité des systèmes d'information de l'Etat du Sénégal (PSSI-ES) est avérée mais son lien avec la SNC2022 n'est pas clairement défini.

Cependant, le nombre de cyber menaces grandissant avec une rapidité extraordinaire surtout en cette période de pandémie et ultérieurement post Covid19, il est plus qu'impératif d'avoir une politique de cybersécurité adoptée. Pour étayer cette thèse, la stratégie prévoit dans son objectif stratégique 1 la création d'une structure politique adéquate devant piloter la mise en œuvre, structure qui du reste peine à voir le jour. Cette même entité s'occuperait aussi de tous les aspects organisationnels y compris l'édiction de normes à adopter aussi bien dans le public que le privé. Devraient s'adosser à cette structure de pilotage des points de contacts nationaux pour la promotion de la culture de la cybersécurité sur l'ensemble du territoire (Objectif stratégique 3).

La mobilisation des acteurs dans la sensibilisation et l'éducation des populations, des agents de l'Etat, des entreprises publiques et privées devient un impératif à travers la mutualisation des actions soutenue par un mécanisme de partenariat inter acteurs.

Les organisations de la société civile qui ont un grand rôle à jouer à plusieurs niveaux doivent relever surtout le défi du plaidoyer et de la sensibilisation ; bien que sporadiquement certaines d'entre elles prennent de belles initiatives et se sont engagées de manière efficace dans la contribution à l'atteinte de l'objectif stratégique 3.

Le succès des actions contenues dans cette stratégie nationale relèvera d'une bonne communication coordonnée. C'est un pan nécessaire qui permettra d'abord à la population de s'approprier la stratégie et de se préparer en conséquence à participer activement aux différentes actions définies à travers les objectifs. Ce qui voudra dire qu'un plan de mise en œuvre intègrera celui d'une communication couvrant toutes les phases.

Suite à ce défi organisationnel, celui technique est à relever. En effet, les piliers techniques qui, pris en compte dans l'organisation architecturale de la stratégie permettront de réaliser les actions de veille et de protection définies. Bien qu'au niveau de l'ADIE (Agence de Développement de l'Informatique de l'Etat) un CSIRT (en anglais, Computer Security Incident Response Team - Une équipe d'intervention en cas d'incident de sécurité informatique) a été mis en place ce qui est une belle initiative qui est en parfaite adéquation avec la SNC2022. Les actions retenues au niveau de l'objectif stratégique 2 « renforcer la protection des infrastructures

d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal » devront impérativement être réalisées. Parmi ces actions, nous pouvons relever l'établissement d'un cadre de gestion des vulnérabilités des IIC et des systèmes d'information de l'Etat afin d'en promouvoir un suivi régulier, l'effectivité de tests et autres activités de surveillance réguliers des IIC et des systèmes d'information du Sénégal, la tenue de répertoire d'incidents, la surveillance, l'analyse, la gestion au niveau des menaces et les risques, l'atténuation, la préparation, l'intervention et le retour d'incidents, la conception et la mise en œuvre des scénarii et programmes de simulation d'incidents de cybersécurité à utiliser lors des exercices nationaux, entre autres. Rien que la réalisation de ces scénarii confirmera ou infirmera la vulnérabilité tant suscitée, par exemple, des sites web gouvernementaux ainsi que celle des systèmes de messagerie électronique qui doivent répondre à un minimum de sécurité qui est le chiffrement. Ceci permettra aussi d'évaluer à grande échelle les solutions de sécurité acquises ou développées en interne.

Le renforcement du capital humain constitue un autre défi à relever. La mise en place de l'Ecole Nationale de cybersécurité à Vocation Régionale est une action salutaire dans le dispositif de formation en cybersécurité. Cette école est en phase avec la stratégie à travers l'objectif stratégique 4 « renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs » avec le renforcement de capacités des agents de l'Etat. Elle n'est pas dans la formation diplômante.

N'empêche, qu'il est plus qu'urgent à l'instant où l'on parle de cyber guerres, où les attaques de grandes envergures se multiplient sur les systèmes financiers par exemple, qu'un investissement à sa juste valeur soit accordé à la production de jeunes ingénieurs et techniciens capables de faire face, promouvoir la recherche. Le pays a besoin d'experts, chevronnés, de haut niveau dans les domaines du digital forensic, de l'audit, de reprise d'activités, voire même constituer des équipes de hackers au service de l'Etat, etc. Le renforcement de ce capital humain passera forcément par la motivation des jeunes à suivre des formations certifiantes et diplômantes, surtout les filles. La principale motivation reste la garantie de l'emploi à la fin de leur formation. Ainsi le défi de la souveraineté technique est par conséquent levé. Le pays reposera sur sa propre expertise pour conduire les opérations d'audit de nos systèmes d'information. Aux menaces cybercriminelles, des solutions locales doivent être disponibles et déployées par des ressources humaines nationales.

Le Sénégal peut se réjouir d'être l'un des premiers pays africains à se doter déjà en 2008 d'un arsenal juridique pour combler le vide qui existait dans le domaine des TIC. Le pays a renforcé le code pénal et le code de procédures pénales, adhéré à la Convention de Budapest, adhéré à la Convention de l'Union Africaine sur la Cybersécurité et la Protection des Données à caractère Personnel (Malabo), adopté les directives de la CEDEAO sur la cybercriminalité. Tout récemment, une initiative de projet de loi sur la protection des données personnelles est agitée.

Aujourd'hui nous assistons à la prolifération de technologies émergentes et il sera donc un défi de s'adapter juridiquement à ces technologies. Dans ce cas, les lois existantes méritent d'être repassées à la loupe pour prendre en compte les technologies blockchain, l'intelligence artificielle, le big data, entre autres. La loi sur la protection des données à caractère personnel a fini de montrer ses limites.

Les finances, unanimement considérées comme le nerf de la guerre constitue un élément fondamental du dispositif. Le budget de la stratégie nationale de cybersécurité est arrêté à trois milliards cent quatre-vingt-dix-huit mille (3 198 000 000) francs CFA. Le défi reste la mobilisation de ces ressources pour une application effective au niveau des postes de dépense prévus sans oublier d'avoir un autre regard sur la répartition de ce budget par rapport aux projets prioritaires.

Un défi plus qu'important reste celui de l'évaluation qui à date fait défaut l'opinion publique qui du reste était mise au parfum de la SNC2022 a besoin d'une évaluation diligentée par la tutelle.

V. Explorer les atteintes aux droits numériques lors de la mise en œuvre de la stratégie nationale de cybersécurité du Sénégal pour la période 2018 – 2020 ;

Selon wikipedia, le droit numérique est la partie du droit spécifique aux nouvelles technologies. Il régit les problèmes créés par l'émergence de la société de l'information, et vise principalement :

- la protection de la vie privée mise à mal par la collecte informatique des données,
- la protection de la propriété intellectuelle, les œuvres étant facilement copiables illicitement sous leur forme numérique.
- l'accessibilité numérique contre la fracture numérique.

Au regard de ce qui ressort de la lecture de la stratégie nationale de cybersécurité, l'objectif stratégique 1 « Renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal » dans son objectif spécifique « renforcer le cadre juridique de la cybersécurité » prend en compte la mise en place d'un dispositif judicaire renforcé chargé de garantir le respect des droits fondamentaux des citoyens quand il s'agit du numérique.

Par contre, il n'est mentionné nulle part dans ladite stratégie une prise en compte de ces droits fondamentaux lors de sa mise en œuvre. Ce qui vraisemblablement peut être une porte ouverte pouvant porter atteintes aux droits. Or le processus de mise en œuvre impliquera forcément le droit d'accès à l'information vu sous trois aspects :

- ✓ la protection des données à caractère personnel
- ✓ les atteintes aux sources d'information et plus spécifiquement l'atteinte au patrimoine informationnel des personnes morales par le biais des techniques cybercriminelles
- ✓ les atteintes au droit de la propriété intellectuelle commises au moyen d'outils de communication électronique.

Le gouvernement du Sénégal, porteur de la Stratégie Nationale de Cybersécurité ne pourra pas éviter les atteintes aux droits numériques dans la mesure où dans son objectif stratégique 2, il est prévu de faire un état des lieux exhaustif des vulnérabilités et des niveaux de sécurité des IIC et des systèmes d'information, d'effectuer des tests et autres activités de surveillance réguliers des IIC et des systèmes d'information. Aussi il est prévu dans la mise en œuvre de la stratégie l'organisation de simulations d'incidents.

Ces actions usant de techniques comme le spamming, le phishing, le Denis de Service, la géolocalisation, des tests de pénétrations, etc., porteront forcément atteinte aux droits d'autant plus que le fonctionnement des systèmes informatiques sera affecté et beaucoup de données seront collectées à l'insu des utilisateurs. Sans oublier les accès ou tentatives d'accès aux systèmes d'information d'autrui punis par la loi sur la cybercriminalité. Etendu au niveau national et privé, l'impact sera dévastateur si toutes les mesures idoines ne sont pas prises pour garantir une bonne sécurité dans l'exécution de ces actions.

VI. Recommandations aux parties prenantes chacun en ce qui le concerne pour la prise en compte du respect des droits de l'homme dans la mise en œuvre de la stratégie nationale de cyber sécurité du Sénégal

La cybersécurité c'est l'affaire de tous, par conséquent tous les acteurs et parties prenantes de ladite stratégie nationale devront incarner une prise en compte certaine du respect des droits de l'homme dans la mise en œuvre.

L'Etat aurait dû commencer déjà à l'aube de la validation de la SNC2022 par l'élaboration d'une politique et la mise à disposition d'un plan de mise en œuvre claire tenant compte du respect des droits fondamentaux.

Fondamentalement le Gouvernement devra

- Initier une loi spécifique sur la cybersécurité qui facilitera l'applicabilité
- Définir et adopter la politique de cybersécurité qui découle de la stratégie nationale, créer les cadres politique, opérationnel et technique, lieux d'échange sur la cybersécurité réunissant tous les acteurs pour développer une culture de la cybersécurité au sein des structures étatiques et privées.et celle des organisations de la société civile
- Favoriser une coopération entre les parties prenantes (Etat, secteur privé et société civile, écoles et universités) pour une mise en œuvre efficace de la stratégie nationale de cybersécurité
- Impliquer les parlementaires qui votent les lois ainsi que les autorités territoriales pour une prise de conscience effective des vulnérabilités du numérique par une sensibilisation efficace, sans oublier la formation continue des autorités judiciaires
- Mette en place un plan de communication couvrant les étapes de la mise en œuvre tout en garantissant le droit à l'information et la protection des données à caractère personnel
- Organiser la revue du cadre législatif à harmoniser avec les besoins des technologies émergentes
- Identifier et mettre en œuvre trois projets phares à fort impact et réalisables d'ici 2022

La Société Civile est un maillon important du processus de mise en œuvre de la Stratégie Nationale de Cybersécurité, les organisations ont un rôle important à jouer.

Elles peuvent mener des actions simples et efficaces qui tiendront compte à éviter les atteintes aux droits du numérique :

- ✓ Mener des campagnes de plaidoyer, de sensibilisation, d'éducation à la cybersécurité et le respect des droits de l'homme
- ✓ Initier des programmes ou participer à des émissions de sensibilisation à la cybersécurité au niveau des média.
- ✓ Aider les autorités judiciaires dans la lutte contre la méconnaissance des lois existantes par les populations.
- ✓ Servir de structure de veille et d'alerte aux atteintes aux droits humains.

Dans l'éducation et la formation à la cybersécurité l'apport des structures académiques pourra être considérable.

Entre autres actions, elles peuvent :

- ✓ Développer un enseignement de la cybersécurité à l'école déjà pour les moins jeunes
- ✓ Développer et mettre en pratique des programmes au niveau de l'enseignement supérieur avec un renforcement des moyens pour des expérimentations
- ✓ Promouvoir la recherche de solutions matérielles, logicielles et opérationnelles avec une mise en place effective d'un CERT/CSIRT universitaire

VII. Conclusion

Le Sénégal s'est dotée d'une bonne stratégie de cybersécurité pour faire face aux menaces auxquelles qui guettent les systèmes d'information du pays. Cependant plusieurs défis à relever font que cette stratégie peine à être effective dans sa mise en œuvre. Néanmoins, après deux années d'existence, des actions salutaires ont été réalisées ou sont en cours de réalisation. Par conséquent, les deux prochaines années seront vraiment déterminantes dans cette recherche de cyber protection. Il revient donc au Gouvernement du Sénégal de tout mettre en œuvre pour atteindre la vision tant déclinée tout en prenant en compte le respect des droits humains.