

LA CYBERSÉCURITÉ ET LA SOUVERAINETÉ NUMÉRIQUE AU SÉNÉGAL



”

**Tendances de la
cybercriminalité en 2025
au Sénégal: Vers un
cyberespace sûr, souverain
et durable?**

”

AUTEUR

Gérard DACOSTA

Ingénieur en MSSI-SysAdmin-IT Trainer & IT Consultant

PRÉFACE

Pape Fodé DRAMÉ

Président de l'Association Africaine des Droits Numériques (ADN)
& Juriste et Délégué à la protection des données (DPO)

LA CYBERSÉCURITÉ
ET LA SOUVERAINETÉ
NUMÉRIQUE AU
SÉNÉGAL

LA CYBERSÉCURITÉ ET LA SOUVERAINETÉ NUMÉRIQUE AU SÉNÉGAL

**«Tendances de la
cybercriminalité en 2025 au
Sénégal: Vers un cyberspace
sûr, souverain et durable?»**

AUTEUR

Gérard DACOSTA

Ingénieur en MSSSI-SysAdmin-IT Trainer & IT Consultant

PRÉFACE

Pape Fodé DRAMÉ

Président de l'Association Africaine des Droits Numériques (ADN)
& Juriste et Délégué à la protection des données (DPO)

LIVRE BLANC

Copyright © 2025

ISBN: 979-10-978269

Mention Légal

Tous droits réservés. Aucune partie de ce livre ne peut être reproduite sans l'autorisation de l'auteur.

PRÉFACE

La cybersécurité représente aujourd'hui un défi majeur pour les organisations, confrontées à des menaces telles que le vol de données, les attaques par ransomware, le phishing, l'usurpation d'identité ou encore les attaques par déni de service.

Ces menaces se professionnalisent, s'automatisent et s'intensifient, tandis que la transformation numérique, en pleine expansion, poursuit une dynamique irréversible. Cela amplifie indubitablement les risques pour les systèmes d'information et le patrimoine informationnel des organisations.

Au cœur de cette mutation technologique se trouve sa matière première : les données. Véritable mine d'informations, elles font l'objet de toutes les convoitises et demeurent la cible privilégiée des cyberattaques. Ces attaques ne se limitent pas au vol, à la diffusion non autorisée ou à l'indisponibilité des données ; elles peuvent causer des perturbations majeures, allant jusqu'à paralyser des services essentiels tels que la santé, l'approvisionnement en eau, l'énergie, les transports, les banques, les administrations, avec des conséquences directes sur la vie quotidienne des citoyens.

Dans ce contexte, l'Intelligence Artificielle (IA), certes l'une des grandes avancées du XXI^e siècle, est en passe de devenir un redoutable vecteur de menaces, notamment parce qu'elle est exploitée à des fins malveillantes. En effet, les cyberdélinquants l'utilisent opportunément pour développer des outils basés sur des modèles existants entraînés à partir de vastes bases de données.

Rappelons qu'en juillet 2023, le Kenya a vu sa plateforme eCitizen, qui permet d'accéder à plus de 5 000 services publics numériques, être la cible d'une cyberattaque majeure. Cette attaque, revendiquée par un groupe appelé Anonymous Sudan, a perturbé des services essentiels tels que les demandes de passeports, les e-visas, les permis de conduire et les dossiers médicaux. Elle a également touché des services bancaires et financiers comme les paiements M-Pesa ainsi que les services de Kenya Power¹. De nombreux experts estiment que l'IA a pu être utilisée pour automatiser certaines étapes et améliorer la coordination de ces attaques à grande échelle.

Plus récemment, le 8 avril 2025, la Caisse nationale de Sécurité sociale (CNSS) du Maroc a subi une cyberattaque d'une ampleur sans précédent. Cet incident a entraîné la fuite de données sensibles, incluant des informations personnelles, financières et médicales de millions de citoyens marocains². Un groupe cybercriminel actif, sur le darknet, a revendiqué l'attaque et publié des fichiers volés pour démontrer son accès aux serveurs internes de l'institution.

Ces incidents illustrent, d'une part, à quel point nos systèmes modernes sont à la fois interdépendants et vulnérables, et d'autre part, les défis auxquels sont confrontés nos gouvernants s'ils ne prennent pas pleinement la mesure des enjeux de la cybersécurité.

De plus, les organisations doivent dépasser les dispositifs classiques et adopter une défense proactive et agile pour contrer ces menaces désormais dopées par l'IA.

De toute évidence, les violations de données à caractère personnel sont devenues monnaie courante au sein des organisations, notamment dans les institutions bancaires, financières et les entreprises de télécommunication, en raison du volume important de données qu'elles traitent. Dès lors, une rigueur renforcée en matière de protection des données est non seulement attendue, mais essentielle pour garantir la confiance des usagers et respecter les exigences réglementaires en vigueur.

¹ Jackson, A. (2023). Cyberattack in Kenya impacts online government platforms.

Cyber Magazine, [Cyberattack in Kenya impacts online government platforms](#) | *Cyber Magazine* consulté le 02 avril 2025

² Elhamzaoui, B. (2025). La cyberattaque contre la CNSS décryptée en neuf points clés.

Médias24 | <https://medias24.com/2025/04/12/la-cyberattaque-contre-la-cnss-decryptee-en-neuf-points-cles/> consulté le 20 avril 2025

À l’instar du Sénégal, plusieurs pays africains sont confrontés aux mêmes problématiques en matière de cybersécurité. Cela met en évidence la nécessité d’une approche panafricaine et une harmonisation des cadres juridiques pour renforcer la résilience numérique à l’échelle du continent. Pour l’heure, il est essentiel de tirer parti des cas récemment relayés par la presse pour moderniser notre dispositif de Lois d’Orientation sur la Société de l’Information³ (LOSI) en vigueur depuis 2008, ainsi que les réglementations sectorielles, et d’adapter les stratégies de réponses aux menaces émergentes. À ce stade, il est impératif de mettre en œuvre des politiques efficaces de sécurité et de gouvernance des données, tout en investissant dans des infrastructures numériques solides.

Il est tout aussi crucial d’instaurer une ligne de défense humaine à tous les niveaux, en s’appuyant sur la sensibilisation, la formation continue et un accompagnement institutionnel adapté. La cybersécurité ne peut plus être envisagée comme une posture statique : elle doit être dynamique, évolutive et capable de répondre aux attentes croissantes des citoyens et des personnes concernées. C’est dans cette optique que l’auteur de ce livre blanc propose des perspectives concrètes, orientées vers plus d’efficacité, de résilience et d’efficience.

Bonne lecture!



Pape Fodé DRAMÉ

Président de l’Association Africaine des Droits Numériques (ADN) &
Juriste - Délégué à la Protection des données (DPO)

Avant-propos



Gérard Joseph Francisco DACOSTA

Ingénieur en cybersécurité – Responsable Pôle Infra à IT4LIFE
– IT Trainer & IT Consultant

Rédiger ce livre blanc a été bien plus qu'un exercice technique ou académique. C'était une manière de poser des mots sur une urgence, celle de faire réellement de la cybersécurité une priorité nationale au Sénégal.

En tant qu'ingénieur en cybersécurité option MSSSI, IT Trainer, IT Consultant, passionné de l'informatique, plus précisément de la cybersécurité et faisant partie des acteurs les plus actifs de l'écosystème, si j'ose dire; j'ai été longtemps témoin de tout ce mouvement noté dans le cyberspace sénégalais : j'ai vu les risques s'intensifier, les failles se creuser, des talents émerger, des communautés s'organiser, mais aussi voir les consciences s'éveiller de jour en jour. C'est à travers cette observation que j'ai écrit ce document.

J'ai voulu qu'il soit concret, structuré, mais surtout accessible à tous. Car derrière chaque donnée fuitée, chaque infrastructure vulnérable, chaque attaque, il y a une réalité peut être : celle d'un citoyen exposé ou d'un Système d'Information fragilisé ou d'une nation menacée.

Je ne prétends pas avoir toutes les réponses. Mais si ce livre peut susciter des débats, éclairer des décisions, inspirer une stratégie, ou simplement réveiller certaines "cybervocation" chez les jeunes, alors j'aurai accompli une petite partie d'une mission que je me suis confiée à savoir aider à rendre notre cyberspace sûr.

L'Afrique peut toujours exprimer son ambition de souveraineté numérique. Le Sénégal peut en être l'un des premiers porte-voix.

Merci à celles et ceux qui croient encore en une transformation digitale intelligente, inclusive et réfléchie pour notre pays, et pour l'ensemble du continent africain.

Auteur: Gérard Joseph Francisco DACOSTA

Ingénieur en cybersécurité – Responsable Pôle Infra à IT4LIFE – IT Trainer & IT Consultant

Je vous souhaite une excellente lecture

ANCRAGE DANS LES RÉFÉRENCES EXISTANTES ET PERSPECTIVES D'ÉVOLUTION

Ce Livre Blanc ne prétend pas inaugurer un débat nouveau, mais plutôt s'inscrire dans la continuité des travaux déjà menés par plusieurs experts sénégalais et africains, qui, ces dernières années, ont contribué à éclairer les enjeux stratégiques de la cybersécurité, de la gouvernance numérique et de la protection des données personnelles.

Parmi ces contributions notables :

- **Dr Papa Assane TOURE**, magistrat, dont les écrits sur la cybercriminalité et la régulation numérique ont posé des bases juridiques solides pour le contexte sénégalais et ouest-africain ;
- **Dr Papa GUEYE**, Directeur de l'École nationale de cybersécurité à vocation régionale de Dakar (ENCVR), enseignant-chercheur et auteur de Criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles (2020), dont les travaux ont enrichi la réflexion sur la cybersécurité et la protection des données en Afrique ;
- **M. Baidy SY**, auteur du Livre Blanc sur la cybersécurité au Sénégal (2019), qui a permis une première analyse critique du cadre juridique et institutionnel ;
- **M. Dr Mouhamadou LO**, expert en protection des données personnelles, ancien président de la Commission des Données Personnelles (CDP) du Sénégal, auteur de La protection des données à caractère personnel en Afrique (2017), dont les travaux ont structuré la réflexion sur la régulation des données en Afrique ;
- **DRAME, Pape Fodé & Maître SARR, Rokhaya**, L'impact du RGPD sur la protection des données personnelles en Afrique, éditions Harmattan, 2021 :

- Les rapports et lignes directrices de la Commission de Protection des Données Personnelles (CDP), de l'ARTP, ainsi que les travaux régionaux (Convention de Malabo, directives CEDEAO) et continentaux (Smart Africa, AfricaCERT, Association Africaine des Droits Numériques - ADN).

Ce présent Livre Blanc vise à compléter ces apports en :

- **Proposant un aperçu de l'état des lieux ;**
- **Intégrant les enjeux liés aux technologies émergentes (IA, Blockchain, Cloud, Ordinateur quantique) ;**
- **Proposant un cadre de gouvernance renforcé, adapté aux réalités sénégalaises et africaines ;**
- **Plaidant pour une approche transversale, inclusive et souveraine de la cybersécurité.**

Une démarche constructive et prospective

Ce Livre Blanc s'inscrit dans une dynamique d'accompagnement et de consolidation : il ne s'agit nullement de remettre en question les efforts engagés, mais de les prolonger par une lecture actualisée des enjeux, enrichie de propositions stratégiques et d'un plaidoyer éclairé. L'ambition est de contribuer à renforcer la résilience du cyberspace sénégalais et d'alimenter, à l'échelle régionale et internationale, une réflexion collective sur la souveraineté numérique.

SOMMAIRE

PRÉFACE.....	8
AVANT-PROPOS.....	11
ANCRAGE DANS LES RÉFÉRENCES EXISTANTES ET PERSPECTIVES D'ÉVOLUTION.....	13
INTRODUCTION.....	18
I. ÉTAT DES LIEUX SÉNÉGAL	20
• A. Aperçu de l'état des lieux.....	21
1. Cadre juridique, réglementaire et institutionnel	
2. Cadre institutionnel de gouvernance cyber	
3. Politique nationale & évaluation stratégique	
4. Approche multipartite en évolution	
• B. Analyse critique du cadre cyber sénégalais.....	27
1. Points positifs	
2. Limites actuelles	
3. Réflexions sur la DCSSI : entre centralisme institutionnel et besoin de refondation organique	
II. LE CONTEXTE DES CYBER MENACES AU SÉNÉGAL	36
• A. Constat des menaces actuelles	37
1. Multiplication des fraudes en ligne et fuites de données	
2. Institutions publiques ciblées par des ransomwares	
3. Vulnérabilités des infrastructures critiques	
• B. Synthèse des principales cyberattaques (2018-2025).....	40
• C. Tableau chronologique.....	42

- D. Focus sur les fraudes et cyberattaques dans les services financiers.....43

III. PROPOSITION DE SOLUTIONS.....46

- A. Cadre de gouvernance.....47
 - 1.Haute Autorité de la Cybersécurité (HAC)48
 - 2.Commandement de Cyberdéfense : vers une 5^e Armée53
 - 3.Haute Autorité pour la Protection des Données (HAPDP)55
- B. Réforme du cadre juridique.....58
 - 1.Mise à jour de la Loi n°2008-11 sur la cybercriminalité
 - 2.Intégration de la souveraineté numérique et régulation GAFAM
 - 3.Création de tribunaux spécialisés
- C. Sensibilisation, formation et culture cybersécurité.....64
 - 1.Culture de cybersécurité durable
 - 2.Intégration dans les curricula scolaires
 - 3.Formation de professionnels qualifiés
- D. Attaques et parades.....68
 - 1.Typologie des menaces et stratégies de défense
 - 2.Réponse aux incidents et cyberrésilience

VI. PERSPECTIVES STRATÉGIQUES ET ENJEUX D'AVENIR.....75

- A. Technologies émergentes et perspectives stratégiques
 - 1.Intelligence Artificielle, Blockchain, IoT, 5G
 - 2.Ordinateur quantique et menaces pour le chiffrement
 - 3.Stratégie technologique souveraine81
- B. Le New Deal Technologique.....85
 - 1.Enjeux et perspectives stratégiques
 - 2.Cybersécurité du New Deal Technologique87
- C. Tribune : Réforme en profondeur de la CDP90

CONCLUSION	92
GLOSSAIRE DES TERMES CLÉS	101
ANNEXES	105
A. Enquête citoyenne sur le New Deal Technologique	105
B. Techniques de fraude numérique	108
REMERCIEMENTS	111
SOURCES ET BIBLIOGRAPHIE	126
PRÉSENTATION DE L'AUTEUR	130
RÉSUMÉ DU LIVRE BLANC	134

INTRODUCTION

Depuis plus d'une décennie, le Sénégal s'est engagé dans une dynamique irréversible de transformation numérique. La dématérialisation des services publics, l'émergence de l'e-gouvernement, l'adoption croissante des plateformes digitales par les citoyens, les entreprises et les institutions sont autant de signes d'un basculement vers une société de plus en plus interconnectée.

Mais cette modernisation, si elle est source d'opportunités, expose aussi le pays à des risques technologiques majeurs. La multiplication des cyberattaques, ciblant aussi bien les services de l'État, les banques, les plateformes éducatives, les télécoms ainsi que certaines cyberactivités, tout ceci reflète une certaine fragilité face aux cybermenaces.

Des épisodes récents de tensions socio-politiques, des vagues de désinformation coordonnées sur les réseaux sociaux, des cyberattaques par ransomware, ou encore des fuites massives de données sensibles viennent rappeler que le cyberspace sénégalais est devenu un véritable terrain de confrontation. À cela s'ajoute un contexte géopolitique particulier, marqué par la découverte de ressources naturelles stratégiques (pétrole, gaz) qui attisent les convoitises et posent de nouveaux enjeux de cybersécurité.

Par ailleurs, l'utilisation grandissante de technologies émergentes comme l'intelligence artificielle, l'IoT, ou encore la biométrie, sans une régulation adaptée ni une stratégie de souveraineté, ouvre la porte à de nouvelles formes d'espionnage, de perte ou de contrôle sur nos données nationales.

C'est dans cette dynamique que le *New Deal Technologique*, initié par l'État du Sénégal à travers le Ministère de la Communication, des Télécommunications et du Numérique, constitue une opportunité qui tombe à point nommé. La réussite de cette vision dépendra de la capacité de l'État, avec l'appui de l'ensemble des parties prenantes, à structurer de manière cohérente la gouvernance de la cybersécurité, à réformer notre arsenal juridique, à sensibiliser les citoyens, les entreprises et les agents publics aux bonnes pratiques en ligne (Cyberhygiène), et à soutenir un écosystème local capable d'innover et de protéger durablement notre *cyberspace*.

Ce livre blanc a pour ambition de dresser un aperçu de l'état des lieux de la cybersécurité au Sénégal, de documenter les cyberattaques marquantes, d'en analyser les failles, et surtout, de formuler des propositions concrètes, inclusives et audacieuses pour permettre au Sénégal de se positionner solidement sans perdre sa souveraineté numérique, dans un monde en pleine mutation.

I

ÉTAT DES LIEUX SENEGAL



A. Aperçu de l'état des lieux



1. Cybersécurité : une urgence mondiale, un défi africain

a. Un monde hyperconnecté, mais exposé

Aujourd'hui, notre monde tourne autour du numérique. Tout est connecté : nos vies personnelles, nos économies, nos administrations. Mais derrière cette avancée technologique se cache une réalité plus sombre : les attaques informatiques sont devenues des armes puissantes, capables de paralyser des pays entiers, de manipuler des élections, ou de faire fuiter des données sensibles. Les grandes puissances le savent, et elles investissent massivement pour se protéger.

Et l'Afrique dans tout ça ? Le continent progresse à grands pas dans sa transformation numérique. Mais cette montée en puissance s'accompagne de nouveaux risques. De nombreuses infrastructures sont encore mal protégées. Les cybercriminels, eux, n'attendent pas. Ils frappent déjà.

b. Le Sahel : quand l'insécurité rencontre le numérique

Dans les pays du Sahel, la situation est encore plus délicate. Ces territoires font face à de nombreuses tensions : conflits armés, terrorisme, instabilité politique, désinformation. Et désormais, une autre menace invisible vient s'ajouter : la cybermenace.

Des groupes malveillants utilisent les outils numériques pour manipuler l'opinion, diffuser de fausses informations, espionner des institutions ou saboter des infrastructures. L'intelligence artificielle, entre de mauvaises mains, peut même servir à créer des vidéos truquées (Deepfakes), amplifier la haine, ou déstabiliser un pays sans tirer une seule balle.

c. Mais tout n'est pas sombre : l'Afrique se réveille

Heureusement, l'Afrique n'est pas passive. Des conventions comme celle de Malabo ont été créées pour encadrer la cybersécurité et la protection des données. Certains pays prennent les devants, développent leurs lois, mettent en place des centres de réponse aux incidents, et forment des experts.

Mais le chemin est encore long. Beaucoup de pays manquent de ressources, de coordination ou simplement de volonté politique. Pourtant, face à ces menaces invisibles mais bien réelles, il devient vital d'agir ensemble.

Et dans cette dynamique, le Sénégal fait figure de modèle. Il s'est très tôt engagé sur ces sujets, et aujourd'hui, il inspire de nombreux autres pays.

2. Cadre juridique, réglementaire et institutionnel de la cybersécurité au Sénégal

a. Instruments juridiques internationaux ratifiés

Le Sénégal se distingue parmi les pays africains, surtout en Afrique de l'Ouest, par son engagement avancé en matière d'adhésion aux instruments internationaux relatifs à la lutte contre la cybercriminalité et à la protection des données personnelles. Il a, à ce titre, ratifié les conventions suivantes :

- La Convention de Budapest sur la cybercriminalité (adoptée le 23 novembre 2001) : le Sénégal a été le deuxième pays d'Afrique après l'Ile Maurice et le premier pays d'Afrique de l'Ouest à signer et ratifier cette convention historique.
- La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (plus connue sous le nom de "Convention 108") (adoptée à Strasbourg, le 28 janvier 1981) : premier traité international juridiquement contraignant en matière de protection des données personnelles, elle vise à garantir à toute personne le respect de ses droits fondamentaux, notamment sa vie privée, face au traitement automatisé de ses données.
- La Convention de Malabo du 27 juin 2014 (Union Africaine) sur la cybersécurité et la protection des données à caractère personnel : là encore, le Sénégal a joué un rôle pionnier en devenant le premier pays africain à ratifier ce texte.
- L'Acte additionnel A/SA.1/01/10 sur la protection des données à caractère personnel du 16 février 2010: ce texte harmonise les législations des États membres de la CEDEAO en matière de protection des données, en posant les principes de consentement, de sécurité et de droits des personnes concernées.
- La Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité adoptée en août 2011 : elle établit un cadre commun pour la prévention, la détection et la répression des infractions informatiques

au sein de la CEDEAO, tout en facilitant la coopération judiciaire régionale. En outre, elle complète l'Acte additionnel A/SA.1/01/10 sur la protection des données personnelles et s'inscrit dans une stratégie globale de cybersécurité pour l'espace ouest-africain.

b. Lois nationales encadrant le cyberspace

À travers ces Conventions, le Sénégal a adapté son arsenal juridique interne en adoptant plusieurs lois structurantes dont :

- La loi n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la société de l'information (LOSI) ;
- La loi n° 2008-08 du 25 janvier 2008 relative aux transactions électroniques ;
- La loi n°2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel ;
- La loi n°2008-11 de la même date, relative à la cybercriminalité et modifiée par la loi n°2016-29 du 08 novembre 2016 ;
- La loi n° 2008-09 sur le droit d'auteur et les droits voisins ;
- La loi n°2008-41 du 20 août 2008 portant sur la cryptologie;
- La loi n°2018-28 du 12 décembre 2018 portant Code des Communications électroniques ;
- Les dispositions spécifiques du Code pénal et du Code de procédure pénale notamment les innovations apportées par la loi n° 2016-29 du 08 novembre 2016 modifiant le Code pénal et par la loi n° 2016-30 de la même date modifiant le Code de procédure pénale.

Certes la réforme de 2016, notamment la loi n°2016-29 du 08 novembre 2016, vient renforcer le dispositif juridique initial,

principalement sur le plan répressif, mais sans intégrer de manière satisfaisante les nouvelles menaces, usages ou technologies nouvelles et à la cybersécurité en général.

3. Cadre institutionnel de gouvernance cyber

Le Sénégal s'est doté de plusieurs entités pour piloter ou accompagner la cybersécurité, avec des rôles souvent complémentaires.

Le tableau ci-dessous vous permettra de mieux comprendre tout le dispositif national :

STRUCTURE	RÔLE PRINCIPAL
CDP (Commission de protection des Données Personnelles)	Régulation de la collecte et du traitement des données
SENUM (ex-ADIE)	Déploiement des infrastructures numériques de l'État
ARTP	Régulation des télécommunications et cybersécurité des opérateurs
Division spéciale cybersécurité (Ministère de l'Intérieur)	Lutte contre la cybercriminalité à l'échelle nationale
Gendarmerie nationale (Section cybercrime)	Enquête numérique et lutte contre les infractions cybercriminelles
CADARCA	Coordination des activités de détection, d'alerte et de réponse aux cyberattaques
ENCVR (L'Ecole Nationale de Cybersécurité à Vocation Régionale)	Renforcer les capacités et les connaissances techniques en Cybersécurité des acteurs du public.
DCSSI (Direction générale du Chiffre et de la Sécurité des Systèmes d'Information)	Autorité Nationale de Cybersécurité

4. Politique nationale et évaluation stratégique

Le Sénégal s'est appuyé également sur plusieurs stratégies nationales et évaluations techniques pour renforcer sa résilience , à savoir :

- Le plan Sénégal Émergent PSE/PSE-AA (2035) - cadre général de développement qui remplace le PSE, sachant qu'une nouvelle vision 2050 a été lancée déjà par la nouvelle alternance ;
- La stratégie Nationale de Cybersécurité 2022 (SNC2022) : stratégie de cybersécurité du Sénégal ;
- La stratégie Nationale d'IA (SNIA): elle vise à positionner le Sénégal comme un acteur souverain, innovant et éthique dans le développement et l'usage de l'intelligence artificielle au service du développement économique et social ;
- La PSSI (Politique de Sécurité des Systèmes d'information) du Sénégal : cadre stratégique définissant les exigences, principes et mesures de sécurité applicables aux systèmes d'information publics, visant à renforcer la résilience numérique de l'État ;
- La stratégie Nationale des Données du Sénégal : Cette stratégie est basée notamment sur quatre principes fondamentaux qui sont la protection de la vie privée, la transparence et l'équité, et la sécurité. Cette stratégie à été validée ce 25 juillet 2023.

Et récemment en 2025, nous avons le New Deal Technologique: nouvelle feuille de route pour la transformation numérique et digitale remplaçant la Stratégie Sénégal numérique SN2025.

5. Une approche multipartite en évolution

Le processus de construction de la gouvernance cyber au Sénégal repose sur une approche multipartite, pilotée par le Ministère en charge du numérique, avec la contribution :

- Des autres ministères (défense, intérieur, justice, économie);
- Des acteurs privés (opérateurs, banques, startups) ;
- Des partenaires techniques et financière (banques de développement, agences internationales) ;
- Et de la société civile.

B. Analyse critique du cadre cyber sénégalais

1. Les points positifs : des fondations pionnières et un engagement réel

Le Sénégal s'est positionné très tôt comme leader en Afrique francophone sur les questions de cybersécurité et de protection des données.

Voici comment il s'est démarqué :

- A été le premier pays d'Afrique noire à ratifier la Convention de Budapest sur la cybercriminalité et la Convention de Malabo sur la cybersécurité ;
- A transposé intégralement la directive CEDEAO de 2011, montrant une réelle volonté d'harmonisation régionale ;
- A disposé d'un arsenal législatif complet, couvrant la majorité des grands domaines (cybercriminalité, protection des données, cryptologie, transactions électroniques) ;
- A créé des institutions et cadres de référence comme la Commission

de Protection des Données à caractère Personnelles (CDP), la Division cybersécurité du Ministère de l'Intérieur, ou encore le Cadre nationale de coordination des Activités de Détection, d'Alerte et de Réponse aux Cyberattaques (CADARCA⁵) qui amorce une logique de réponse coordonnée aux incidents ;

- A élaboré des stratégies telles que SNC20-22 ou SSN25-35 , le New Deal Technologique attestant d'une volonté d'ancrer la cybersécurité dans une vision globale de développement.

En résumé : les bases tangibles et viables sont posées. Le Sénégal semble avoir pris une longueur d'avance politique et institutionnelle par rapport à plusieurs pays de la sous-région.

2. Les limites actuelles : fragmentation, obsolescence et manque de coordination

Ces avancées notés plus haut se heurtent aujourd'hui à plusieurs freins structurels et opérationnels dont :

a. Un cadre juridique avec une évolution très lente

- Les principales lois datent de 2008 à 2011. Elles n'intègrent pas les nouvelles technologies émergentes comme :
 - l'intelligence artificielle ;
 - la biométrie à grande échelle ;
 - les plateformes de surveillance globale (OSINT, SIGINT) ;
 - la souveraineté des données (cloud, datacenters, GAFAM) ;
 - ou encore la désinformation algorithmique.

b. Une fragmentation des acteurs

- Trop d'institutions interviennent dans le domaine, sans qu'une véritable coordination centrale ne soit assurée :
 - La Commission de Protection des Données Personnelles ci-après CDP, en tant qu'autorité de régulation des données personnelles, dispose d'un véritable pouvoir réglementaire et de moyens de coercition, notamment la possibilité d'imposer des sanctions pécuniaires allant de 1 à 100 millions de francs CFA. Toutefois, elle ne perçoit pas directement les montants issus de ces sanctions. Par ailleurs, si l'on se réfère à sa jurisprudence, aucune sanction pécuniaire publiée n'a été prononcée depuis sa création en 2008.
 - En revanche, l'exigence de respecter plusieurs étapes préalables à toute sanction pécuniaire telles que la mise en demeure, l'avertissement, la procédure contradictoire ou encore le retrait d'autorisation, rend l'application effective de ces sanctions particulièrement difficile. Cela dit, on comprend que l'esprit de la loi visait avant tout à encourager la mise en conformité plutôt qu'à sanctionner systématiquement. C'est pourquoi, dans un contexte mondial actuel marqué par des violations de plus en plus graves et systématiques des données personnelles, une révision de cette approche s'impose. Certaines infractions justifieraient des mesures immédiates, efficaces et dissuasives telles que des sanctions pécuniaires substantielles.
 - Le Département du Chiffre et de la Sécurité des Systèmes d'Information, ci-après DCSSI bien qu'il conseille la Présidence de la République, reste trop enfermé dans cette mission institutionnelle, occultant trop souvent sa mission d'information et de sensibilisation auprès du grand public. Il est pourtant principalement concerné par la protection et la sécurité des données au même titre que la CDP. Il serait

- pertinent de mettre en place des cadres institutionnels dédiés afin de coordonner les actions et d'améliorer l'efficacité des interventions de chacune des entités. Par ailleurs, une approche structurée permettrait d'assurer une meilleure synergie entre les différentes entités impliquées.
 - La Coordination des activités de détection, d'alerte et de réponse aux cyberattaques, ci-après dénommée CADARCA, n'est pas encore pleinement opérationnelle comme CERT national.
- Le partage d'informations entre institutions est faible, voire inexistant et cela compromet l'efficacité du dispositif en place.

c. Un manque de moyens humains et techniques

- Les profils experts en cybersécurité sont rares dans l'administration, souvent mal rémunérés ou pas formés aux standards actuels.
- Les outils de veille, d'analyse de malware, de threat intelligence ou de cybersurveillance sont insuffisants voire absents.
- Peu d'investissements dans l'industrialisation de solutions souveraines (SIEM, firewall, cloud sécurisé...).

d. Une faible sensibilisation du public

- L'hygiène numérique est peu enseignée à l'école.
- Il n'y a pas encore de campagne nationale de prévention, ni de plateforme d'alerte grand public.
- Les citoyens restent les premières victimes d'arnaques, d'usurpation ou de fuite de données, "souvent sans recours".

e. Des enjeux numériques et de cybersécurité encore insuffisamment pris en compte

- Le cyberespionnage géostratégique : le contexte gazier, pétrolier et militaire demande une réponse cyberdéfense que peu d'institutions savent encore organiser.
- La cybersécurité des objets connectés (IoT) dans les transports, les hôpitaux, l'agriculture ou la surveillance urbaine.
- Les menaces dopées par l'IA (APT) : hameçonnage génératif, fausses vidéos politiques, attaques de type zero-day assistées par machine learning.
- La cybersécurité des systèmes électoraux : enjeu de confiance dans les élections et la démocratie numérique.
- La lutte contre le désinformation de masse et la manipulations politiques sur les réseaux sociaux : peu de mécanismes de détection rapide ou de réponse institutionnelle coordonnée.

3. Réflexions sur la DCSSI : entre centralisme institutionnel et besoin de refondation organique



La Direction du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI), logée au Palais de la République, se présente officiellement comme l'autorité nationale de cybersécurité au Sénégal. Historiquement héritée de l'appareil régalien de l'État chargé de protéger les échanges confidentiels entre hautes autorités, elle s'est vue confier des missions élargies de veille, de coordination et de pilotage stratégique du cyberspace national.

Important : Cette analyse a été rédigée dans un contexte de transition institutionnelle. Avec l'arrivée d'un nouveau directeur à la DCSSI, cette réflexion se veut avant tout constructive et prospective. L'objectif n'est pas de porter un jugement sur les orientations actuelles, mais bien d'identifier et de formaliser, le cas échéant, quelques pistes concrètes pour améliorer l'avenir de la cybersécurité du pays.

De nombreux experts du domaine, après les avoir consultés, pensent qu'il y a de nombreuses zones d'ombre qui entachent sa lisibilité, son efficacité et sa légitimité.

Voici les points d'achoppement qui ont été notés :

a. Une autorité logée au Palais : un symbole fort, mais un positionnement problématique

Le fait que la DCSSI soit rattachée physiquement et administrativement à la Présidence lui donne une dimension hautement stratégique. Mais ce placement ultra-centralisé a aussi créé une rupture de dialogue avec les acteurs du terrain, notamment :

- Les administrations techniques (santé, éducation, finances, collectivités) ;
- Les acteurs économiques (entreprises, banques, startups) ;
- Les experts civils (IT-consultant, chercheurs, formateurs, communautés techniques) ;

- Les citoyens eux-mêmes, premières victimes des menaces numériques.

L'absence d'un accès des locaux au public, d'une visibilité institutionnelle, de lignes de communication qui touche le grand public a donné à cette structure l'image d'un cercle fermé, réservé à des agents secrets, où la cybersécurité nationale serait gérée comme une affaire militaire d'exception, et non comme un bien public.

b. Une confusion persistante entre chiffrement étatique et cybersécurité collective

Initialement axée sur le chiffrement des données sensibles de l'État, la DCSSI a élargi ses attributions à la cybersécurité. Mais cette extension s'est faite sans changement d'approche et d'architecture fonctionnelle.

Or, le chiffrement et la cybersécurité sont deux domaines distincts :

- Le premier relève plus de la sécurité d'État, discret, cloisonné, strictement encadré.
- Le second est un écosystème vivant, dynamique, transversal, impliquant tous les pans de la société.

En concentrant la cybersécurité dans une structure de chiffrement étatique, le Sénégal s'est privé d'une vision holistique, participative et proactive de la gouvernance de son cyberspace.

c. Aucune initiative structurante ou action visible à l'échelle nationale

Malgré ses missions, la DCSSI ne publiait pratiquement aucun rapport, n'organisait aucun événement ouvert au grand public, en particulier aux communautés IT, n'émettait aucun référentiel de cybersécurité, et n'interagissait quasiment avec aucune autre autorité visible.

- Pas de communication pendant les vagues de cyberattaques contre des banques ou institutions ;
- Pas de coordination officielle avec les établissements universitaires, ni de soutien à la formation des jeunes ;
- Pas de stratégie publique de réponse aux menaces, de plateforme d'alerte ou de campagne de sensibilisation.

À l'heure où d'autres pays africains comme le Rwanda, la Côte d'Ivoire ou le Kenya ont lancé des agences cyber dynamiques, connectées et visibles, le Sénégal semble freiné par l'inertie d'une direction invisible, silencieuse, et perçue comme fantomatique.

d. Des limites structurelles face à la transformation numérique actuelle

Les défis actuels (cyber criminalité transnationale, espionnage industriel, désinformation, sécurité des objets connectés, IA malveillante...) nécessitent une réponse agile, visible, technique et territorialisée.

Or, la DCSSI ne dispose ni d'un CERT national opérationnel ouvert au public, ni de pôles régionaux, ni d'un programme de détection des vulnérabilités ou d'une transparence dans le processus de recrutement.

Elle reste enfermée dans un paradigme régalien étroit, à rebours des standards internationaux qui promeuvent la cybersécurité comme un bien commun, piloté par une autorité ouverte, technique, connectée à la société.

e. Proposition : Vers une Haute Autorité de la Cybersécurité (HAC)

Cette proposition ne vise pas à critiquer l'existant, mais à imaginer collectivement un modèle d'organisation adapté aux défis de demain.

L'objectif est de faire évoluer plutôt que de remplacer, en s'appuyant sur l'expertise acquise.

DCSSI (actuelle)	HAC (proposée)
Basée au Palais	Autorité autonome avec présence nationale
Orientée chiffrement et secret	Axée sur gouvernance, réponse, formation
Opacité fonctionnelle	Transparence et dialogue public
Fermée à l'écosystème civil	Interface entre État, secteur privé, citoyens
Silencieuse face aux crises	Actrice publique proactive et pédagogique
Non visible ni accessible	Site web dédié intégrant une plateforme de signalement, CERT

Une opportunité de refondation constructive

Avec l'arrivée du nouveau Directeur Général, la cybersécurité sénégalaise entre dans une nouvelle ère. Cette transition constitue une opportunité de repenser l'organisation institutionnelle afin de mieux répondre aux défis contemporains.

Cette réflexion se veut une contribution au débat sur l'avenir de notre sécurité numérique collective.

NB: Un peu plus bas, je vais revenir en détail sur comment je vois HAC.

II

LE CONTEXTE DES CYBER MENACES AU SÉNÉGAL



A. Constat

Au Sénégal, le numérique a profondément transformé notre manière de vivre, de travailler, de communiquer. En quelques années à peine, les technologies se sont immiscées dans notre quotidien, jusqu'à devenir le socle de nombreuses activités essentielles. Mais cette évolution rapide n'a pas été accompagnée du même élan en matière de cybersécurité.

Aujourd'hui, nous faisons face à une Cyberréalité inquiétante, que trop peu de gens mesurent à sa juste gravité.

1. Multiplication des cas d'usurpation d'identité, de fraudes en ligne et de fuites de données

Chaque jour, des citoyens sénégalais sont victimes de vols de comptes sur les réseaux sociaux, de fraudes sur les plateformes de mobile money, ou encore d'usurpation d'identité sur les réseaux sociaux. Des données personnelles circulent sans protection, parfois même issues d'institutions ou de services en ligne qui devraient garantir leur confidentialité. Les victimes sont souvent démunies, ne sachant ni quoi faire, ni vers qui se tourner. Ces cyberviolences laissent des traces profondes : perte de confiance, traumatisme, sentiment d'abandon et bien d'autres conséquences dévastatrices sur les victimes.

2. Institutions publiques ciblées par des ransomwares

Nos administrations, collectivités territoriales, établissements publics et même nos universités sont devenus les cibles de cybercriminels organisés (APT). Des attaques par ransomware ont paralysé des systèmes entiers, bloquant l'accès à des données cruciales. Ces attaques, souvent passées sous silence, fragilisent l'État dans sa capacité à rendre ses services, à assurer la continuité administrative et à protéger les informations sensibles des citoyens.

3. Vulnérabilités dans les infrastructures critiques (OIV)

Nos infrastructures critiques : hôpitaux, banques, réseaux de communication, système de distribution d'eau ou d'électricité sont connectées, mais vulnérables.

La moindre faille peut avoir des conséquences dramatiques : interruption de soins, pertes financières, chaos dans les services de base.

Malgré toutes les inquiétudes, très peu de ces Systèmes d'Information ne font pas l'objet d'audits réguliers ou ne bénéficient pas d'une cybersécurité réellement adaptée, alors même que le cyberrique est bien réel.

4. Faible sensibilisation généralisée à la cybersécurité

D'une manière générale, le citoyen sénégalais lambda n'est pas formé aux cyberrisques. Les gestes simples de protection sont souvent inconnus. Les enfants grandissent dans un environnement numérique sans repères sécuritaires. Les enseignants, les parents, les responsables publics ne sont pas suffisamment formés. Ce déficit de culture à la cybersécurité alimente l'insécurité en ligne et empêche toute cyberriposte coordonnée et efficace.

5. Nouveaux enjeux géostratégiques et militaire : pétrole, gaz et cyberespionnage

L'arrivée du pétrole et du gaz place le Sénégal dans une nouvelle ère géopolitique. Ces investissements et partenariats attirent des intérêts étatiques et privés étrangers qui, dans certains cas, peuvent recourir à l'espionnage industriel, au sabotage numérique ou à la manipulation de données. Il est donc impératif de sécuriser ces infrastructures critiques et de protéger les secrets industriels et économiques du pays.

Dans un Sahel déjà fragilisé par les menaces terroristes traditionnelles, le numérique vient bouleverser les dynamiques de conflit en introduisant de nouvelles formes de menaces : les cyberattaques.

6. Cyberattaques dans un contexte politique instable

Le climat politique sénégalais, parfois tendu, a donné lieu à des cyberattaques de nature politique perpétrées par un type de hackers spécifiques, catégorisés sous le nom de Hacktivistes, animés par diverses causes comme le cas d'**Anonymus**.

Des conséquences alarmantes sont notées: fuites d'informations confidentielles, piratage de comptes de personnalités publiques, campagnes de désinformation massives sur les réseaux sociaux, manipulation de vidéos ou d'images. Ces attaques fragilisent la démocratie, nourrissent la haine et menacent la stabilité nationale.

Un cri d'alarme... mais aussi un appel à l'action

Ce constat ne vise pas à faire peur. Il est un appel à la lucidité, à la responsabilité, et surtout à l'engagement collectif. Le Sénégal ne peut pas entrer dans sa nouvelle ère du numérique (New Deal Technologique) sans se doter d'une vision claire, ambitieuse et inclusive de la cybersécurité. C'est aussi le sens de ce livre blanc.

Nous ne devons plus attendre qu'une crise majeure se produise pour agir. Il est temps de passer de la prise de conscience à l'action structurée, de la réactivité à la proactivité.

Instabilités sahéliennes : un terreau fertile pour les cybermenaces et dérives de l'IA

Dans la région du Sahel, l'instabilité politique chronique, la présence de groupes armés non étatiques, les tensions sociales et la faiblesse des institutions rendent les États particulièrement vulnérables aux cybermenaces et aux dérives liées à l'intelligence artificielle. Des campagnes de désinformation coordonnées, alimentées par des

intelligences artificielles génératives, peuvent amplifier les divisions communautaires, semer le doute sur les processus électoraux ou encore alimenter des narratifs extrémistes. Dans un tel contexte, l'absence de régulation des technologies numériques devient un véritable risque pour la sécurité nationale, la souveraineté technologique et la cohésion sociale des pays sahéliens. Il est donc urgent de penser une stratégie régionale résiliente et mutualisée pour encadrer l'usage de l'IA et renforcer la cybersécurité face aux menaces hybrides.

B. Synthèse des principales cyberattaques au Sénégal (2018 - 2025)

Voici une synthèse complète des cyberattaques recensées au Sénégal depuis 2018 jusqu'en 2025, incluant les contextes politiques sensibles comme les tensions socio-politiques, la découverte du pétrole et du gaz, et les prises de parole de figures politiques telles que l'actuel Premier ministre Ousmane Sonko ou le député Guy Marius Sagna.



- **Mars 2018** : Tentative d'intrusion dans le système informatique d'une institution bancaire sénégalaise

Cible : Grande banque locale

Type : Intrusion dans les systèmes bancaires

Acteurs : Cybercriminels ouest-africains (réseaux transnationaux)

Conséquence : Arrestation de plusieurs individus impliqués

- **Octobre 2022** : Fuite massive de données dans une agence de régulation

Cible : Autorité publique de régulation du secteur numérique

Type : Exfiltration de données sensibles (plus de 100 Go)

Acteurs : Groupe structuré utilisant des méthodes de rançongiciel

Réaction : Refus de négociation, publication des données sur le Dark Web

- **Mai 2023** : Attaque coordonnée contre des portails institutionnels

Cibles : Plusieurs ministères et sites stratégiques de l'État

Type : Dénégation de service distribué (DDoS)

Acteurs : Collectif revendiquant une motivation politique

Motif déclaré : Contestation du régime en place

- **Décembre 2024** : Compromission grave d'une banque nationale de logement

Cible : Institution bancaire spécialisée dans le logement

Type : Ransomware avec vol massif de données

Perte estimée : Environ 500 000 dossiers de clients affectés

Rançon : Exigence de plusieurs centaines de milliers de dollars

Impact : Blocage temporaire des services numériques bancaires

- **Décembre 2024** : Interpellation politique sur la cybersécurité nationale

Contexte : Multiplication des incidents sur les portails publics

Réaction : Déclarations officielles à l'Assemblée nationale

Message : Appel urgent à la mise en place d'un cadre de cybersécurité robuste

- **Janvier 2025** : Série d'attaques sur des structures gouvernementales

Cibles : Institutions publiques diverses

Nature : Vols de données sensibles et interruptions de services

Réaction : Interpellation gouvernementale par des représentants élus

NB: J'ai veillé à anonymiser et pseudonymiser l'ensemble des données et informations partagées

C. Tableau chronologique de quelques principales cyberattaques au Sénégal (2018–2025) : attaques, impacts et mesures de réponse

Date	Cible (anonymisée)	Type d'attaque	Impact / Réaction
Mars 2018	Banque A (institution bancaire locale)	Intrusion bancaire	Arrestation de plusieurs cybercriminels ouest-africains
Octobre 2022	Autorité B (régulation des télécoms)	Exfiltration de données, rançongiciel (≈102 Go)	Refus de rançon, données publiées sur le Dark Web
Mai 2023	Ministères A, B, C, D	DDoS coordonné	Sites inaccessibles, revendication politique
Décembre 2024	Banque B (secteur logement)	Ransomware / Vol de données (≈500 000 dossiers)	Blocage des services numériques, rançon exigée, crise de confiance temporaire

Décembre 2024	Institution centrales	Intrusions multiples	Débat parlementaire sur la cybersécurité, interpellation officielle
Janvier 2025	Diverses structures étatiques	Fuites de données, interruptions de services	Renforcement en urgence des capacités cyber au niveau gouvernemental

Légende :

- Banque A / Banque B → institutions financières différentes
- Ministères A-D → secteurs tels que la défense, l'environnement, les infrastructures, etc.
- Autorité B → organismes de régulation numérique

NB: J'ai veillé à anonymiser et pseudonymiser l'ensemble des données et informations partagées

D. Le Phénomène de fraudes et cyberattaques dans les services financiers

La digitalisation rapide des services financiers (**Mobile Money, banques en ligne, fintechs**) a ouvert de nouvelles opportunités d'inclusion, mais aussi de vulnérabilités.

Ces dernières années, le Sénégal a connu une multiplication d'arnaques, de fraudes et d'attaques ciblant directement les citoyens et les institutions financières.

1. Les causes principales

- Faible sensibilisation des utilisateurs aux bonnes pratiques numériques ;
- Sécurisation inégale des plateformes et absence d'authentification forte ;
- Multiplicité d'acteurs sans coordination claire (banques, opérateurs, fintechs) ;
- Évolution rapide des techniques de fraude : SIM swap, phishing, usurpation d'identité, fausses apps de prêt ;
- Cadre réglementaire encore en retard par rapport aux pratiques numériques.

2. Conséquences observées

- Pertes financières parfois massives pour des particuliers ;
- Perte de confiance dans les services numériques ;
- Menaces systémiques sur certaines institutions (banques, opérateurs) ;
- Ralentissement de l'inclusion financière dans les zones rurales.

3. Pistes de réponse

- Éduquer massivement les usagers (campagnes ciblées, éducation numérique) ;
- Renforcer la sécurité des plateformes (MFA, chiffrement, monitoring) ;
- Clarifier les responsabilités en cas de fraude ;
- Harmoniser les normes entre acteurs du secteur ;
- Créer un Plan Directeur Cyber (PDC-ISS) pour structurer l'action globale ;
- Coopération régionale renforcée pour l'échange d'alertes et d'expertise.

La lutte contre Fraudes et cyberattaques dans les services financiers est une bataille pour tous, surtout les États qui sont les premiers concernés.

Sans sécurité, il n'y a pas d'inclusion durable.

Et sans inclusion, il n'y a pas de transformation numérique équitable et ordonnée.

III

PROPOSITION DE SOLUTIONS



A. Cadre de gouvernance

Face à l'évolution fulgurante du cyberspace et à la complexification croissante des cybermenaces, le Sénégal est confronté à un double impératif : garantir la sécurité de ses infrastructures critiques et préserver sa souveraineté numérique dans un environnement interconnecté et géostratégiquement⁷ sensible.

L'expérience internationale montre que les États qui ont su anticiper ces enjeux ont renforcé leur résilience et affirmé leur souveraineté. L'exemple marquant de l'Estonie, frappée en 2007 par une cyberattaque massive paralysant ses institutions financières, administratives et médiatiques, a constitué un tournant historique : cette crise a incité de nombreux pays à travers le monde à revoir leurs architectures institutionnelles et juridiques, en intégrant la cybersécurité comme un pilier fondamental de leur défense nationale.

Prenons l'exemple de la France qui, à la suite des cyberévénements majeurs comme ceux survenus en Estonie en 2007, a progressivement élevé la cybersécurité au rang de priorité stratégique nationale. Sans réviser formellement sa Constitution, la France traite désormais la protection du cyberspace avec la même rigueur que la défense du territoire physique. Cette prise de conscience s'est traduite par l'adoption de politiques publiques ambitieuses, de stratégies nationales dédiées, par un renforcement du cadre législatif pour anticiper, détecter et répondre efficacement aux menaces numériques et par la naissance de l'ANSSI⁸.

Dans ce contexte global, le Sénégal ne peut rester en marge. L'émergence de nouvelles menaces ou de cas de cybercriminalité transnationale, de cyberespionnage, de cybermanipulation, de sabotage d'infrastructures critiques exige une réforme structurelle ambitieuse de son écosystème de gouvernance cyber.

C'est pourquoi dans ce Livre Blanc, il est proposé la création de trois entités stratégiques, dotées chacune d'un mandat clair, d'une autorité

⁷Définition de géostratégiquement : <https://fr.opentran.net/creole-haiti/g%C3%A9ostrat%C3%A9giement.html>

⁸Agence nationale de la sécurité des systèmes d'information (ANSSI), Stratégie nationale pour la cybersécurité, République française, 2021, disponible sur : <https://www.ssi.gouv.fr/>, consulté le 15 mai 2025.

institutionnelle affirmée et d'une expertise ciblée. Ces instances visent à bâtir une gouvernance intégrée, agile et moderne, à la hauteur des défis contemporains, en assurant la sécurité, la résilience et la souveraineté du cyberspace sénégalais non seulement pour aujourd'hui, mais pour les générations futures.

1. Mise en place d'une Haute Autorité de la Cybersécurité (HAC)



a. Positionnement Institutionnel

Sous l'autorité directe du Premier Ministre, la Haute Autorité de la Cybersécurité (HAC) devra collaborer fonctionnellement avec plusieurs entités stratégiques de l'État, notamment :

- **Ministère de la Communication, des Télécommunications et de l'Économie Numérique;**
- **Société Sénégal Numérique (SENUM S.A.);**
- **Ministère des Finances et du Budget;**
- **Ministère de la Justice;**
- **Ministère de l'Intérieur;**
- **Ministère des Forces Armées;**
- **Ministère de l'Industrie et du Commerce.**

b. Pourquoi ce choix ?

- Assurer une gouvernance civile, ouverte et transparente
 - Pour ne pas répéter le schéma ultra-fermé de la DCSSI
- Garantir une coopération étroite avec les forces de sécurité
 - Police, gendarmerie et armée restent les piliers de la défense du territoire intérieur comme extérieur. Mais aujourd'hui, les menaces ne sont plus uniquement physiques, elles sont aussi numériques donc invisibles et transfrontalières.
- Ancrer la HAC dans une logique multipartite
 - État, privé, société civile, experts, tous autour de la table
Justification : Face à la recrudescence des cyberattaques ciblant les institutions stratégiques du pays, le positionnement de la HAC sera sous la haute autorité du premier ministre (la primature) et devra assurer une coordination transversale et une réactivité au plus haut niveau.

c. Missions

- Surveiller et analyser les menaces cybernétiques nationales et internationales;
- Élaborer la stratégie nationale de cybersécurité et en assurer le suivi;
- Assister les institutions publiques et privées dans la sécurisation de leurs infrastructures numériques;
- Coordonner les actions en matière de gestion des incidents majeurs;
- Promouvoir la culture de la cybersécurité par la sensibilisation, la formation, et la simulation d'incidents;
- Représenter le Sénégal dans les instances internationales de cybersécurité;
- Accompagnement et suivi des victimes pour renforcer la vulgarisation de la cybernétique à l'échelle citoyenne.

e. Fonctionnement de la HAC

- **Gouvernance Interne**

La HAC sera dirigée par un Directeur Général assisté d'un DGA et d'un Conseil Consultatif Pluridisciplinaire.

- **Ressources Humaines**

Recrutement d'experts certifiés, de cyberjuristes, d'analystes SOC, de formateurs cyber, d'ingénieurs, entre autres.

- **Infrastructures & Moyens Techniques**

Utilisation de datacenters souverains, SOC national, outils SIEM, cyber range, CERT national, laboratoires forensiques, entre autres.

Collaboration & Écosystème

Collaboration avec les CERT privés - Africain et Mondial tout à ayant son propre CERT national, FAI, banques, universités, ONG, et partenaires internationaux (AFRICERT, ITU, INTERPOL, entre autres).

- **Pilotage Stratégique**

Mise en œuvre du Plan National de Cybersécurité, sensibilisation, cyber drills, et reporting annuel.

- **Cadre Réglementaire**

Appui à l'élaboration d'un code de la cybersécurité, de normes et de protocoles de coopération.

- **Indicateurs de Performance**

- Nombre d'incidents résolus
- Taux de conformité des institutions
- Participation à des exercices Cyber
- Taux de sensibilisation et satisfaction

f. Collaboration Stratégiques Prioritaires

- **Ministère de la Communication, des Télécommunications et de l'Économie Numérique**

Ce ministère constitue un partenaire stratégique de premier plan, car il pilote la transformation digitale nationale. Son rôle aux côtés de la HAC inclura :

- La co-construction des politiques publiques numériques sécurisées
- L'intégration de la cybersécurité dans tous les programmes de digitalisation gouvernementale
- La sensibilisation des citoyens et entreprises à la sécurité numérique

- **SENUM S.A. – Société Sénégal Numérique**

SENUM apportera un soutien technique essentiel à la HAC :

- Hébergement et sécurisation des systèmes critiques via les datacenters souverains
- Appui technique pour les SOC, outils de supervision et cloud souverain
- Résilience des infrastructures numériques de l'État

- **Ministère des Finances et du Budget**

La cybersécurité implique des ressources financières importantes. Ce ministère garantira un financement prioritaire et intégré dans les lois de finances.

- **Ministère de la Justice**

Création d'un Pôle de Lutte contre la Cybercriminalité permettant la spécialisation des magistrats, une meilleure coordination et une jurisprudence adaptée.

- **Ministère de l'Intérieur**

Renforcement de la Division Spéciale Cybercriminalité de la Police Nationale avec des compétences en investigation numérique, veille et forensique.

- **Ministère des Forces Armées**

Gendarmerie et 5^e Armée joueront un rôle central dans la lutte contre la cybercriminalité, à travers des unités spécialisées et la veille stratégique.

- **Ministère de l'Industrie et du Commerce**

Ce ministère protégera les activités économiques numériques (PME, fintech, marketplaces) en intégrant la cybersécurité dans les régulations.

g. Création d'un Pôle national de coordination des forces de lutte contre la cybercriminalité

Dans une perspective de renforcement de l'efficacité de la réponse nationale aux menaces cyber, il apparaît stratégique de **mutualiser les efforts de la Division Spéciale de Lutte contre la Cybercriminalité (DSC) de la Police nationale** et de la **Plateforme de Lutte contre la Cybercriminalité (PLCC) de la Gendarmerie nationale**. Ces deux entités jouent un rôle essentiel dans la prévention, la détection et la répression des infractions liées aux technologies de l'information.

La création d'un **Pôle national de coordination des forces de lutte contre la cybercriminalité**, placé sous la tutelle de la Haute Autorité de Cybersécurité (HAC), permettrait :

- Une meilleure **synergie opérationnelle** entre les deux forces, évitant les doublons et facilitant le partage d'informations en temps réel ;
- La centralisation des ressources techniques et la mutualisation des outils d'investigation numérique ;
- La **création d'un cadre d'échange structuré** entre la police, la gendarmerie, les services judiciaires, les opérateurs de télécommunications et les entités de régulation ;

- L'élaboration d'un **cadre d'intervention harmonisé** dans les situations de crise cyber ou les enquêtes transfrontalières.

Ce pôle pourrait également être un levier pour la **coopération internationale** (INTERPOL, AFRIPOL, ENISA, entre autres.), facilitant les échanges d'informations avec les partenaires étrangers.

Enfin, ce dispositif renforcerait la **cohérence stratégique et la souveraineté numérique** du pays face à l'ampleur croissante des menaces cybernétiques.

2. Le Commandement de Cyberdéfense : vers une 5^e Armée Sénégalaise



Face à la militarisation croissante du cyberspace et aux menaces hybrides, il devient impératif pour le Sénégal de structurer sa cyberdéfense non plus comme une simple autorité civile, mais comme une force armée à part entière.

a. Positionnement institutionnel

- Le Commandement de la Cyberdéfense sera institué comme la cinquième composante des Forces Armées sénégalaises, aux côtés de :

- L'Armée de Terre,
 - La Marine,
 - L'Armée de l'Air,
 - Et de la Gendarmerie nationale.
- Il sera rattaché au Ministère des Forces Armées, avec l'appui stratégique du Haut Commandement et un lien de coordination avec la Présidence.

b. Missions principales

- Détection, anticipation et neutralisation des cybermenaces d'origine étatique ou criminelle (Cyberguerre).
- Contre-cyberespionnage, y compris dans les zones stratégiques : hydrocarbures, diplomatie, infrastructures critiques.
- Protection des systèmes d'information de défense, y compris les satellites, drones, systèmes de commandement.
- Capacité offensive dans le cadre de la doctrine de légitime défense numérique.
- Formation et équipement d'unités cyber spécialisées (opérateurs, analystes, ingénieurs).

c. Structure interne

- Centre d'opérations cyber (Cyber-CO) : pilotage des missions.
- Unité de cyber-renseignement (SIGINT / OSINT).
- Unité de cyberguerre.
- Académie militaire de cyberdéfense (en partenariat avec l'École de Guerre, la DCSSI, ENCVR et des ITSCHOOL).
- Branche de réponse rapide (Gaindé Cyber Riposte).

d. Dimension régionale

Le Sénégal, fort de sa stabilité et de son avance diplomatique, peut devenir un pôle régional de cyberdéfense en Afrique de l'Ouest, en coopération avec :

- Le G5 Sahel,
- La CEDEAO,
- Et les partenaires stratégiques internationaux (France, États-Unis, OTAN).

e. Pourquoi une telle évolution est nécessaire ?

- Parce que la cybersécurité militaire ne peut plus être externalisée ou marginalisée.
- Parce que les conflits modernes (Ukraine, Israël, Sahel) se jouent aussi dans le cyberspace.
- Et surtout parce que le Sénégal doit protéger ses intérêts vitaux numériques (hydrocarbures, diplomatie, finances, santé, gouvernance...).

3. Haute Autorité pour la Protection des Données Personnelles (HAPDP)



a. Missions clés

- Protéger les citoyens contre les abus, les dérives ou la surveillance massive.
- Auditer, sanctionner et encadrer tous les acteurs traitant des données personnelles.
- Accompagner la mise en conformité (référentiels, formations, conseils).
- Veiller à la souveraineté numérique dans les traitements publics ou sensibles (biométrie, cloud, IA, etc.).
- Sensibiliser la population à ses droits numériques dans toutes les langues locales.

b. Organisation

- Indépendance constitutionnelle, placée sous le contrôle direct de l'Assemblée Nationale.
- Présidence indépendante, nommée après audition publique pour compétence, neutralité et intégrité.
- Budget voté par le Parlement, avec une autonomie de gestion.

c. Pouvoirs

- Pouvoir de sanction financière directe, avec encaissement autonome des amendes au profit de son propre budget.
- Droit de saisine d'office : elle peut s'auto-saisir de toute situation touchant à la protection des données (public, privé, ou secteur informel).

- Pouvoir d'injonction auprès des ministères, entreprises, collectivités ou plateformes numériques.

d. Conseil Consultatif Pluridisciplinaire

- Regroupe des experts en droit, cybersécurité, technologies, société civile, secteur privé.
- Joue un rôle de veille stratégique et d'orientation prospective.

e. Autres axes de réformes et recommandations

- Adoption rapide de la réforme de la loi de 2008 sur la protection des données.
- Création de garanties pour les données sensibles (santé, biométrie, enfants).
- Autonomie dans les nominations, dans l'élaboration de son budget et dans ses missions de contrôle.
- Obligation de notification en cas de violation de données.
- Généralisation des campagnes de sensibilisation à la culture numérique.

B. Réforme du cadre juridique



Le cadre législatif sénégalais est aujourd'hui inadapté pour répondre aux réalités numériques actuelles. En effet, le droit est un pilier essentiel de la cybersécurité nationale. Afin de répondre à l'évolution rapide des cybermenaces et des usages technologiques, le Sénégal doit impérativement actualiser et renforcer son cadre juridique.

Pour ce faire, nous formulons les propositions ci-après :

1. Mise à jour de la Loi n°2008-11 sur la cybercriminalité

Adoptée il y a plus de 15 ans, cette loi n'est plus d'actualité en raison de la complexité et de la technicité des nouvelles menaces. Il faut une révision complète et elle devra intégrer entre autres :

- Les nouveaux types de cybercrimes (ransomware, deepfakes, usurpation d'identité, escroqueries basées sur l'IA, etc.).
- L'encadrement du cloud computing, de la blockchain et des cryptoactifs.

- La clarification des compétences territoriales pour les infractions transfrontalières.
- Le renforcement des sanctions et des procédures de cyber-enquête.

2. Évolution nécessaire de la LOSI ou création d'une loi d'orientation dédiée à la cybersécurité

À l'heure où les enjeux numériques deviennent de plus en plus stratégiques, il apparaît nécessaire de **réinterroger le cadre législatif structurant la société de l'information** au Sénégal. La **Loi d'Orientation sur la Société de l'Information (LOSI)**, bien qu'utile à sa création, mérite aujourd'hui une **mise à jour en profondeur** pour mieux prendre en compte les **nouveaux défis liés à la cybersécurité, à la souveraineté numérique et à la résilience des systèmes d'information.**

Deux pistes peuvent être envisagées :

- Une **révision de la LOSI**, pour y intégrer des dispositions claires sur la cybersécurité, la protection des infrastructures critiques, la régulation des technologies émergentes et les droits numériques ;
- Ou, à défaut, l'adoption d'une loi d'orientation spécifique à la cybersécurité, qui viendrait établir les grands principes encadrant la sécurité du cyberspace national.

Une telle évolution législative permettrait :

- De poser une **vision stratégique partagée** sur la sécurité numérique ;
- De clarifier les rôles et responsabilités des différents acteurs (État, secteur privé, forces de défense, société civile) ;

- De garantir une meilleure **cohérence entre les textes existants** (protection des données, cybercriminalité, télécommunications) et les évolutions technologiques en cours (IA, cloud, blockchain, entre autres.).

3. Intégration d'un cadre légal pour la souveraineté numérique, l'open data et la régulation des plateformes en ligne (GAFAM), (BATX⁹-HUAWEI) et BIG TECH DE L'IA

Pour préserver les intérêts stratégiques du pays dans le cyberspace, il faut nécessairement :

- Une souveraineté des données : obligation d'hébergement local ou régional des données sensibles ; définition de ce qui constitue des données d'intérêt national.
- Un Open data sécurisé : créer un cadre pour l'ouverture des données publiques tout en garantissant la confidentialité, l'intégrité et la traçabilité.
- Un encadrement des GAFAM et des BATX - Huawei: avec une obligation de transparence sur les algorithmes utilisés, une fiscalité numérique bien maîtrisée, le respect de la vie privée des citoyens, la lutte contre les contenus illicites et la manipulation de l'information.
- Et une régulation des Big Tech de l'IA : avec un cadre éthique et légal strict, une transparence sur les modèles d'IA utilisés, une évaluation des risques liés aux biais algorithmiques, la protection des droits fondamentaux et un contrôle accru de l'impact sociétal de l'IA sur les citoyens.

4. Création de pôles judiciaires spécialisés aux niveaux des tribunaux de Grande Instance

Face à la technicité des infractions numériques, il est crucial d'avoir :

- Des juridictions spécialisées dotées de magistrats formés en cyberdroit.
- Une procédure accélérée pour les infractions numériques complexes (cyberextorsion, atteintes aux systèmes critiques, harcèlement en ligne, etc.).
- Des experts judiciaires accrédités pour appuyer les enquêtes et procès.

5. Intégration de la cyberdéfense dans le Code pénal et le Code de justice militaire

L'approche de la cybersécurité ne peut ignorer la dimension géostratégique. Ainsi :

- Le Code pénal doit reconnaître les actes de cyberespionnage, cybersabotage, cyberguerre comme des crimes contre la sécurité nationale.
- Le Code de justice militaire doit intégrer des articles spécifiques à la cyberdéfense, au cyberrenseignement, et à la cyber riposte en cas d'attaque contre des infrastructures vitales (OIV).
- La coopération entre les forces armées, les agences civiles et les autorités judiciaires doit être formalisée et encadrée.

6. Intégration de la cybersécurité et de la cyberdéfense dans les écoles de formation régaliennes

Dans un contexte marqué par la montée des menaces numériques, la formation des acteurs de la sécurité et de la justice ne peut faire l'impasse sur les enjeux liés à la cybersécurité. Il est essentiel que les futurs policiers et magistrats soient préparés à faire face aux défis juridiques, techniques et stratégiques posés par le cyberespace.

a. Pour l'École Nationale de Police : Cybersécurité et cyberdéfense appliquées

Objectif : Permettre aux futurs policiers de comprendre les réalités du cyberespace surtout les cybermenaces.

Contenu proposé :

- **Introduction aux menaces cyber :** phishing, rançongiciels, cybercriminalité organisée, usurpation d'identité, etc.
- **Sensibilisation à la cyberdéfense :** notions de cyberintelligence, riposte, prévention, coordination interservices.
- **Notions juridiques de base :** infractions numériques, cadre légal national et international, procédures de collecte de preuves numériques.
- **Coopération interinstitutionnelle :** articulation entre services de police, autorités judiciaires et organes de cybersécurité nationale.

Bénéfice attendu : Préparer des agents capables de comprendre et prévenir efficacement les menaces cyber.

b. Pour l'École Nationale de la Magistrature : Introduction à la cybersécurité pour magistrats

Objectif : Donner aux futurs magistrats les clés de lecture juridique et stratégique pour statuer sur des affaires numériques.

Contenu proposé :

- **Éveil aux enjeux de souveraineté numérique :** rôle du juge face à des attaques ciblant les intérêts nationaux.
- **Cadre juridique de la cybercriminalité :** lois applicables, compétences territoriales, coopération judiciaire internationale.
- **Compréhension de la preuve numérique :** validité, traçabilité, intégrité et confidentialité.
- **Cas pratiques :** analyses de jurisprudences cyber, simulations de traitement d'affaires numériques complexes.
- **Cybersécurité des systèmes judiciaires :** sensibilisation à la protection des données et des infrastructures critiques.

Bénéfice attendu : Former des magistrats capables d'appréhender les nouvelles formes de criminalité numérique, de mieux encadrer les procédures, et de juger avec pertinence et efficacité dans un contexte de transformation digitale de la société.

C. Sensibilisation, Formation et Promotion d'une Culture de Cybersécurité Durable



1. Sensibilisation générale et ciblée de la population

La cybersécurité est l'affaire de tous. Il est fondamental de sensibiliser l'ensemble de la population sénégalaise, quel que soit l'âge, le niveau d'éducation ou la profession.

Mesures proposées :

- Campagnes de sensibilisation nationales via radio, télé, réseaux sociaux, en langues locales et en français.
- Vulgarisation des concepts clés de la cybersécurité : mots de passe, liens suspects, arnaques, Wi-Fi public, fake news entre autres.
- Focus particulier sur la sécurité des objets connectés (IoT), de plus en plus présents dans les foyers : caméras, enceintes connectées, électroménagers, etc.

- **Recommandations simples : changer les mots de passe par défaut, mettre à jour régulièrement, ne pas tout connecter au même réseau.**
- Sensibilisation des parents, enseignants, éducateurs et leaders communautaires :
 - Organisation d'ateliers dans les écoles, centres culturels, collectivités.
 - Capsules vidéos, supports imprimés, webinaires.
 - Partenariat avec les médias pour diffuser les bonnes pratiques.

2. Intégration de la cyberhygiène et de la cybersécurité dans les curricula scolaires

Dès l'école primaire, il est essentiel d'introduire des notions simples mais fondamentales telles que :

- Les bons réflexes face aux contenus en ligne et aux messages douteux.
- La gestion sécurisée des mots de passe et la protection des données personnelles.
- L'usage responsable des smartphones, tablettes et autres terminaux connectés.
- Les premiers repères face à la désinformation (fake news) et aux risques liés aux réseaux sociaux.

Au collège et au lycée, les contenus doivent évoluer vers :

- La compréhension de la sécurité des systèmes d'information.

- L'identification des cyber menaces courantes (phishing, ransomware, spyware...).
- Les cyber droits et la e-reputation responsable.
- Une introduction à la cybersécurité des objets connectés (IoT), en expliquant leur fonctionnement, les risques liés à leur utilisation (surveillance, intrusion, piratage), et les moyens de s'en protéger.

3. Création de clubs de détection de talents et accompagnement des vocations

a. Création de clubs scolaires de cybersécurité

Implantés dans les collèges, lycées et universités, ces clubs auront pour missions de :

- Susciter l'intérêt pour les métiers du numérique et de la cybersécurité.
- Organiser des concours, des jeux pédagogiques, des simulations d'attaques/défenses.
- Identifier les jeunes à fort potentiel et les orienter vers des programmes de mentorat, de bourses ou d'incubation.

b. Soutien aux initiatives communautaires et événements tech

- CTF (Capture The Flag) : compétitions de hacking éthique.
- Hackathons : résolutions collaboratives de défis technologiques.
- Bootcamps : formations intensives sur des thématiques précises (pentesting, forensique, SOC...).

L'État devra fournir un soutien logistique, financier et technique, notamment en mettant à disposition des experts et des infrastructures

4. Déploiement d'une plateforme éducative numérique sécurisée

Proposition de création d'une plateforme nationale de sensibilisation coordonné par ENCVR (Ecole Nationale de Cybersécurité à Vocation Régionale) :

- Cours interactifs sur le cyber hygiène et la cybersécurité.
- Espaces ludiques de simulation (phishing, attaques, protections...).
- Ressources pour tous les niveaux (élèves, enseignants, parents).
- CyberRange (Plateforme de simulation de cyberattaques).
- Suivi des progrès, badges et certifications numériques.

NB: “Nu Jang Informatique” a déjà créé et mis en place une plateforme e-learning made in Sénégal, elle pourra être utile à la cause¹¹

5. Journée ou Mois Nationale de la Cybersécurité

Institution d'une Semaine Nationale ou d'un Mois de la Cybersécurité, chaque année dans tout le pays :

- Forums, ateliers, conférences, concours dans toutes les régions.
- Activités dans les écoles, collectivités, entreprises, zones rurales.
- Partenariats avec les secteurs public, privé, académique et communautaire.

¹¹ Nu Jang Informatique, Site officiel, en ligne, disponible sur : <https://nujanginformatique.com> ou <https://nujanginformatique.sn>, consulté le 01 Février 2025.
Nu Jang E-Learning, Plateforme de formation en ligne, en ligne, disponible sur : <https://www.nujang.com>, consulté le 01 Février 2025.

- Valorisation des compétences locales, des innovations et des bonnes pratiques.

NB: Depuis bientôt 5 ans, la communauté rootSN célèbre chaque mois un concept nommé : **l'Octobre Cyber by Community rootSN¹²**, qui est une initiative citoyenne engagée dans le cadre du Mois Internationale de la Cybersécurité.

6. Former en masse des professionnels qualifiés en cybersécurité

Le Sénégal doit structurer un réservoir national de compétences techniques et juridiques, capable de répondre à la demande croissante en cybersécurité :

- Intégrer des programmes de cybersécurité dans les écoles supérieures et universités (ingénierie, droit, gestion...).
- Développer des filières professionnalisantes en alternance.
- Nouer des partenariats pour certifier les compétences (CEH, CISSP, ISO 27001, etc.).
- Créer des instituts spécialisés dans les métiers du cyberspace : gouvernance, pentesting, forensic, sécurité cloud, etc.

D. Attaques et Parades : comprendre les menaces pour mieux se défendre

Alors que le Sénégal s'engage dans une transition numérique ambitieuse à savoir le New Deal Technologique, les cyber menaces deviennent plus sophistiquées, fréquentes et ciblées. Cette section vise à identifier les types d'attaques les plus dévastatrices, leurs

vecteurs d'intrusion, et tenter de proposer des parades techniques et organisationnelles adaptées au contexte sénégalais.

1. Typologie des attaques les plus répandues

Type d'attaque	Exemples concrets	Vecteurs d'intrusion	Parades proposées
Phishing / Spear phishing	Campagnes de faux mails à certaines structures étatiques, bancaires et entreprises.	Email, SMS, liens malveillants, WhatsApp	-MFA -Sensibilisation utilisateurs -Filtrage DNS / anti-spam
Ransomware	Cas de banques et universités en 2023-2024	Pièces jointes infectées Accès RDP mal sécurisé	-Sauvegarde régulière -Segmentation réseau -Surveillance SOC
DDoS (déni de service)	Sites institutionnels lors des tensions politiques	Bots / botnets, requêtes massives	-CDN / WAF -Filtrage IP -Services de mitigation DDoS

Fuite de données	Données d'étudiants, fichiers RH divulgués	Vol de compte admin, mauvaise configuration cloud	-Chiffrement -IAM rigoureux -Audit régulier
Deepfake / désinformation	Faux discours de figures publiques (2021)	Réseaux sociaux, groupes WhatsApp, TikTok	-Cellule OSINT nationale -Fact-checking -IA de détection vidéo

NB: J'ai veillé à anonymiser et pseudonymiser l'ensemble des données et informations partagées

2. La stratégie de défense en profondeur

« La meilleure tactique consiste à prendre une position que l'ennemi n'osera attaquer. » - Sun Tzu, L'Art de la guerre

La défense en profondeur repose sur la multiplication des couches de sécurité, en combinant outils, politiques, formations, et veille continue :



Niveaux clés :

- Périmètre : Firewall, proxy, VPN
- Réseau : segmentation, VLAN, IDS/IPS
- Postes de travail : antivirus, GPO, EDR
- Serveurs : hardening, journalisation, bastion
- Identité : SSO, MFA, gestion des droits
- Utilisateurs : sensibilisation, anti-phishing
- Réaction : plan de réponse, backups, forensic

3. La réponse aux incidents : de la détection à la reconstruction



Le cycle de gestion d'un incident doit inclure 6 étapes :

- Préparation : plan IR, rôle du SOC
- Détection : journaux, SIEM, alertes
- Confinement : isolement des machines infectées
- Éradication : suppression des malwares, comptes suspects
- Restauration : retour aux opérations normales
- Leçon tirée : analyse post-mortem, patching, durcissement

4. Cas pratiques sénégalais & enseignements à y tirer

Année	Cible	Nature de l'attaque	Impact constaté	Mesures prises / Recommandations ¹³
2020	Autorités publiques ¹⁴	Intrusion et vol de fichiers internes	Atteinte à la confidentialité des documents	-Formation du personnel -Audit ISO 27001 -Restriction des accès
2023	Établissement d'enseignement supérieur	Ransomware via fichier PDF infecté	Données étudiantes verrouillées	-Segmentation du réseau -Backups hors-ligne réguliers
2024	Plateforme étatique (pré-électorale)	Attaque DDoS	Indisponibilité des services (3 heures)	-Activation d'un WAF -Collaboration avec un prestataire spécialisé
2025	Haut responsable gouvernemental	Compromission de messagerie professionnelle	Fuites dans la presse	-Renforcement de l'authentification (MFA) -Sensibilisation des VIP -Déploiement DLP

NB: J'ai veillé à anonymiser et pseudonymiser l'ensemble des données et informations partagées

5. Vers une culture nationale de cyberrésilience

La résilience ne dépend pas uniquement des machines, mais de l'humain accompagné de bons réflexes et de bonnes doctrines.

Il est urgent de :

¹³ Les recommandations sont formulées à partir de standards internationaux (ISO, NIST) et bonnes pratiques du secteur.

¹⁴ Les identités des institutions ont été anonymisées pour se conformer aux standards de responsabilité numérique.

- Établir un Centre National de Réponse aux Incidents (CERT),
- Former des équipes d'intervention rapide (CSIRT),
- Équiper chaque ministère, région, grande entreprise d'un plan de réponse cyber,
- Et de créer une culture partagée du cyber-risque.

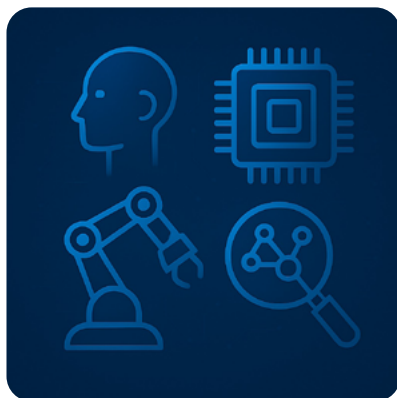
La cyberdéfense ne doit plus être une réaction, mais une posture proactive, collective et stratégique.

IV

PERSPECTIVES STRATÉGIQUES ET ENJEUX D'AVENIR DU NUMÉRIQUE AU SÉNÉGAL



A. Technologies émergentes et perspectives stratégiques



1. Une nouvelle révolution technologique en marche

La montée en force des technologies émergentes comme l'IA, la blockchain, l'IoT, le cloud, la 5G...) ouvre un monde d'opportunités, mais aussi de risques amplifiés ou une augmentation de la surface d'attaque pour les nations qui ne maîtrisent pas leur politique numérique.

Pour un pays comme le Sénégal, engagé dans une transformation digitale ambitieuse (New Deal Technologique), ces technologies représentent à la fois un levier de développement et une source potentielle de dépendance si elles ne sont pas encadrées avec vision, compétence et souveraineté.

Dans ce contexte, il est impératif de comprendre, anticiper et encadrer ces innovations afin de ne pas en devenir les consommateurs passifs ou les cybervictimes.

2. Technologies à fort impact stratégique

a. Intelligence Artificielle (IA)

- **Opportunités** : automatisation des services publics, santé prédictive, sécurité, agriculture de précision et bien d'autres choses.
- **Risques** : manipulation de l'information (deepfakes), surveillance massive, prise de décision opaque, menaces dopées par l'IA à savoir les APT (malwares intelligents, IA générative pour hameçonnage...).
- **Priorités** :
 - Éthique de l'IA adaptée au contexte africain ;
 - Création d'un Centre National de Recherche en IA ;
 - Encadrement législatif de l'usage public et privé de l'IA.

À noter que le Sénégal s'est déjà doté d'une stratégie nationale en intelligence artificielle, qui a été présentée en septembre 2023 et finalisée en janvier 2024¹⁵.

b. Blockchain et Web3

- **Usages potentiels** : registre foncier sécurisé, transparence électorale, traçabilité des ressources (pétrole, gaz), vote électronique.
- **Risques** : escroqueries (ICO frauduleuses), perte de souveraineté en cas d'utilisation d'une blockchain étrangère.
- **Axes stratégiques** :
 - Expérimentations réglementées ;
 - Incubateurs spécialisés en blockchain ;

¹⁵ Ministère de la Communication, des Télécommunications et de l'Économie Numérique, Stratégie nationale sur l'intelligence artificielle (SNIA), République du Sénégal, présentée officiellement le 14 septembre 2023, en ligne sur : <https://bhc.ceiad.sn/2023/09/15/intelligence-artificielle-ia-le-senegal-adopte-une-strategie-nationale&https://africadataprotection.org/sources/Synth%C3%A8se%20de%20la%20strat%C3%A9gie%20IA%20du%20S%C3%A9n%C3%A9gal.pdf>, consulté tous deux le 20 Avril 2025.

- voir comment intégrer le cadre pour les actifs virtuels tels que les cryptomonnaies (Bitcoin, Ethereum etc.), les Token non fongibles (NFT) dans loi du 14.02.24 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des armes de destruction massives.

La loi du 14 février 2024 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des armes de destruction massive, a transposé une directive communautaire de l'UMOA. Elle définit explicitement la notion d'actif virtuel, encadre les prestataires de services sur actifs virtuels (PSAV), fixe les conditions d'agrément, ainsi que les obligations en matière de conformité, de vigilance et de déclaration des opérations suspectes.

c. Objets connectés (IoT)

- Opportunités : smart cities, télésanté, agriculture connectée, gestion énergétique.
- Risques : espionnage industriel, vulnérabilités dans les capteurs, piratage d'infrastructures.
- Priorités :
 - Audit des objets IoT dans les administrations ;
 - Normes locales de sécurité IoT ;
 - Création d'un observatoire national de l'IoT.

d.5G et au-delà

- Opportunités : téléchirurgie, véhicules autonomes, connectivité massive dans les zones rurales.
- Risques : dépendance technologique vis-à-vis de fournisseurs étrangers, risques géopolitiques (espionnage, backdoors).

- Stratégie :
 - Analyse de souveraineté avant tout déploiement ;
 - Création de réseaux sécurisés pour les services critiques.

e. Systèmes biométriques et données sensibles

- Le Sénégal, à travers sa carte d'identité biométrique CEDEAO, ses systèmes de sécurité aéroportuaire et bientôt ses projets de digitalisation énumérés dans le New Deal Technologique, stockerait et traiterait une masse croissante de données sensibles.
- Cela nécessite un encadrement strict :
 - Protection légale contre l'exploitation abusive ;
 - Stockage local chiffré ;
 - Formation des Délégués à la Protection des Données (DPO) dans le secteur public.

f. Cloud computing et données souveraines

- La majorité des données sénégalaises sont actuellement hébergées à l'étranger, via des services tels que Google, AWS ou Microsoft.
- Cela pose un problème de souveraineté et de juridiction.
- Proposition :
 - Mise en place d'un Cloud Souverain Sénégalais ou ouest-africain ;
 - Appel à projets pour hébergement sécurisé dans des datacenters nationaux.

g. L'ordinateur quantique : une menace pour le chiffrement actuel

L'émergence de l'ordinateur quantique représente une avancée technologique majeure, susceptible de remettre en cause la cybersécurité mondiale.

Les systèmes actuels de chiffrement (RSA, ECC...) reposent sur la complexité mathématique que seuls les ordinateurs classiques mettent des milliers d'années à résoudre.

Or, avec les puissances de calcul que va offrir cette machine quantique, certaines mesures de protection (chiffrement et autres) pourraient être cassées en quelques heures.

Même si la maîtrise industrielle de l'ordinateur quantique n'est pas immédiate, le Sénégal et l'Afrique doivent intégrer cette perspective dans leur stratégie numérique.

Dès aujourd'hui, il devient crucial de :

- Faire en sorte que nos chercheurs et autres responsables suivent les travaux de normalisation du NIST sur la cryptographie post-quantique etc.).
- Protéger les données sensibles contre l'effet «store now, decrypt later» (stocker maintenant, déchiffrer plus tard).
- Encourager la recherche et la formation autour de la cybersécurité quantique dans nos universités.

La souveraineté numérique du Sénégal ne saurait être complète sans une anticipation lucide et réfléchie sur les technologies émergentes à venir.

3. Vers une stratégie technologique souveraine

La gestion de ces technologies émergentes ne peut plus être laissée au hasard.

Il est temps pour le Sénégal de bâtir une véritable stratégie technologique souveraine, qui s'articulera autour des points suivants :

- Veille technologique permanente : Cette cellule de prospective devra être rattachée à la Présidence ou à la primature.
- Investissements en Recherche & Développement : Soutenir les universités et startups du domaine.
- Régulation agile et repensée : Mettre en place des lois qui encadrent mais qui ne devront pas bloquer l'innovation.
- Capacitation locale : Implanter des centres de formation, créer des partenariats avec les grandes écoles, proposer des bourses en IA et Blockchain.
- Dialogue public-privé : Faire une réalité, l'inclusion des startups, des chercheurs, des ingénieurs dans la construction des politiques publiques.
- Création de think-tank ou groupe de réflexions pour inviter une contribution internationale de chercheurs, universitaires et toute figure de proue dans le domaine.
- Promouvoir une coopération internationale à caractère privé ou sur une base de bénévolat de tout gardien (angel hacker) de la cybernet.

4. Un enjeu de souveraineté, mais aussi d'équité

La **liberté d'information** est un pilier fondamental des sociétés démocratiques, garantissant à chaque individu le droit d'accéder à

des informations fiables et de les partager sans entrave. Elle joue un rôle essentiel dans la transparence, la gouvernance et la participation citoyenne, permettant aux populations de s'informer, de débattre et de prendre des décisions éclairées. ***Comme l'a souligné la juriste Aminata Sawadogo, la liberté d'information est essentielle à la liberté d'expression puisque c'est en étant bien informé qu'on peut exprimer une opinion éclairée.*** Pour autant, il est nécessaire que les données ou les flux d'information, souvent manipulés ou restreints, fassent l'objet d'une protection effective.

A l'ère du deepfake et des technologies émergentes, la liberté d'information se heurte à des défis sans précédents. Les avancées en IA permettent désormais de manipuler des images, des voix et figures avec une réelle précision, remettant en question même la véracité de l'information.

Il faut donc intégrer les technologies émergentes dans la stratégie nationale, c'est aussi une manière de garantir que personne ne soit laissé de côté. L'inclusion des jeunes, des femmes, des zones rurales, des personnes en situation de handicap est un pilier fondamental de toute politique numérique durable, car au-delà des chiffres et des infrastructures, il s'agit de construire un numérique sûr, éthique, green et accessible à tous.

En définitive, le leitmotiv est de trouver un équilibre : comment avancer technologiquement sans compromettre nos droits.

5. Tableau récapitulatif des Technologies Émergentes

Technologie	Opportunités	Risques / Défis	Pistes stratégiques pour le Sénégal
IA (Intelligence Artificielle)	<ul style="list-style-type: none"> - Santé prédictive - Automatisation e-services - Détection menaces cyber 	<ul style="list-style-type: none"> - Deepfakes, IA malveillante - Décisions opaques - Surveillance de masse 	<ul style="list-style-type: none"> - Lancer un centre national IA - Créer un cadre éthique sénégalais - Réglementer usage public/privé
Blockchain / Web3	<ul style="list-style-type: none"> - Traçabilité - Transparence (élections, foncier) - NFTs / Crypto actifs 	<ul style="list-style-type: none"> - Escroqueries - Cadre juridique inexistant - Dépendance aux plateformes étrangères 	<ul style="list-style-type: none"> - Incubateurs blockchain - Cadre pour cryptoéconomie locale - Pilotes institutionnels régulés
IoT (Objets connectés)	<ul style="list-style-type: none"> - Smart cities - Santé à distance - Agriculture connectée 	<ul style="list-style-type: none"> - Sabotage, piratage - Données non chiffrées - Intrusion dans la vie privée 	<ul style="list-style-type: none"> - Normes de sécurité IoT locales - Audit des objets dans l'administration - Observatoire national de l'IoT

5G / 6G	<ul style="list-style-type: none"> - Villes intelligentes - Connexion zones rurales - Industrie 4.0 	<ul style="list-style-type: none"> - Backdoors étrangères - Risques d'espionnage - Monopole de certains fournisseurs 	<ul style="list-style-type: none"> - Clause de souveraineté technologique - Évaluation préalable à tout déploiement
Systèmes biométriques	<ul style="list-style-type: none"> - Identification sécurisée - Accès aux services - Contrôle des frontières 	<ul style="list-style-type: none"> - Détournement de données - Absence de consentement Hébergement externe 	<ul style="list-style-type: none"> - Stockage local & chiffré - Instaurer ou Adhérer à un cadre sur le Règlement sur la protection des DP africain - Formations DPO publics
Cloud computing	<ul style="list-style-type: none"> - Efficacité des services - Mutualisation des ressources -Dématérialisation 	<ul style="list-style-type: none"> - Données hébergées à l'étranger - Juridictions extraterritoriales 	<ul style="list-style-type: none"> - Création d'un Cloud Souverain - Partenariats locaux & régionaux - Hébergement des services publics au pays
Ordinateur quantique	<p>Calculs exponentiellement plus rapides</p> <p>Révolutions scientifiques et industrielles futures</p>	<p>Menace directe sur le chiffrement classique (RSA, ECC, ...)</p> <p>Risque de décodage des données archivées</p>	<ul style="list-style-type: none"> -Transition vers la cryptographie post-quantique - Suivi des standards NIST -Sensibilisation des institutions critiques

B. Le New Deal Technologique: Enjeux et Perspectives



1. Présentation

Le Sénégal s'engage résolument dans une transformation numérique visant à positionner le pays comme un leader africain dans le domaine du digital. Cette ambition, portée par le New Deal Technologique, repose sur une vision intégrée de la digitalisation de l'administration, du développement de l'économie numérique et de la souveraineté technologique.

2. Un enjeu stratégique majeur

Le numérique est désormais perçu comme un moteur de croissance économique et sociale. Le gouvernement sénégalais a fait de la digitalisation un objectif politique prioritaire, avec des retombées attendues significatives : une contribution de 10% au PIB et la création de 140.000 emplois directs et indirects. Cet engagement s'inscrit dans l'axe 4 du Plan Sénégal Émergent (PSE), qui met en avant l'innovation et la modernisation des services publics.

3. Les axes stratégiques du New Deal Technologique

Pour atteindre ses objectifs, cette nouvelle stratégie numérique du Sénégal repose sur quatre axes majeurs :

- Développement de l'économie numérique : Encourager l'innovation et une compétitivité saine des entreprises du secteur.
- Digitalisation de l'administration : Simplifier les services publics grâce aux outils numériques et digitaux.
- Souveraineté nationale : Renforcer la cybersécurité et maîtriser les infrastructures critiques.
- Faire du Sénégal un leader africain du numérique : Développer des pôles technologiques et des services numériques compétitifs à l'échelle continentale.

4. Un cadre favorable à la transformation

Pour garantir le succès de cette stratégie, trois prérequis fondamentaux ont été définis :

- Un cadre juridique et institutionnel adapté pour accompagner les innovations numériques.
- Un capital humain qualifié grâce à des programmes de formation aux métiers du numérique.
- Une confiance numérique renforcée à travers des politiques de cybersécurité et de protection des données.

5. Un état des lieux encourageant

Le Sénégal se positionne de plus en plus comme un acteur clé du numérique en Afrique. En 2021, 58,1% de la population avait accès à Internet, plaçant le pays parmi les leaders en Afrique de l'Ouest. Toutefois, des efforts restent à fournir pour améliorer la vitesse moyenne de connexion et réduire le coût de l'Internet, encore élevé par rapport aux standards internationaux.

En termes de développement des TIC, le Sénégal figure parmi les 15 premiers pays africains et occupe la 12^e place des exportateurs de services numériques en Afrique, avec un chiffre d'affaires de 500 millions de dollars.

6. Enjeux de la cybersécurité du New Deal Technologique

Le New Deal Technologique ne peut réussir qu'avec une approche robuste de la cybersécurité. En effet, toute transformation numérique ambitieuse dans le monde repose sur une infrastructure fiable, résiliente et digne de confiance. Et sans cybersécurité, il n'y a ni confiance, ni souveraineté, ni durabilité.

a. Sécuriser les fondations de la transformation numérique

Les projets phares du New Deal Technologique qu'il s'agisse de la digitalisation des services publics, de la dématérialisation de l'administration, ou de l'interconnexion des services publics vont s'appuyer sur des systèmes d'information complexes, interopérables mais avec une mauvaise mise en place, ils seront vulnérables. Chaque brique numérique doit donc être pensée avec une approche «secure by design», intégrant des exigences de sécurité dès la conception.

Cela implique :

- La protection des données sensibles des citoyens et de l'État ;
- La sécurisation des plateformes d'e-gouvernement contre les attaques DDoS, les intrusions, ou les rançongiciels ;
- L'audit régulier des infrastructures critiques , permettra de connaître les forces et faiblesse du SI des OIV et ainsi anticiper les cyberattaques ;
- L'évaluation des cyberrisques avant le déploiement de toute solution technologique.

b. Préserver la souveraineté numérique du Sénégal

Dans un contexte de dépendance technologique vis-à-vis des grandes puissances et des géants de la TECH à l'image des GAFAM , BATX - Huawei , le New Deal Technologique doit également être un levier de souveraineté. Cela passe par :

- La maîtrise des infrastructures stratégiques (cloud souverain, hébergement local, contrôle des flux de données) ;
- Le développement de logiciels et d'outils locaux adaptés aux réalités sénégalaises ;
- La négociation de partenariats équilibrés avec les fournisseurs technologiques étrangers, dans le respect de nos lois, règlements et de nos propres intérêts.

c. Préparer les ressources humaines à l'ère de la cybersécurité

Un E-État est aussi un État vulnérable, s'il n'investit pas dans la formation de ses talents. Le New Deal Technologique doit donc intégrer ou promouvoir un volet fort de développement des compétences en cybersécurité, à tous les niveaux :

- Formations techniques pour les ingénieurs, développeurs et administrateurs systèmes ;
- Sensibilisation des décideurs politiques à la cybersécurité ;
- Appui à la recherche locale en cybersécurité et cryptographie ;
- Soutien à l'émergence d'un écosystème local de startups surtout ceux en cybersec.

d. Instaurer une gouvernance cyber claire et coordonnée

Un projet de transformation aussi vaste que le New Deal Technologique nécessite une architecture de gouvernance claire, coordonnée entre les acteurs publics, privés, communautaires et académiques. Il faut éviter les silos, les chevauchements, les zones grises. Cela suppose :

- Une stratégie nationale de cybersécurité actualisée et alignée avec les objectifs du New Deal Technologique ;
- Une Haute Autorité dédiée pour piloter et superviser les efforts cyber à l'échelle nationale ;
- Un cadre juridique rénové, protecteur et incitatif.

Avec l'accélération de la digitalisation et des investissements dans les infrastructures technologiques, le Sénégal se donne les moyens de devenir un hub numérique en Afrique. L'implication des acteurs privés, l'amélioration des services numériques et l'intégration de solutions technologiques avancées seront des leviers essentiels pour atteindre ces objectifs ambitieux.

En plaçant le numérique au cœur de son développement, le Sénégal fait un pari gagnant sur l'avenir, avec une ambition claire : bâtir une économie numérique inclusive, compétitive et souveraine.

C. Tribune de l'Association Africaine des Droits Numériques : Pour une réforme en profondeur du dispositif national de protection des données personnelles



Dans une tribune publiée sur Seneweb en Mai 2024, l'Association Africaine des Droits Numériques (ADN)¹⁶ appelle à une refonte en profondeur du dispositif national de protection des données à caractère personnel. Cette contribution souligne l'importance stratégique de la gouvernance des données pour le développement numérique du Sénégal et sa compétitivité internationale.

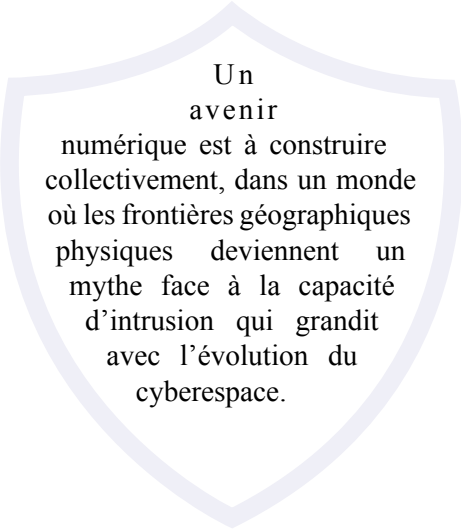
L'Association formule plusieurs recommandations clés, notamment :

- Accélérer l'adoption du projet de loi de réforme du cadre légal actuel (loi de 2008), pour l'adapter aux défis contemporains (cloud, biométrie, IA, données massives).
- Renforcer le pouvoir d'auto-saisine de la future HAPDP, afin qu'elle puisse agir même sans requête préalable.

- Permettre à toute personne physique ou morale, y compris les associations légalement constituées, de saisir l’Autorité.
- Garantir l’indépendance réelle de l’Autorité en revoyant :
 - sa composition et son mode de désignation;
 - son autonomie budgétaire;
 - son pouvoir de sanction et d’audit.
- Introduire une obligation d’information systématique en cas de fuite ou de violation grave de données.
- Renforcer la législation sectorielle, notamment sur les données de santé, afin de mieux encadrer leur collecte, traitement et hébergement.
- Accompagner la réforme d’un vaste programme de sensibilisation des citoyens, des entreprises et des administrations publiques.

L’objectif affiché est clair : faire du Sénégal un modèle régional en matière de souveraineté, d’éthique, de régulation numérique et de protection efficace des droits fondamentaux.

CONCLUSION



Un
avenir
numérique est à construire
collectivement, dans un monde
où les frontières géographiques
physiques deviennent un
mythe face à la capacité
d'intrusion qui grandit
avec l'évolution du
cyberespace.

Le monde change rapidement et avec lui, le numérique est devenu à la fois levier de développement et champ de bataille invisible. Le Sénégal, un pays de talents, d'ambitions et de promesses, ne peut rester en marge de cette transformation ni subir passivement les cyber menaces venues en interne ou d'ailleurs.

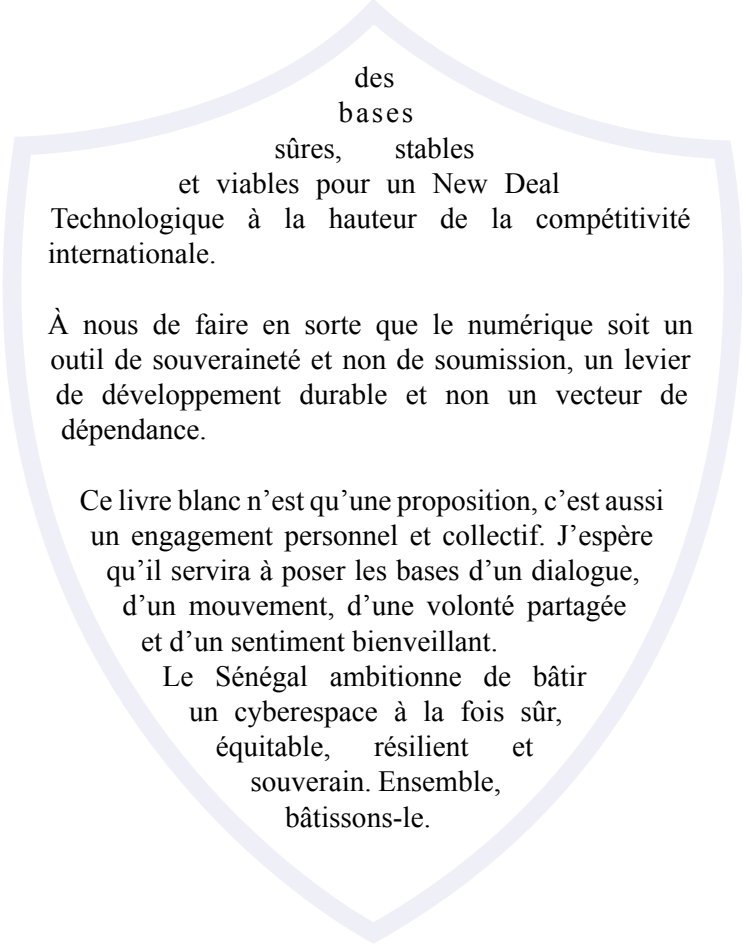
Les cyberattaques documentées dans ce livre blanc, les failles relevées, les constats parfois alarmants, ne sont pas une condamnation, mais un appel à l'action collective. Elles témoignent de la nécessité de bâtir un modèle sénégalais de cybersécurité, à la fois souverain, résilient, inclusif et tourné vers l'avenir.

Cela devra forcément passer par une gouvernance centralisée et visionnaire, capable de piloter une politique nationale cohérente; des lois mises à jour ou adoptées, protectrices de nos cyberdroits et de nos cyberintérêts ; une stratégie éducative ambitieuse, afin de former des citoyens conscients et des experts nationaux compétents et un écosystème numérique souverain, porté par nos talents, nos startups, nos institutions.

Mais au-delà des textes, des plans et des schémas, ce livre blanc est un outil de sensibilisation pour tout le monde mais surtout pour les preneurs de décisions, qui apprendront à avoir plus d'engagement et de responsabilité pour se prémunir davantage face au enjeux sécuritaires dans un monde où les cyberattaques constituent des menaces permanentes (**à chaque millième de seconde, une cyberattaque risque de détruire certains éléments de notre cyberspace et même aller jusqu'à perturber l'harmonie dans nos cadres de vie, nos écosystèmes**).

La cybersécurité n'est pas qu'une affaire de techniciens, de lois ou de ministères ou d'agences ou de directions; **C'est une affaire de tous. C'est une question de confiance, de souveraineté et de dignité.**

Nous avons aujourd'hui une fenêtre historique : celle d'un nouveau leadership, d'une ambition renouvelée, et d'un peuple connecté et éveillé. Il est donc très important d'accompagner nos dirigeants à asseoir



des
bases
sûres, stables
et viables pour un New Deal
Technologique à la hauteur de la compétitivité
internationale.

À nous de faire en sorte que le numérique soit un outil de souveraineté et non de soumission, un levier de développement durable et non un vecteur de dépendance.

Ce livre blanc n'est qu'une proposition, c'est aussi un engagement personnel et collectif. J'espère qu'il servira à poser les bases d'un dialogue, d'un mouvement, d'une volonté partagée et d'un sentiment bienveillant.

Le Sénégal ambitionne de bâtir
un cyberspace à la fois sûr,
équitable, résilient et
souverain. Ensemble,
bâtissons-le.

TABLE DES MATIÈRES

PRÉFACE	8
AVANT-PROPOS	11
ANCRAGE DANS LES RÉFÉRENCES EXISTANTES ET PERSPECTIVES D'ÉVOLUTION	13
GLOSSAIRE DES TERMES CLÉS	15
INTRODUCTION	18
I. ÉTAT DES LIEUX SENEGAL	20
A. Aperçu de l'état des lieux	21
1. Cybersécurité : une urgence mondiale, un défi africain	21
a. Un monde hyperconnecté, mais exposé	21
b. Le Sahel : quand l'insécurité rencontre le numérique	22
c. Mais tout n'est pas sombre : l'Afrique se réveille	22
2. Cadre juridique, réglementaire et institutionnel de la cybersécurité au Sénégal	22
a. Instruments juridiques internationaux ratifiés	23
b. Lois nationales encadrant le cyberspace	24
3. Cadre institutionnel de gouvernance cyber	25
4. Politique nationale & évaluation stratégique	26
5. Une approche multipartite en évolution	26
B. Analyse critique du cadre cyber sénégalais	27
1. Les points positifs : des fondations pionnières et un engagement réel	27
2. Les limites actuelles : fragmentation, obsolescence et manque de coordination	28
a. Un cadre juridique avec une évolution très lente	28
b. Une fragmentation des acteurs	29
c. Un manque de moyens humains et techniques	30
d. Une faible sensibilisation du public	30
e. Des enjeux numériques et de cybersécurité encore insuffisamment pris en compte	31
3. Réflexions sur la DCSSI : entre centralisme institutionnel et besoin de refondation organique	31

a. Une autorité logée au Palais : un symbole fort, mais un positionnement problématique	32
b. Une confusion persistante entre chiffrement étatique et cybersécurité collective	33
c. Aucune initiative structurante ou action visible à l'échelle nationale	33
d. Des limites structurelles face à la transformation numérique actuelle	34
e. Proposition : Vers une Haute Autorité de la Cybersécurité (HAC)	34
II. LE CONTEXTE DES CYBER MENACES AU SÉNÉGAL...36	
A. Constat	37
1. Multiplication des cas d'usurpation d'identité, de fraudes en ligne et de fuites de données	37
2. Institutions publiques ciblées par des ransomwares	37
3. Vulnérabilités dans les infrastructures critiques (OIV)	38
4. Faible sensibilisation généralisée à la cybersécurité	38
5. Nouveaux enjeux géostratégiques : pétrole, gaz et cyberespionnage	38
6. Cyberattaques dans un contexte politique instable	39
B. Synthèse des principales cyberattaques au Sénégal (2018-2025)...40	
C. Tableau chronologique de quelques principales cyberattaques au Sénégal (2018–2025) : attaques, impacts et mesures de réponse.....	42
D. Focus Fraudes et cyberattaques dans les services financiers.....	43
1. Les causes principales	44
2. Conséquences observées	44
3. Pistes de réponse	44
III. PROPOSITION DE SOLUTIONS.....51	
A. Cadre de gouvernance	47
1. Mise en place d'une Haute Autorité de la Cybersécurité (HAC).....	48
a. Positionnement institutionnel	48
b. Pourquoi ce choix ?	49
c. Missions	49
e. Fonctionnement de la HAC	50
f. Collaborations stratégiques prioritaires	51

g. Création d'un Pôle national de coordination des forces de lutte contre la cybercriminalité	52
2. Le Commandement de Cyberdéfense : vers une 5 ^e Armée Sénégalaise	53
a. Positionnement institutionnel	53
b. Missions principales	54
c. Structure interne	54
d. Dimension régionale	55
e. Pourquoi une telle évolution est nécessaire ?	55
3. Haute Autorité pour la Protection des Données Personnelles (HAPDP)	55
a. Missions clés	56
b. Organisation	56
c. Pouvoirs	56
d. Conseil consultatif pluridisciplinaire	57
e. Autres axes de réformes et recommandations	57
B. Réforme du cadre juridique	58
1. Mise à jour de la Loi n°2008-11 sur la cybercriminalité	58
2. Intégration d'un cadre légal pour la souveraineté numérique, l'open data et la régulation des plateformes en ligne (GAFAM).....	59
3. Création de tribunaux spécialisés en cybercriminalité si ce n'est pas encore le cas	60
4. Intégration de la cyberdéfense dans le Code pénal et le Code de justice militaire	61
5. Intégration de la cyberdéfense dans le Code pénal et le Code de justice militaire	61
6. Intégration de la cybersécurité et de la cyberdéfense dans les écoles de formation régaliennes	62
a. Pour l'École Nationale de Police : Cybersécurité et cyberdéfense appliquées	62
b. Pour l'École Nationale de la Magistrature : Introduction à la cybersécurité pour magistrats	63
C. Sensibilisation, Formation et Promotion d'une Culture de Cybersécurité Durable	64
1. Sensibilisation générale et ciblée de la population	64

2. Intégration de la cyberhygiène et de la cybersécurité dans les curricula scolaires	65
3. Création de clubs de détection de talents et accompagnement des vocations	66
a. Création de clubs scolaires de cybersécurité	66
b. Soutien aux initiatives communautaires et événements tech	66
4. Déploiement d'une plateforme éducative numérique sécurisée.....	67
5. Journée ou Mois National de la Cybersécurité	67
6. Former en masse des professionnels qualifiés en cybersécurité.....	68
D. Attaques et Parades : comprendre les menaces pour mieux se défendre.....	68
1. Typologie des attaques les plus répandues	69
2. La stratégie de défense en profondeur	71
3. La réponse aux incidents : de la détection à la reconstruction.....	72
4. Cas pratiques sénégalais & enseignements	72
5. Vers une culture nationale de cyberrésilience	73

II. PERSPECTIVES STRATÉGIQUES ET ENJEUX D'AVENIR DU NUMÉRIQUE AU SÉNÉGAL.....

A. Technologies émergentes et perspectives stratégiques	76
1. Une nouvelle révolution technologique en marche	76
2. Technologies à fort impact stratégique	77
a. Intelligence Artificielle (IA)	77
b. Blockchain et Web3	77
c. Objets connectés (IoT)	78
d. 5G et au-delà	78
e. Systèmes biométriques et données sensibles	79
f. Cloud computing et données souveraines	79
g. L'ordinateur quantique : une menace pour le chiffrement actuel.....	80
3. Vers une stratégie technologique souveraine	81
4. Un enjeu de souveraineté, mais aussi d'équité	81
5. Tableau récapitulatif des Technologies Émergentes	83
B. Le New Deal Technologique : Enjeux et Perspectives	85
1. Présentation	85

2. Un enjeu stratégique majeur	85
3. Les axes stratégiques du New Deal Technologique	86
4. Un cadre favorable à la transformation	86
5. Un état des lieux encourageant	86
6. Enjeu de la cybersécurité du New Deal Technologique	87
a. Sécuriser les fondations de la transformation numérique	87
b. Préserver la souveraineté numérique du Sénégal	88
c. Préparer les ressources humaines à l'ère de la cybersécurité....	88
d. Instaurer une gouvernance cyber claire et coordonnée	89
C. Tribune de l'Association Africaine des Droits Numériques : Pour une réforme en profondeur de la CDP	90
CONCLUSION	92
TABLE DES MATIÈRES	96
GLOSSAIRE DES TERMES CLÉS	101
ANNEXE	105
A. Résultats de l'enquête citoyenne sur le New Deal Technologique.....	105
1. Contexte	105
2. Résultats	105
3. Extraits de messages adressés aux décideurs	107
B. Comprendre et reconnaître les principales techniques de fraude numérique.....	108
1. Phishing (hameçonnage)	108
2. SIM Swap (détournement de carte SIM)	109
3. Usurpation d'identité	109
4. Applications de prêt frauduleuses	110
REMERCIEMENTS	111
REMERCIEMENTS SPÉCIAUX	124
SOURCES	126
A. Bibliographie	126
1. Ressources nationales (Sénégal)	126
2. Ressources régionales (Afrique)	126
3. Ressources internationales	127

B. Webographie	127
1. Ressources nationales (Sénégal)	127
2. Ressources régionales (Afrique)	128
3. Ressources internationales	128
PRÉCAUTION D'USAGE	129
PRÉSENTATION DE L'AUTEUR	130
CONTACT ET RETOURS	133
RÉSUMÉ DU LIVRE BLANC	134

GLOSSAIRE DES TERMES CLÉS

A

ADIE / SENUM : Agence de l'Informatique de l'État devenue Sénégal Numérique SA, chargée du développement des infrastructures et services numériques de l'administration.

ARTP: Agence de régulation des télécommunications et des Postes.

APT (Advanced Persistent Threat) : Menace avancée et persistante, souvent le fait d'un groupe bien organisé (souvent étatique), ciblant spécifiquement une organisation avec des attaques sophistiquées et continues.

Authentification Multifacteur (MFA) : Technique de sécurité qui combine plusieurs méthodes d'authentification (mot de passe + code SMS, empreinte digitale, etc.).

B

Blockchain : Technologie de registre distribué permettant un enregistrement transparent et infalsifiable des transactions, utilisée pour les cryptoactifs ou les processus comme le vote électronique.

Bootcamp : Formation intensive sur une courte période, axée sur la pratique et souvent utilisée dans les domaines technologiques.

Burp Suite : Outil utilisé en test d'intrusion pour identifier les failles dans les applications web.

C

CDP (Commission des Données Personnelles) : Autorité sénégalaise de régulation et de protection des données à caractère personnel.

CERT / CSIRT : Centre de réponse aux incidents de sécurité, chargé d'identifier, traiter et coordonner la réponse aux cyberattaques.

Chiffrement : Procédé de codage des données pour les rendre illisibles à toute personne non autorisée.

Cloud Souverain : Solution de stockage de données dans des infrastructures nationales pour garantir la souveraineté numérique.

Cyberespionnage : Utilisation du numérique pour collecter

illégalement des informations sensibles, souvent à des fins politiques ou économiques.

Cybermenace : Tout type de risque ou d'attaque possible visant les systèmes numériques.

Cybersécurité : Ensemble des moyens techniques, juridiques et humains destinés à protéger les systèmes informatiques et les données numériques.

CCD : Commandant Cyberdéfense

D

Dark Web : Partie du web non indexée par les moteurs de recherche traditionnels, souvent utilisée pour des activités illicites.

DCSSI : Direction du Chiffrement et de la Sécurité des Systèmes d'Information du Sénégal, structure étatique logée à la Présidence, critiquée pour son opacité.

DDoS (Distributed Denial of Service) : Attaque par déni de service visant à rendre un service web indisponible en saturant son serveur de requêtes.

DLP (Data Loss Prevention)

: Technologies utilisées pour prévenir les fuites de données sensibles.

Deepfake : Vidéo, image ou audio falsifié grâce à l'IA pour imiter une personne réelle.

E

EDR (Endpoint Detection and Response) : Logiciels installés sur les terminaux pour surveiller, détecter et répondre aux menaces.

Encryption / Chiffrement : Technique de sécurité consistant à rendre des données illisibles sans une clé de déchiffrement.

ENCVR (Ecole Nationale de Cybersécurité à Vocation Régionale) : Son objectif principal est de renforcer les capacités et les connaissances techniques en Cybersécurité des acteurs du public.

F

Firewall (pare-feu) : Outil de sécurité réseau qui filtre le trafic entrant et sortant selon des règles définies.

NIST (National Institute of Standards and Technology en français) : « Institut national des normes et de la technologie ») : C'est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des normes de concert avec l'industrie.

pour identifier les vulnérabilités d'un système.

PSAV (Prestataires de Services liés aux Actifs Virtuels) : désigne une société qui exerce tout ou partie des activités ou opérations telles l'échange, le transfert, la conservation, la gestion et les services financiers relatifs aux actifs virtuels comme les cryptomonnaies.

O

OSINT (Open Source Intelligence) : Collecte d'informations à partir de sources ouvertes comme internet, médias sociaux, bases publiques, etc.

OIV (Opérateur d'Importance Vitale) : C'est une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.

P

Phishing / Spear Phishing : Technique de hameçonnage pour tromper une personne et lui faire divulguer ses données sensibles.

Pentesting (test d'intrusion) : Simulation contrôlée d'attaque

R

Ransomware : Malware qui chiffre les données d'un utilisateur ou d'une entreprise en exigeant une rançon pour les déverrouiller.

RGPD : Règlement général sur la protection des données de l'UE, modèle de référence en matière de protection des données.

S

SIEM (Security Information and Event Management) : Système d'analyse centralisée de la sécurité basé sur les logs et événements de sécurité.

SOC (Security Operations Center) : Centre de surveillance

des incidents de cybersécurité.

SysAdmin, activement exploitée par des attaquants.

SI (Système d'Information)

: C'est l'ensemble des ressources de l'entreprise qui permettent la gestion de l'information.

Zero Trust : Modèle de sécurité qui part du principe que personne ne doit être automatiquement digne de confiance, même à l'intérieur du périmètre réseau.

si (système informatique) :

C'est l'ensemble des éléments matériels de l'entreprise qui permettent le traitement de l'information.

T

Threat Intelligence (CTI) :

Collecte et analyse de données sur les cybermenaces pour anticiper les attaques.

Telcos: Les opérateurs de télécommunications

V

VPN (Virtual Private Network) :

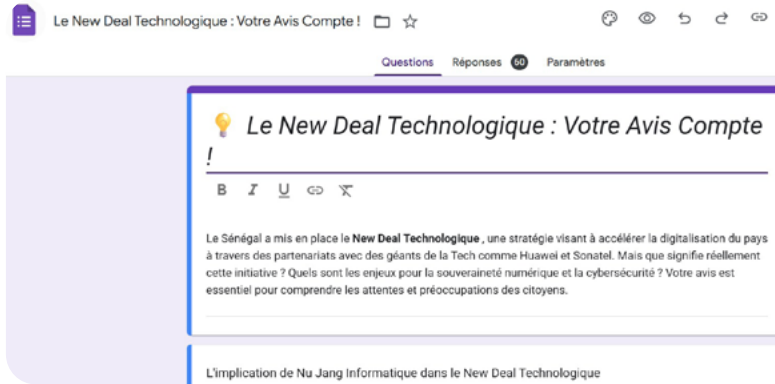
Outil de sécurisation de la connexion en chiffrant le trafic internet.

Z

Zero-day : Vulnérabilité inconnue des développeurs ou des

ANNEXE

A. Résultats de l'enquête citoyenne sur le New Deal Technologique



1. Contexte

En mars 2025, un formulaire d'enquête a été diffusé dans les communautés techniques et éducatives du numérique sénégalais. Il a récolté 60 réponses exploitables. L'objectif : connaître la perception citoyenne sur le New Deal Technologique.

2. Résultats

Connaissance générale :

- 66 % connaissent le New Deal
- 34 % le connaissent en détail

Objectifs perçus (choix multiples) :

- Digitalisation des services publics – 92 %
- Souveraineté numérique – 84 %
- Améliorer la connectivité – 58 %
- Attirer les entreprises tech – 56 %

Perception des partenariats tech (Huawei, Sonatel...) :

- Plutôt positifs – 42 %
- Mitigés – 32 %
- Négatifs – 4 %

Risques perçus (choix multiples) :

- Dépendance technologique – 84 %
- Perte de souveraineté sur les données – 60 %
- Impact sur les startups locales – 60 %
- Manque de transparence – 36 %

Mesures attendues de l'État :

- Renforcement des lois cyber – 90 %
- Hébergement local des données – 80 %
- Intégration des startups locales – 80 %

- Consultation publique – 74 %
- Formation citoyenne – 38 %

Secteurs des répondants : Informatique, cybersécurité, télécom, éducation, statistique, Web3, armée, énergie, IA, etc.

3. Extraits de messages adressés aux décideurs

« La jeunesse est oubliée. Il faut intégrer les jeunes ingénieurs sénégalais dans le projet. »

« Le New Deal doit garantir la souveraineté numérique. »

« Plus de transparence. Arrêtez de politiser les postes. »

« Formons dès l'enfance.

Construisons des datacenters alimentés par l'énergie solaire. »

Cette enquête révèle une prise de conscience citoyenne forte, qui vient appuyer la nécessité d'un cadre de gouvernance cyberclair, indépendant, et connecté aux réalités locales.

NB: à ce jour le formulaire est toujours actif via ce lien, n'hésitez pas à y contribuer et aussi partager:

<https://forms.gle/KuOeY2DnpyfiERDT8>



B. Comprendre et reconnaître les principales techniques de fraude numérique

Dans cette annexe, nous proposons un guide pratique pour aider les citoyens, les entreprises et les institutions à mieux comprendre et détecter les fraudes numériques les plus courantes au Sénégal.



1. Phishing (hameçonnage)

Définition : technique où l'arnaqueur se fait passer pour une entité de confiance (banque, opérateur mobile, entreprise) pour soutirer des informations sensibles (mot de passe, code PIN).

Comment le reconnaître :

- message ou email alarmant («Votre compte sera suspendu...»)
- liens suspects ou sites web imitant un site officiel
- demande urgente de confirmer vos identifiants

Conseil :

ne jamais cliquer sur les liens suspects. Contacter directement l'institution en question via ses canaux officiels.

2.SIM Swap (détournement de carte SIM)

Définition : technique qui consiste à prendre le contrôle de votre numéro de téléphone en le transférant frauduleusement sur une autre carte SIM.

Comment le reconnaître :

- vous perdez soudainement le réseau
- vous ne recevez plus d'appels ou de SMS
- alertes de changement d'informations sur vos comptes

Conseil :

activer l'authentification forte auprès de votre opérateur (code PIN SIM) et surveiller tout changement anormal.

3.Usurpation d'identité

Définition : un individu vole vos données personnelles (CNI, photo, numéro de compte) pour ouvrir des comptes à votre nom ou commettre des fraudes.

Comment le reconnaître :

- vous recevez des notifications de comptes ou crédits que vous n'avez pas ouverts
- des prélèvements inexplicables apparaissent

Conseil :

protéger ses documents officiels, ne jamais les partager en ligne sans raison légitime.

4. Applications de prêt frauduleuses

Définition : de fausses applications de crédit rapide promettent des prêts instantanés mais volent vos données ou votre argent.

Comment le reconnaître :

- application non vérifiée sur le Play Store
- conditions floues ou inexistence d'une adresse physique
- demande de frais avant déblocage du prêt

Conseil :

Toujours vérifier que l'application est agréée par la BCEAO ou les autorités locales.

La réalisation de ce livre blanc a été rendue possible grâce au soutien,

REMERCIEMENTS

à l'inspiration et à la collaboration de nombreuses personnes et institutions. Je tiens à exprimer ma profonde gratitude envers :

- **Son Excellence Monsieur Bassirou Diomaye Faye, Président de la République du Sénégal**, pour sa vision éclairée en matière de transformation numérique et son engagement en faveur d'une cybersécurité renforcée.
- **Monsieur Ousmane Sonko, Premier Ministre du Sénégal**, pour sa foi et son engagement dans le domaine numérique, digital et cybersécurité.
- **Monsieur El Malick Ndiaye, Président de l'Assemblée nationale du Sénégal**, pour son engagement à renforcer le cadre législatif en matière de numérique, de cybersécurité et de protection des données, contribuant ainsi à asseoir une gouvernance numérique efficace et souveraine.
- **Monsieur Oumar Samba BA, Ministre Secrétaire général de la Présidence de la République**, pour sa vision, son leadership éclairé et son engagement constant en faveur de la transformation numérique, de la modernisation de l'administration et du renforcement de la gouvernance stratégique de l'État du Sénégal.
- **Monseigneur André Guèye**, Archevêque métropolitain de Dakar, pour ses prières, ses conseils avisés et son engagement constant en faveur de la paix, du dialogue et de la promotion de l'éthique dans la société sénégalaise.

- **Les Khalifes généraux des confréries musulmanes du Sénégal** (Tidiane, Mouride, Khadre, Layène, Niassène), pour leurs prières, leurs bénédictions et leur engagement constant en faveur de la paix sociale, de la cohésion nationale et de la promotion de l'éthique dans notre société.
- **Monsieur Alioune Sall, Ministre de la Communication, des Télécommunications et de l'Économie Numérique**, pour son leadership dans le développement du secteur numérique sénégalais.
- **Monsieur Isidore Diouf, Directeur de Sénégal Numérique**, pour son dévouement à l'amélioration des services publics numériques.
- **Monsieur Ousmane Thiongane, Président de la Commission de Protection des Données Personnelles (CDP)**, pour son engagement à garantir la protection des données personnelles au Sénégal.
- **Monsieur Sékou Dramé, pour son leadership à la tête de SONATEL** et son accompagnement constant sur les enjeux de cybersécurité, de connectivité et d'innovation numérique, et à **Monsieur Brelotte Ba, nouveau Directeur Général**, nos vœux de succès pour une continuité porteuse d'impact et de progrès.
- **Monsieur Dahirou THIAM Directeur Général L'Autorité de Régulation des Télécommunications et des Postes (ARTP)**, pour ses ressources, son expertise et ses éclairages réglementaires essentiels au développement d'un cyberspace sécurisé.
- **Monsieur Ibrahima Nour Eddine Diagne, Administrateur Général de GAINDE 2000**, pour ses initiatives pionnières en matière de dématérialisation, de e-gouvernance et de promotion de la confiance numérique au Sénégal et en Afrique.
- **Docteur Babacar Ndaw**, pour le travail accompli à la tête

de la Direction du Chiffrement et de la Sécurité des Systèmes d'Information (DCSSI), et au **Colonel Aly Mime**, qui lui succède, nos remerciements et nos encouragements pour poursuivre, avec engagement et rigueur, les efforts de renforcement de la souveraineté numérique du Sénégal..

- **Monsieur Jean Baptiste Tine**, Ministre de l'Intérieur et de la Sécurité publique, pour son action déterminée en faveur de la sécurité nationale, de la protection des infrastructures critiques et de la lutte contre la cybercriminalité.
- **Général de Corps d'Armée Général Mbaye CISSE, Chef d'État-major général des Armées**, pour son engagement stratégique à intégrer la cybersécurité et la cyberdéfense dans les dispositifs de défense nationale, renforçant ainsi la résilience du territoire numérique sénégalais.
- **Général de Division Martin Faye**, Haut Commandant de la Gendarmerie nationale et Directeur de la Justice militaire, pour ses actions déterminantes dans la sécurisation des espaces numériques, la lutte contre la cybercriminalité et le maintien de l'ordre dans un contexte numérique en mutation.
- **À l'ensemble des membres du Gouvernement du Sénégal**, pour leur engagement constant en faveur de la transformation numérique du pays, leur soutien aux initiatives de cybersécurité et leur volonté de bâtir un écosystème numérique inclusif, résilient et souverain.
- **À l'ensemble des acteurs de l'écosystème numérique sénégalais**, notamment les professionnels de l'IT, les chercheurs, les universitaires, les entrepreneurs du digital, les membres de la société civile, les communautés techniques, les associations, les start-ups, ainsi que les institutions publiques et privées engagées, pour leurs contributions inestimables au développement d'un cyberspace innovant, résilient et souverain.

Je tiens à adresser mes remerciements les plus sincères à toutes les personnes qui, par leur présence, leur soutien ou leurs conseils, ont contribué à ce travail :

- Tous les membres de ma famille.
- Ma mère Madame Dacosta - Arenise Mendy et ma marraine Madame Mendy – Caroline Mendy, pour leur amour inconditionnel et leurs encouragements constants.
- Monsieur et Madame Mendy - Papis & Maguy : pour leur soutien et leur accompagnement au quotidien.
- Monsieur et Madame Mendy - François & Caroline : pour leur soutien et leur accompagnement au quotidien.
- Monsieur et Madame Mendy - Emmanuel & Madeleine : pour leur soutien et leur accompagnement au quotidien.
- Monsieur et Madame Ndecky - Alexy & Elisabeth : pour leur soutien et leur accompagnement au quotidien.
- Mes frères (José, Emiliano et Benjamin Dacosta) et ma sœur (Rebecca Dacosta), pour leur soutien moral et leur énergie qui me porte.
- Mes oncles, tantes, cousins et cousines, pour leur appui constant.
- Monsieur et Madame Kanfom, pour la confiance qu'ils ont placée en moi.
- Monsieur Félix Corneille M. Minyem pour son accompagnement et ses conseils.
- Madame Aminata Sawadogo, pour son assistance précieuse durant la rédaction du livre.
- Madame Adja Fatou Kane Dia , pour le respect et la considération.
- Monsieur Papis Tandiag , pour le soutien moral et l'accompagnement.
- Monsieur Babou Sarr , pour le soutien et les conseils.
- Monsieur Mamadou Ndiaye alias Boston , pour le soutien , la suivie et l'accompagnement.
- Madame Cécile Antoinette Basse et Madame Mariama Ndiaye pour le soutien.
- Monsieur El Hadji Ibrahima Diago pour ses réalisations (wolotech) et son soutien
- Monsieur Ibrahima Coundié Ndiaye , pour la confiance et le support.

- Monsieur Bamba Sall , pour le soutien et l'accompagnement.
- Monsieur Bamba Faye , pour son implication dans la réussite de la culture de la cybersécurité au Sénégal.
- Monsieur Tony Mancabo , pour tout ton engagement dans le domaine cyber.
- Adjudant de Police Codé Touré , spécialiste en cybersécurité , pour l'accompagnement et l'effort de sécuriser notre cyberspace.
- Monsieur Clement Domingo alias Saxx , pour cette sensibilisation de masse de tous les jours.
- Tous mes mentors, pour leurs orientations déterminantes et leurs conseils éclairés.
- Le Colonel (er) Ibrahima Diouf, mon mentor, pour ses conseils lucides et son indéfectible soutien tout au long de mon parcours.
- Monsieur Youssef Khill, pour m'avoir guidé et soutenu sans faille dans le milieu informatique.
- Monsieur Mohamadou Mbengue, pour son accompagnement constant dans mes projets.
- Monsieur Hoballah Saadeck, pour cette confiance placée en moi.
- Monsieur Basile Niane, pour son engagement dans la promotion du numérique au Sénégal.
- Madame Jaly Badiane, une dame de fer, merci pour tes prises de position et ton accompagnement.
- Madame Salimata Diallo, merci pour le soutien et l'accompagnement.
- Monsieur Abdou Karim Pouye, pour avoir toujours été là pour me soutenir.
- Monsieur Mame Mané Diop, pour m'avoir initié à la cybersécurité et aidé à m'orienter.
- Monsieur Souleymane Touré , pour l'encadrement et le soutien.
- Monsieur Amdy Moustapha Sène, pour avoir été mon tout premier mentor et un ami fidèle dans le domaine.
- Monsieur Mamadou Faty, pour ses conseils précieux et son impact dans ma vie professionnelle.
- Monsieur Mortalla Gueye, mon jumeau de parcours et véritable source de motivation.

- Monsieur Bentaleb SOW, pour sa sincérité, son respect et son patriotisme exemplaire.
- Madame Racky Sèye, pour tout le soutien et l'accompagnement.
- Monsieur Cheikh Ahmadou Bamba Fall , pour le soutien et les conseils.
- Monsieur Algor Bengeloum, pour l'accompagnement.
- Mes camarades de promotion, amis et connaissances, pour les moments inoubliables partagés et leur contribution à mon épanouissement personnel et professionnel.
- À toute l'équipe d'IT4LIFE, en particulier le fondateur Sébastien Kuszniér et le DG Stéphane Margerit, pour la confiance qu'ils m'ont accordée.
- Les membres des communautés rootSN, Daara IT, et toutes les autres communautés que je fréquente, pour leur esprit de partage et leur engagement technologique.
- Toutes les communautés et associations de Saint Paul, notamment la Génération Scout 2000, où j'ai appris la vie en commun, le don de soi et le service à la patrie.
- Monsieur Mouhamadou Sall, pour l'honneur de m'avoir confié la responsabilité du premier centre BTS Cybersécurité du Sénégal.
- Madame Issatou Barry pour le soutien et la confiance.
- Monsieur Baidy Sy, pour son accompagnement professionnel et sa fraternité.
- Professeur Djiby Sow, pour sa rigueur et sa passion transmise pour les sciences et la technologie.
- Monsieur Thindella Kébé, pour son encadrement pendant mes stages et son professionnalisme.
- Monsieur Mamadou Wade Diop , pour votre engagement dans le milieu cyber et technologie émergentes.
- Monsieur Mamadou Dieng , pour le soutien et l'accompagnement.
- Monsieur Souleymane Diouf , pour le soutien et l'amitié.
- Monsieur Maurice Diouf , pour le soutien et l'accompagnement.
- Monsieur Ben Montero , pour le soutien ,
- Madame Bitty Diouf Ndiaye , pour la confiance et le soutien.
- Madame Fatimatou Binetou Ndiaye , pour le soutien et la confiance.
- Madame Khady Diouf , pour la confiance et l'accompagnement.

- Monsieur Aziz Gueye , pour m’avoir bien formé en cybersécurité durant mes périodes de stages.
- Monsieur Aboubacar Sidiki Yalcouyé ,pour le soutien.
- Colonel Aly Mime, mon conseiller discret et guide éclairé.
- Madame Thiara Loume, pour son soutien moral constant et d’avoir fait de moi le parrain de son fils.
- Monsieur Mamadou Ndiaye , pour la vulgarisation du numérique dans la langue wolof.
- Capitaine Albert Mendy, pour son soutien et conseils
- Madame Lil Lina Ndior pour ces conseils
- Madame Ndéye Marie Aïda ndiéguène pour son soutien et tout ce qu’elle fait pour le Sénégal
- Monsieur Serigne Mouhamadane Diop, pour le soutien et les conseils
- Monsieur François Marena pour son soutien.
- Madame Merry Beye , pour la vulgarisation du numérique au Sénégal à travers les langues locales.
- Monsieur Abdoulaye Ly alais Berger Hightech, pour tout cet effort et l’amour que tu mets chaque jour à la vulgarisation du numérique au Sénégal, en Afrique et partout dans le monde.
- Monsieur Samba Kane alias Bathie Drizzy , pour les conseils avisés en ligne.
- Monsieur Abraham D. Montang Sadio, pour son appui quotidien et sa contribution à mes projets.
- Madame Mariétou Diedhiou, pour sa présence indéfectible dans tous mes projets.
- Monsieur Ousmane Gueye, pour son travail remarquable dans le domaine numérique.
- Monsieur Mamadou Diouf (PMD), pour son accompagnement bienveillant.
- Monsieur Amadou Mactar Coly, pour son aide et son engagement.
- Monsieur Bachir Lo , pour tout l’accompagnement.
- Monsieur Nestor Mendy , pour votre accompagnement.
- Monsieur Oumar Diallo, pour son action au service de la jeunesse dans l’écosystème numérique.

- Monsieur Mamadou Diallo, pour son expertise et son soutien.
- Monsieur Mamadou Diagne, pour sa confiance inestimable.
- Monsieur Abdoulaye Kébé, pour son professionnalisme et son soutien continu.
- Madame Mbathio Kama, pour son accompagnement attentif et son écoute.
- Commissaire Gueye, pour être mon pilier dans le domaine de la cybersécurité, à la fois conseiller et formateur.
- Commissaire Katim Touré, pour la confiance et l'accompagnement.
- Monsieur Abdou Khadre Mbengue, mon grand frère et mentor, pour ses conseils avisés.
- Dr Ousmane Ndiaye, pour son action déterminante dans le secteur.
- Monsieur Amadou Baro, pour son rôle de guide en cybersécurité.
- Massamba Lô, pour son soutien constant dans ma progression.
- Monsieur Abdou Aziz Ndiaye, mon bras droit, pour sa loyauté et son efficacité.
- Monsieur Bamba Bathily, pour tous les efforts de sensibilisation que tu fais pour ton pays et toute l'Afrique.
- Monsieur Ibrahima Mbodji, pour l'aide, les conseils et l'accompagnement.
- Madame Viviane Mendy pour son soutien.
- Madame Ndeye Astou Diongue pour son soutien.
- Madame Dior Gueye, pour sa générosité et son soutien désintéressé.
- Madame Balkissa Ahmadou, «la reine de LinkedIn», pour son inspiration et son leadership.
- Madame Maguette Ba, pour sa motivation et sa fidélité dans le domaine.
- Monsieur Youssef Destefani, mon frère et mentor dans la cybersécurité.
- Monsieur Saliou Thiam, ami fidèle, pour son appui de toujours.
- Monsieur Kamal Touré, pour tout cet effort en matière de lutte contre la cybercriminalité dans le monde.
- Monsieur Samba Sidibé, mentor de l'ombre, pour son soutien discret.
- Monsieur Samba Kane, pour son amitié et son accompagnement sans faille.

- Madame Aida Diop, grande Dame, pour son appui constant.
- Monsieur Moussa Sall , pour tout l'accompagnement et tes contributions pour un cyberspace sûr.
- Monsieur Abdourahmane Guèye , pour ton professionnalisme et tout ce que tu fais comme formation en cybersécurité pour les jeunes.
- Madame Martine Ndéo Diouf , pour cette sensibilisation en ligne portant sur la protection des données personnelles.
- Monsieur Mouhammad Ciss , pour cet accompagnement et soutien dans tous mes projets.
- Madame Gnagna Diène, pour son soutien quotidien.
- Madame Pélagie Olga Sène, pour son accompagnement fidèle.
- Monsieur Chérif Diallo, pour son aide continue dans mes projets personnels.
- Monsieur Thierno Ousmane Ba, pour sa confiance et son soutien.
- Monsieur Moussa Diedhiou, pour son assistance.
- Monsieur Mohamed Boye, pour son accompagnement.
- Monsieur Massamba Lo, pour sa protection et son rôle de mentor.
- Monsieur Samba Souaré, pour sa confiance et son soutien.
- Monsieur Etienne Diémé, pour sa foi en moi.
- Monsieur Valeri Pallawoh , pour le soutien et la confiance.
- Monsieur Mamadou Deer , pour le soutien et l'accompagnement.
- Monsieur Assane Sy , pour les efforts de sensibilisation.
- Monsieur Emmanuel Diokh , pour les missions de sensibilisation en matière de cyberlois.
- Monsieur Birame Ndour , pour le soutien indéfectible.
- Monsieur Souleymane Ngom , pour ton engagement et ta participation à la formation des jeunes dans le domaine numérique.
- Monsieur Dominique Mendy , pour être mon parrain et mon conseiller.
- Monsieur Cheikh Ameth Tidiane Touré , pour toute la confiance placée en moi.
- Monsieur Mamadou Lamine Diop , pour son soutien et son professionnalisme.
- Monsieur Mohamed Amar Athie, pour son accompagnement précieux.

- Monsieur Nicolas Diémé , pour le soutien et l'accompagnement.
- Monsieur Thomas Mendy , pour avoir fait partie de ceux qui m'ont formé dès le bas âge.
- Monsieur Gervais Mendy , pour tout ce que tu fais dans le domaine IT.
- Monsieur Alex Corenthin , pour avoir été l'un des pionniers de la tech au Sénégal.
- Madame Jeanne Roux Bilong , pour toute la confiance placée en moi.
- Monsieur Samuel Ouya , pour tout ce que vous faites dans le domaine.
- Dr Latyr Ndiaye , pour les opportunités et la confiance.
- Monsieur et Madame Sambou, pour l'honneur de m'avoir choisi comme parrain de leur fils.
- Monsieur Bara Diaw , pour ton temps que tu mets au service de la formation des jeunes du pays.
- Madame Anta Dieng , pour sa confiance et son soutien.
- Monsieur Abib Sultan Ndoye , pour l'accompagnement et le soutien.
- Madame Banel Sow, pour ses conseils et son soutien.
- Madame Martine Ndéo Diouf, pour son soutien et ses conseils.
- Madame Astou Diouf, pour l'accompagnement.
- Monsieur Mountaga Cissé , pour le soutien et l'accompagnement.
- Monsieur Demba Gueye pour son engagement et ses actions dans l'écosystème numérique.
- Monsieur Mouhammad Cissé, pour le soutien.
- Madame Faye , Joanna , pour son accompagnement, son soutien et ces conseils.
- La famille Damas-Sambou, notamment Madame Emilie Sambou, son Mari Charles Sambou et son fils Jean-Paul Dady Damas Sambou, pour leurs soutiens et conseils dans les moments difficiles.
- Mes filleules , pour le soutien moral et le bonheur que vous me procurait.
- Tous les membres de l'Association Africaine des Droits Numériques, pour leur expertise en matière de cyberdroit et de protection des données personnelles.

- Toute l'équipe de Kaay Job, pour leur soutien et leur implication dans la promotion du livre blanc.
- Les directeurs d'universités IT et les responsables de filières qui m'ont accordé leur confiance, ainsi que mes étudiants pour leur engagement et leur soif d'apprendre.
- Mes étudiants des différents IT-Schools, pour leur respect, leur écoute et leur patience.
- Le groupe Chambre 22, pour leur implication dans le développement de la cybersécurité.
- La team CONELSI, pour leur engagement dans la cyberprotection au Sénégal.
- La team GFM (Global Fraud Management), pour leur rôle dans la sécurisation du secteur bancaire, monétique et télécom.
- Mes lecteurs et les membres de mon réseau, pour leur fidélité et leurs retours constructifs, qui ont nourri et enrichi ce travail.
- Ma paroisse Saint Paul de Grand-Yoff, pour avoir été ma source spirituelle, mon ancrage dans la foi et pour m'avoir donné un lieu d'apprentissage de la vie d'un bon chrétien, des valeurs de service, de partage et de responsabilité.
- Toutes les paroisses du Sénégal, pour leur rôle essentiel dans l'accompagnement spirituel, moral et communautaire des fidèles, et pour leur contribution à l'éducation, à la paix et à la cohésion dans notre société.
- Aux universités et écoles supérieures dans lesquelles j'ai eu l'honneur d'enseigner ou fait office de membre du jury durant les soutenances, pour la confiance accordée et pour leur contribution à la formation de la prochaine génération d'experts en cybersécurité.

À toutes celles et tous ceux que j'ai cités ou non, je tiens à exprimer ma profonde reconnaissance.

- Monsieur Nicolas Diémé , pour le soutien et l'accompagnement.
- Monsieur Thomas Mendy , pour avoir fait partie de ceux qui m'ont formé dès le bas âge.
- Monsieur Gervais Mendy , pour tout ce que tu fais dans le domaine IT.
- Monsieur Alex Corenthin , pour avoir été l'un des pionniers de la tech au Sénégal.
- Madame Jeanne Roux Bilong , pour toute la confiance placée en moi.
- Monsieur Samuel Ouya , pour tout ce que vous faites dans le domaine.
- Dr Latyr Ndiaye , pour les opportunités et la confiance.
- Monsieur et Madame Sambou, pour l'honneur de m'avoir choisi comme parrain de leur fils.
- Monsieur Bara Diaw , pour ton temps que tu mets au service de la formation des jeunes du pays.
- Madame Anta Dieng , pour sa confiance et son soutien.
- Monsieur Abib Sultan Ndoye , pour l'accompagnement et le soutien.
- Madame Banel Sow, pour ses conseils et son soutien.
- Madame Martine Ndéo Diouf, pour son soutien et ses conseils.
- Madame Astou Diouf, pour l'accompagnement.
- Monsieur Mountaga Cissé , pour le soutien et l'accompagnement.
- Monsieur Demba Gueye pour son engagement et ses actions dans l'écosystème numérique.
- Monsieur Mouhammad Cissé, pour le soutien.
- Madame Faye , Joanna , pour son accompagnement, son soutien et ces conseils.
- La famille Damas-Sambou, notamment Madame Emilie Sambou, son Mari Charles Sambou et son fils Jean-Paul Dady Damas Sambou, pour leurs soutiens et conseils dans les moments difficiles.
- Mes filleules , pour le soutien moral et le bonheur que vous me procurait.
- Tous les membres de l'Association Africaine des Droits Numériques, pour leur expertise en matière de cyberdroit et de protection des données personnelles.

- Toute l'équipe de Kaay Job, pour leur soutien et leur implication dans la promotion du livre blanc.
- Les directeurs d'universités IT et les responsables de filières qui m'ont accordé leur confiance, ainsi que mes étudiants pour leur engagement et leur soif d'apprendre.
- Mes étudiants des différents IT-Schools, pour leur respect, leur écoute et leur patience.
- Le groupe Chambre 22, pour leur implication dans le développement de la cybersécurité.
- La team CONELSI, pour leur engagement dans la cyberprotection au Sénégal.
- La team GFM (Global Fraud Management), pour leur rôle dans la sécurisation du secteur bancaire, monétique et télécom.
- Mes lecteurs et les membres de mon réseau, pour leur fidélité et leurs retours constructifs, qui ont nourri et enrichi ce travail.
- Ma paroisse Saint Paul de Grand-Yoff, pour avoir été ma source spirituelle, mon ancrage dans la foi et pour m'avoir donné un lieu d'apprentissage de la vie d'un bon chrétien, des valeurs de service, de partage et de responsabilité.
- Toutes les paroisses du Sénégal, pour leur rôle essentiel dans l'accompagnement spirituel, moral et communautaire des fidèles, et pour leur contribution à l'éducation, à la paix et à la cohésion dans notre société.
- Aux universités et écoles supérieures dans lesquelles j'ai eu l'honneur d'enseigner ou fait office de membre du jury durant les soutenances, pour la confiance accordée et pour leur contribution à la formation de la prochaine génération d'experts en cybersécurité.
- À Monsieur et Madame Ndong (Léopold et Mamie) pour le soutien et la confiance.
- À mes frères et soeurs du quartier, merci beaucoup pour le soutien.
- À tout le quartier de Taïba 2, merci beaucoup pour le soutien.
- À toutes celles et tous ceux que j'ai cités ou non, je tiens à exprimer ma profonde reconnaissance.

REMERCIEMENTS SPÉCIAUX

Ce livre blanc n'est pas le fruit d'un travail solitaire. Il est le reflet de nombreux échanges, relectures, conseils et regards bienveillants, sans lesquels ce projet n'aurait pas pu aboutir sous cette forme.

Je tiens à exprimer ma gratitude à :

- Monsieur Pape Fodé Dramé (Juriste droit du numérique - Co-auteur de l'ouvrage [L'Impact du Rgpd en Afrique](#) - Délégué à la Protection des données & Président de l'Association Africaine des Droits Numériques (ADN)): pour ses relectures précieuses, la rédaction de la préface et ses suggestions toujours justes¹⁵.
- Colonel (er) Ibrahima Diouf (Cyber Colonel de l'armée Sénégalaise à la retraite et IT Trainer): pour ses suggestions et critiques constructifs.
- Monsieur Daouda Diagne (Expert en Cybersécurité et en Gouvernance Numérique) : pour son soutien, relecture, suggestions et amélioration du contenu.
- Madame Aminata Sawadogo (juriste en droit des affaires et du numérique): pour avoir corrigé le document et apporté des critiques constructives.
- Madame Dieynaba Tandiang (Journaliste): pour son temps précieux qui a servi à corriger et mettre en forme tout le document .
- Monsieur Aboubacar Sadikh Ndiaye (Expert/Consultant en stratégie de Transformation digitale et Intelligence Artificielle): pour l'accompagnement à la finalisation de la rédaction du document.

- Monsieur Souleymane Macalou CISSE (Professeur de français et d'Histoire-Géographie): pour la relecture et la correction de tout le document.
- Monsieur José Dacosta (Développeur Full Stack) : pour le soutien fraternel et la refonte de la page du site pour la publication du livre .
- Monsieur Guilaye Tine (Consultant en Design et Transformation Digital, CEO Arte-Fakt) : pour son soutien, accompagnement et design du livre.
- Monsieur Ousseynou Diop (CEO Xarala et Développeur web & Mobil): pour l'accompagnement et la maintenance du site de publication du livre.
- Madame Nadine Kanfom (Experte en QOS): À mon ombre bienveillante, pour ses précieux conseils, son soutien constant, sa relecture et ses suggestions éclairées.
- Monsieur Cyprien Andrew Sadio (Software Engineer et Entrepreneur) : Merci d'avoir challenger le document de par tes questions, suggestions et critiques.
- Monsieur Chiekh Ahmadou Bamba Ndiaye (User Experience Designer) : Merci pour le teaser et l'accompagnement, toujours là quand j'ai besoin de toi.
- Papa Samba Traoré (Freelance spécialisé en ingénierie logiciel) : pour la réactivité et le support qui ont contribué à la finalisation du livre.

À toutes celles et ceux qui, de près ou de loin, ont contribué à faire mûrir mes idées, à les confronter au réel, à les clarifier ou à les enrichir : MERCI INFINIMENT !!!

SOURCES

A. BIBLIOGRAPHIE

1. Ressources nationales (Sénégal)

- **TOURÉ, Papa Assane.** *Le traitement de la cybercriminalité devant le juge : l'exemple du Sénégal.* Dakar : L'Harmattan, 2014
- **TOURÉ, Papa Assane.** *Cybercriminalité : Enjeux et perspectives pour le Sénégal.* Dakar : L'Harmattan Sénégal, 2016.
- **LO, Mouhamadou.** *La protection des données à caractère personnel en Afrique : réglementation et régulation.* Dakar : Baol Éditions, 2017.
- **GUEYE, Papa.** *Criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles.* Dakar : L'Harmattan Sénégal, 2018.
- **SY, Baidy.** *Livre Blanc sur la cybersécurité au Sénégal.* Dakar : L'Harmattan Sénégal, 2019.
- **TOURÉ, Papa Assane.** *Cybercriminalité : Code pénal et textes pénaux spéciaux commentés et annotés.* Dakar : L'Harmattan Sénégal, 2023.
- **DRAME, Pape Fodé & SARR, Rokhaya,** *L'impact du RGPD en Afrique:* L'Harmattan Sénégal, 2021.
- Loi n°2008-11 relative à la cybercriminalité.
- Loi n°2008-12 relative à la protection des données personnelles.
- Loi n°2008-08 sur les transactions électroniques.
- Politique de Sécurité des Systèmes d'Information (PSSI).
- Stratégie nationale de cybersécurité (SNC2022).
- Stratégie Sénégal Numérique 2025-2035.

2. Ressources régionales (Afrique)

- **Union Africaine :** Convention de Malabo sur la cybersécurité et la protection des données personnelles, 2014.

- **CEDEAO** : Directive C/DIR.1/08/11 relative à la lutte contre la cybercriminalité en Afrique de l’Ouest, 2011.
- **Conseil de l’Europe** : Convention 108+ sur la protection des données, 2018.

3. Ressources internationales

- **ISO/IEC 27001** : Technologies de l’information — Techniques de sécurité — Systèmes de management de la sécurité de l’information — Exigences, 2013.
- **NIST** : *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1. Gaithersburg (USA) : National Institute of Standards and Technology, 2018.
- **ENISA** : *Threat Landscape Report*. European Union Agency for Cybersecurity, 2022.
- **MITRE ATT&CK** : *Knowledge base of adversary tactics and techniques*. [En ligne] <https://attack.mitre.org>

B. WEBOGRAPHIE

1. Ressources nationales (Sénégal)

- Sénégal Numérique (ex-ADIE) : <https://www.adie.sn>
- Commission des Données Personnelles (CDP) : <https://www.cdp.sn>
- Autorité de Régulation des Télécommunications et des Postes (ARTP) : <https://www.artp.sn>
- Direction de la Cybersécurité (DCSSI) : <https://stec-ssi.sn>
- Présidence de la République du Sénégal : <https://www.presidence.sn>
- Gouvernement du Sénégal (Primature) : <https://primature.sn>

- Le Monde Du Numérique (blog) : <https://lemondedunumerique.com>
- Nu Jang Informatique : <https://nujanginformatique.sn>
- Plateforme E-Learning Nu Jang: <https://www.nujang.com>
- **Association Africaine des Droits Numériques (ADN)**, *Plaidoyer pour une réforme approfondie de la protection des données au Sénégal* : https://www.pressafrik.com/TRIBUNE-pour-une-reforme-en-profondeur-du-dispositif-senegalais-de-la-protection-des-donnees-a-caractere-personnel_a272913.html

2. Ressources régionales (Afrique)

- Smart Africa: <https://smartafrica.org>
- AfricaCERT : <https://africacert.org>
- CIPESA: <https://cipesa.org>
- Paradigm Initiative : <https://paradigmhq.org>

3. Ressources internationales

- The Hacker News : <https://thehackernews.com>
- DarkReading : <https://www.darkreading.com>
- Wired Security : <https://www.wired.com>
- ZDNet Cybersecurity : <https://www.zdnet.com/topic/security>

PRÉCAUTION D'USAGE

Ce document a été structuré et relu avec l'appui de l'intelligence artificielle ChatGPT, développé par OpenAI.

J'ai fourni l'ensemble des idées, réflexions, exemples concrets et solutions, que le robot assistant a aidé à organiser, corriger et proposer des exemples de plan. Aucune génération automatique de contenu brut n'a été utilisée.

Les images qui se trouvent dans le document sont générées par l'assistant IA sous ma directive.

A cela s'ajoute que les images générées par l'IA ne bénéficient pas automatiquement d'une protection par le droit d'auteur, car elles ne résultent pas directement d'une création humaine.

En définitive, je ne détiens aucun droit d'auteur sur ces images et ne suis donc pas en mesure d'en autoriser les réutilisations.

PRÉSENTATION DE L'AUTEUR



M. Gérard Joseph Francisco DACOSTA alias #rootSN

Je me nomme Gérard Joseph Francisco DACOSTA, ingénieur en cybersécurité spécialisé en Management de la Sécurité des Systèmes d'Information (MSSI). Je cumule 10 ans d'expérience dans les domaines des réseaux, des systèmes et de la sécurité informatique, avec une passion profonde pour la formation, la sensibilisation et l'accompagnement des entreprises dans leurs enjeux numériques.

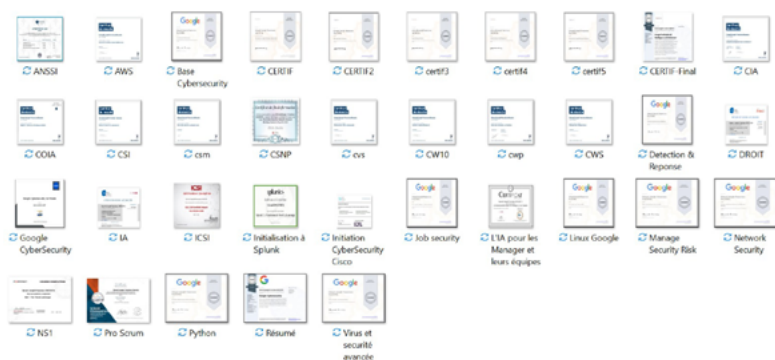
Actuellement, je suis Responsable du Pôle Infrastructure chez IT4LIFE, consultant en cybersécurité, et formateur dans plusieurs écoles IT au Sénégal, telles que ISI, UCAO, HEMI, SUPDECO, ECPI, ITSCHOOL-CITS, ESMT , IIBS pour ne citer que cela.

En parallèle, je suis cofondateur et CEO de Nu Jang Informatique, une EdTech spécialisée dans la création de contenu IT, la formation pratique, et l'accessibilité numérique en Afrique.

J'ai eu l'honneur, au fil des années, d'être distingué à plusieurs reprises :

- En 2024, j'ai eu l'honneur de recevoir un trophée devant toute la communauté Manjak, en reconnaissance de mon engagement et de mes actions dans le domaine de la cybersécurité, qui contribuent à faire rayonner notre identité et nos valeurs.
- En 2023, j'ai été nommé président de centre pour le tout premier examen national de BTS en cybersécurité au Sénégal, une responsabilité symbolique de la reconnaissance de mon engagement dans la formation des jeunes talents.
- En 2022, j'ai été sélectionné, aux côtés de quatre autres jeunes, par l'Ambassade de l'Inde au Sénégal dans le cadre du projet Gen Next Democracy. Cette initiative visait à nous faire découvrir non seulement la richesse culturelle de l'Inde, mais aussi ses avancées scientifiques et technologiques. Il s'agissait de la première expédition de jeunes issus de pays francophones, jusqu'à exclusivement réservée aux participants des pays anglophones.
- La même année, j'ai eu l'honneur d'être élu Citoyen Modèle dans la catégorie IT par le Club Modèle, une distinction saluant mon parcours et mes contributions dans le domaine du numérique.
- En 2019, j'ai été lauréat du challenge panafricain "L'Afrique c'est Chic - 2063", récompensant ma vision prospective pour un continent africain résilient, innovant et souverain à l'horizon 2063.

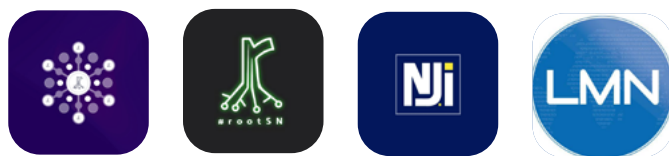
Je suis également titulaire de plus de 35 attestations et certifications internationales dans des domaines clés tels que le cloud, la cybersécurité offensive et défensive, les réseaux et systèmes, la gestion de projets, l'architecture IT, et bien d'autres.



Mon engagement communautaire se manifeste à travers la communauté Daara IT et la communauté rootSN, que j’ai cofondée, mais aussi à travers mon blog «lemondedunumerique.com», dédié à la vulgarisation technologique sur le continent.

Enfin, je multiplie les interventions dans les médias, webinaires et forums professionnels, pour porter la voix d’une Afrique numérique, souveraine et résiliente.

Ma mission est simple mais ambitieuse : rendre le numérique plus accessible, plus sécurisé, et plus inclusif pour tous.



Ma phrase préférée: **“Sur Internet, rien n’est vraiment gratuit. Si c’est gratuit, dans la plupart des cas... c’est vous le produit.”**

CONTACTS ET RETOURS

Vos retours comptent !

Vous avez des suggestions, corrections, ou tout simplement l'envie de contribuer à enrichir cette réflexion collective ?

Je suis à votre écoute à travers ce formulaire :

<https://forms.gle/ffXkicYnp0BsZFBR6>



Politique de confidentialité et protection des données personnelles

«Je m'engage à protéger votre vie privée. En renseignant votre adresse e-mail pour recevoir le livre blanc et en envoyant éventuellement vos suggestions ou commentaires via les contacts ci-dessous, vous m'autorisez à stocker et traiter vos données personnelles afin de vous fournir le contenu demandé. Conformément à la LCPD, vous disposez d'un droit d'accès, de rectification, et d'opposition au traitement de vos données personnelles. Pour exercer ce droit, veuillez me contacter via les coordonnées mentionnées ci-dessus.»

Ci-après les différents contacts :

- **Mail :** gdacosta@nujanginformatique.com
- **Tel :** 00221 77 328 98 61
- **Linkedin :** <https://www.linkedin.com/in/g%C3%A9rard-joseph-francisco-dacosta-49865a155/>
- **Facebook :**
<https://www.facebook.com/share/1687CEcRop/?mibextid=wwXIf>
- **Twitter :** @DacostaGerard

Merci de votre collaboration et de votre engagement pour un cyberspace plus sûr et souverain.

RÉSUMÉ DU LIVRE BLANC

Ce Livre Blanc a pour objectif d'informer sur la cybersécurité et la souveraineté numérique au Sénégal. A cette fin, il dresse un état des lieux sans concession du cyberspace sénégalais, analysant d'emblée le cadre juridique, institutionnel, et technologique mis en place pour garantir sa sécurité.

Découvrez, au fil de la lecture, les différentes cybermenaces et les failles persistantes, accompagnées d'une chronologie des principales cyberattaques marquantes (2018 - 2025) ainsi que des mesures de réponse déployées.

L'analyse porte également sur la gouvernance institutionnelle de la cybersécurité, actuellement entravée par un manque de coordination stratégique et une sensibilisation encore insuffisante.

Les enjeux sont immenses et protéiformes. Il est donc essentiel de s'armer de solutions concrètes pour renforcer notre dispositif de cybersécurité, en s'appuyant notamment sur trois axes majeurs :

- La mise en place d'un nouveau modèle de gouvernance cyber (création d'une Haute Autorité de la Cybersécurité, renforcement de la cyberdéfense nationale, réforme de la protection des données personnelles);
- La modernisation ambitieuse du cadre légal, adaptée aux réalités contemporaines et aux nouveaux enjeux géostratégiques;
- L'élaboration d'un plan d'action structuré, en matière de formation, de sensibilisation, et de développement d'une véritable culture de cybersécurité à l'échelle nationale.

Ce livre s'enrichit aussi d'une autre partie très fournie, explorant:

- L'impact des technologies émergentes (IA, Blockchain, Cloud, Ordinateur quantique);
- Le New Deal technologique sénégalais:
- Un plaidoyer pour une réforme approfondie du cadre de protection des données au Sénégal et en Afrique, portée par l'Association Africaine des Droits Numériques (ADN);

À travers cet ouvrage, mon objectif est d'apporter, avec réalisme, un ensemble d'informations, de vulgarisations, d'analyses, d'éclairages et de perspectives, afin de contribuer à la construction d'un cyberspace sénégalais souverain, sécurisé et durable.

LIVRE BLANC SUR LA CYBERSÉ- CURITÉ ET LA SOUVERAINETÉ NUMÉRIQUE AU SÉNÉGAL

« Tendances de la cybercriminalité en 2025 au Sénégal: Vers un cyberspace sûr, souverain et durable? »

À l'heure où les cybermenaces se multiplient, ce Livre Blanc dresse un état des lieux sans concession du cyberspace sénégalais : cadre juridique, institutions, technologies, mais aussi failles persistantes, gouvernance insuffisante et chronologie des attaques marquantes de 2018 à 2025.

L'auteur propose des solutions concrètes articulées autour de trois piliers : une gouvernance rénovée, un cadre légal modernisé, et une stratégie nationale de sensibilisation et de formation.

L'ouvrage aborde également l'impact des technologies émergentes (IA, blockchain, cloud, quantique) et appelle à une réforme ambitieuse du système de protection des données personnelles, dans un plaidoyer porté par l'Association Africaine des Droits Numériques (ADN).

Un livre essentiel pour comprendre, agir et bâtir une Afrique numérique plus souveraine, plus sûre et plus résiliente.



À PROPOS DE L'AUTEUR

Gérard Joseph Francisco DACOSTA est ingénieur en cybersécurité option Management de la Sécurité des Systèmes d'Information (MSSI). Fort de 10 ans d'expérience dans les réseaux, systèmes et la cybersécurité, il est également IT Trainer, IT consultant, blogueur et CEO de Nu Jang Informatique.

Engagé dans la formation des jeunes talents et la promotion d'un numérique inclusif, il cumule plusieurs distinctions nationales et panafricaines. Il est aussi le cofondateur des communautés Daara IT et rootSN.

Citation :

“Sur Internet, rien n'est vraiment gratuit. Si c'est gratuit, dans la plupart des cas... c'est vous le produit.”

ISBN : 979-10-978269

© 2025 – Tous droits réservés

**Ce Livre Blanc n'est pas
destiné à la vente**

