

Intelligence Artificielle et Cybersécurité dans le secteur Éducatif au Niger : Enjeux et Perspectives.

Présenté par Abdoul Karim Mamani Malam Goga.

Niamey 09 - 03 - 2025.



SOMMAIRE

I. Introduction

II. L'Intelligence Artificielle dans l'Éducation

III. La Cybersécurité dans l'Éducation

IV. Cas pratique IA : Exploiter les LLM pour apprendre

V. Cas pratique Cybersécurité: Meilleures pratiques et Outils

VI. Conclusion



INTRODUCTION



INTRODUCTION



- 1. Contexte général**
- 2. Définition de l'Intelligence Artificielle**
- 3. Définition de la Cybersécurité**
- 4. État de la couverture réseau et de l'accès à Internet au Niger**

1. Contexte général

Les **technologies numériques** transforment profondément le **secteur éducatif** à travers le monde.

- ❑ **L'intelligence artificielle (IA)** améliore les méthodes d'enseignement et d'apprentissage.
- ❑ **La cybersécurité** devient un enjeu central pour protéger les données sensibles.

Au Niger, bien que le **développement du numérique** progresse et ouvre des opportunités pour **l'utilisation de l'IA**, plusieurs défis demeurent, tels que **l'insuffisance des infrastructures**, la **fracture numérique**, particulièrement dans les zones rurales, et l'augmentation des **menaces cybernétiques**.

Cette présentation vise à explorer les enjeux et perspectives de l'IA et de la cybersécurité dans l'éducation nigérienne.

2. Définition de l'Intelligence Artificielle



L'intelligence artificielle (IA) désigne un ensemble de technologies permettant à des machines d'exécuter des tâches qui nécessitent généralement l'intelligence humaine. Elle repose sur plusieurs techniques, notamment :

- ❑ **Le Machine Learning (apprentissage automatique)** : Permet aux machines d'apprendre à partir de données sans être explicitement programmées.
- ❑ **Le Traitement Automatique du Langage Naturel (NLP)** : Permet aux machines de comprendre, analyser et interpréter le langage naturel, tel que parlé ou écrit et générer des réponses.
- ❑ **La Vision par ordinateur** : Permet d'analyser et interpréter des images et vidéos.

Dans l'éducation, l'IA est utilisée pour **personnaliser l'apprentissage**, **proposer des tuteurs intelligents**, analyser les **performances des élèves** et optimiser les **ressources pédagogiques**.

3. Définition de la Cybersécurité

La cybersécurité regroupe l'ensemble des pratiques et technologies visant à protéger les systèmes informatiques, les réseaux et les données contre les cyberattaques.

Elle repose sur plusieurs principes :

- ❑ **Confidentialité** : Assurer que seules les personnes autorisées peuvent accéder aux données.
- ❑ **Intégrité** : Garantir que les informations ne sont pas altérées de manière malveillante.
- ❑ **Disponibilité** : Veiller à ce que les systèmes restent opérationnels malgré les menaces.

Dans le secteur éducatif, la cybersécurité est essentielle pour protéger les **plateformes de formation**, sécuriser les **données des étudiants et enseignants**, et prévenir les attaques contre les **systèmes éducatifs connectés**.

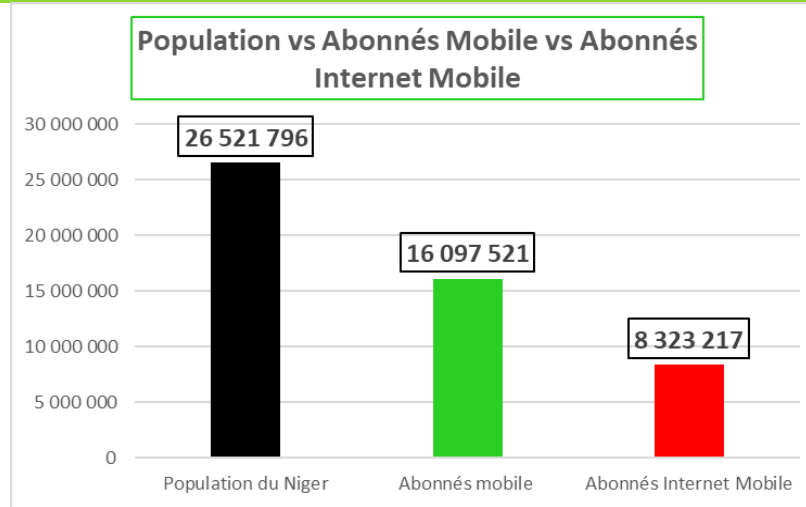
4. État de la couverture réseau et de l'accès à Internet au Niger



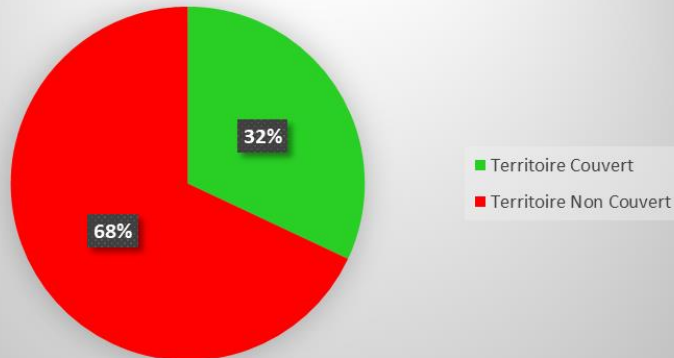
Selon l'Observatoire des Communications Électroniques de l'ARCEP, au 3 ème Trimestre 2024 :

- ❑ 16 097 521 d'abonnés mobile, soit 60,7 % de la population.
- ❑ 8 323 217 d'abonnés Internet mobile, 32 % de la population et 52 % des abonnés mobile.
- ❑ 32 % du territoire couvert, mais 76 % de la population a accès au réseau mobile **(données partielles sans Airtel pour la couverture géo et sans NT pour les deux couvertures)**.
- ❑ Plus de 8 milliards FCFA investis par (Airtel, Moov et Niger Télécom).
- ❑ Arrivée de STARLINK.

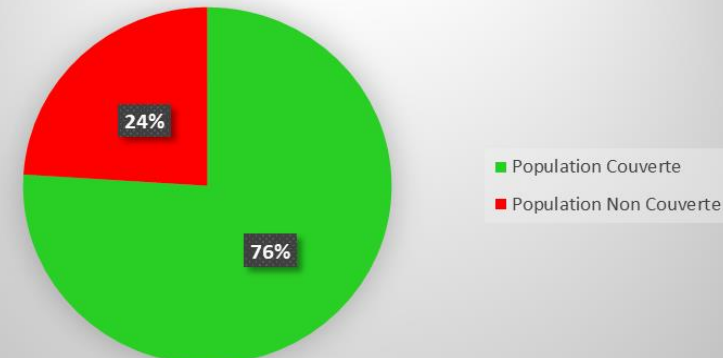
4. État de la couverture réseau et de l'accès à Internet au Niger



Couverture Géographique



Couverture Population



4. État de la couverture réseau et de l'accès à Internet au Niger



4.1 Points positifs :

- ❑ Bonne couverture réseau de la population (76%).
- ❑ Adoption croissante du numérique dans certaines écoles et universités.
- ❑ Initiatives gouvernementales pour la réduction de la fracture numérique :
 - Autorisation de Starlink , Projet Lire
 - PVI et toutes les actions de l'ANSI
 - Séminaire en Juillet 2024 organisé par l'ARCEP.

4.2 Défis :

- ❑ Accès limité à Internet, notamment en milieu rural (32 % population et 52 % abonnés mobile).
- ❑ Manque d'équipements numériques dans de nombreux établissements.
- ❑ Insuffisance de formations en IA et cybersécurité pour les enseignants et étudiants.
- ❑ Risques accrus de cyberattaques, avec une sensibilisation encore faible.

L'IA DANS L'ÉDUCATION AU NIGER



L'IA DANS L'ÉDUCATION AU NIGER



1. Enjeux de l'IA

2. Perspectives pour l'IA

1. Enjeux de l'IA dans l'éducation au Niger

L'intelligence artificielle (IA) représente une opportunité majeure pour moderniser l'éducation au Niger, mais son intégration soulève plusieurs défis.

1.1 Opportunités offertes par l'IA :

L'IA peut transformer positivement le système éducatif nigérien en améliorant :

- **L'apprentissage personnalisé** : Les algorithmes d'IA peuvent analyser les performances des élèves et proposer des contenus adaptés à leur niveau et style d'apprentissage.
- **L'automatisation des tâches répétitives** : Correction automatique des devoirs, génération de rapports pédagogiques et gestion administrative allégée.
- **L'accessibilité aux ressources pédagogiques** : Développement de tuteurs virtuels et assistants pédagogiques pour aider les élèves en dehors des heures de classe.
- **L'intégration des langues locales** : L'IA permet de créer des outils de traduction et d'apprentissage dans les langues nationales, facilitant l'éducation en zones rurales.

1. Enjeux de l'IA dans l'éducation au Niger



1.2 Défis dans l'adoption de l'IA :

Malgré ses bénéfices, plusieurs défis peuvent freiner l'adoption de l'IA dans l'éducation au Niger :

- **Manque de données pour l'apprentissage**
- **Manque d'infrastructures numériques.**
- **Pénurie de compétences en IA.**
- **Coût élevé des technologies IA.**
- **Dépendance aux solutions étrangères.**
- **Risque d'inégalités numériques.**

2. Perspectives pour l'IA dans l'éducation

Pour exploiter pleinement le potentiel de l'IA dans l'éducation au Niger, plusieurs actions stratégiques doivent être envisagées :

- **Lancer une large campagne de collecte de données :**

- Données sur les parcours éducatifs et pratiques pédagogiques.
- Données sur les élèves (forces, difficultés, performances, apprentissage).

- **Renforcer l'accès aux infrastructures numériques :**

- Étendre la couverture Internet dans les établissements scolaires, notamment en milieu rural.
- Encourager l'utilisation de matériels informatiques accessibles et adaptés au contexte nigérien.

- **Former enseignants et élèves à l'IA :**

- Intégrer des modules sur l'IA dans les programmes scolaires et universitaires.
- Organiser des formations pour les enseignants afin qu'ils maîtrisent les outils IA.

2. Perspectives pour l'IA dans l'éducation

- **Développer des solutions IA adaptées au contexte local :**

- Encourager les startups et chercheurs nigériens à créer des applications éducatives basées sur l'IA.
- Intégrer les langues nationales dans les assistants IA pour un apprentissage inclusif.

- **Favoriser des partenariats public-privé :**

- Collaborer avec des entreprises technologiques et des organisations internationales pour financer et déployer des outils IA dans l'éducation.
- Encourager l'investissement dans la recherche et l'innovation en IA éducative.

- **Garantir une IA éthique et inclusive :**

- Éviter les biais algorithmiques qui pourraient désavantager certains élèves.
- Mettre en place des réglementations pour encadrer l'utilisation de l'IA dans l'éducation.

**LA CYBERSÉCURITÉ
DANS L'ÉDUCATION
AU NIGER**



LA CYBERSÉCURITÉ DANS L'ÉDUCATION AU NIGER



- 1. Enjeux de la Cybersécurité**
- 2. Perspectives pour renforcer la cybersécurité**

1. Enjeux de la Cybersécurité dans l'éducation

1.1 Principales menaces en cybersécurité dans l'éducation :

- ☐ Fuites et vols de données.
- ☐ Cyberattaques contre les plateformes d'apprentissage.
- ☐ Phishing et ingénierie sociale.
- ☐ Malwares et ransomwares.
- ☐ Atteinte à l'intégrité des données.

1. Enjeux de la Cybersécurité dans l'éducation



1.2 Défis de la cybersécurité dans l'éducation :

- ☐ Manque de sensibilisation et de formation.
- ☐ Faible protection des infrastructures IT.
- ☐ Absence de réglementation spécifique à la cybersécurité dans l'éducation.
- ☐ Budget limité pour la cybersécurité.
- ☐ Usage non contrôlé des outils numériques.

2. Perspectives pour renforcer la cybersécurité dans l'éducation



2.1 Sensibilisation et formation à la cybersécurité :

- ☐ Intégrer des cours de cybersécurité dans les programmes scolaires et universitaires.
- ☐ Organiser des campagnes de sensibilisation pour les enseignants, élèves et administrateurs.
- ☐ Former des référents cybersécurité dans les établissements éducatifs.

2.2 Sécurisation des infrastructures numériques :

- ☐ Mettre en place des pare-feux et solutions antivirus dans les écoles et universités.
- ☐ Assurer des mises à jour régulières des systèmes informatiques.
- ☐ Protéger les accès aux plateformes éducatives avec l'authentification multi-facteurs (MFA).

2. Perspectives pour renforcer la cybersécurité dans l'éducation



2.3 Encadrement réglementaire et gouvernance :

- ☐ Élaborer une politique nationale de cybersécurité pour l'éducation.
- ☐ Exiger des établissements éducatifs la mise en place de protocoles de protection des données.
- ☐ Collaborer avec le gouvernement pour renforcer les mesures de cybersécurité.

2.3 Encourager l'innovation et la recherche en cybersécurité :

- ☐ Soutenir les projets académiques et universitaires en cybersécurité.
- ☐ Développer des plateformes locales sécurisées pour l'e-learning.
- ☐ Promouvoir les startups spécialisées en cybersécurité éducative.

2.4 Développer des partenariats :

- ☐ Collaborer avec des entreprises et associations comme APSI NE.
- ☐ S'inspirer des autres pays de l'Afrique.

CAS PRATIQUE IA : EXPLOITER LES LLM POUR APPRENDRE





1. Présentation

2. Utiliser l'IA pour optimiser l'apprentissage

1. Les erreurs à éviter avec les LLM

1. Présentation



L'intelligence artificielle, et en particulier les **LLM (Large Language Models)**, également appelés **IA génératives**, transforment profondément et à grande vitesse nos modes de travail, d'apprentissage et nos usages quotidiens.

Parmi les exemples notables de LLM, on retrouve **ChatGPT d'OpenAI, Gemini de Google, Deepseek développé par les Chinois ainsi que Mistral qui est Français.**

Parmi les nombreux secteurs pouvant tirer parti de ces technologies, **l'éducation et l'apprentissage** figurent parmi les bénéficiaires, tout en étant également parmi les plus exposés aux **dérives potentielles de l'IA générative**

2. Utiliser l'IA pour optimiser l'apprentissage

2.1 Quelques outils d'IA utilisés dans l'éducation :

- **Magic School AI** : Une suite complète de plus de 60 outils d'IA pour aider les enseignants dans la planification des cours, la création d'évaluations et l'élaboration de plans d'enseignement individualisés. Version gratuite avec accès limité et version payante à 4 915 FCFA par mois pour des fonctionnalités supplémentaires → <https://magicschool.ai/>
- **Kahoot!** : Une plateforme interactive qui utilise l'IA pour créer des quiz et des jeux éducatifs. Offre une version gratuite avec des fonctionnalités de base, plans payants disponibles à partir de 4 177 FCFA par mois pour des fonctionnalités avancées → <https://kahoot.com/>
- **Quizlet** : Utilise l'IA pour développer des flashcards et des jeux éducatifs, facilitant la mémorisation et la préparation aux examens. Propose une version gratuite avec la version Quizlet Plus disponible à 21 151 FCFA par an → <https://quizlet.com/>

2. Utiliser l'IA pour optimiser l'apprentissage

- **Math GPT Pro** : Un outil d'IA conçu pour aider à résoudre des problèmes mathématiques complexes et fournir des explications détaillées, s'adaptant aux besoins individuels des élèves. Offre un plan gratuit avec une limite de 10 quotas, des abonnements payants sont disponibles à partir de 5 311 FCFA par mois → <https://mathgptpro.com/>
- **ClassPoint AI** : Permet aux enseignants de créer des quiz instantanés et prend en charge plusieurs langues. Propose une version gratuite avec des fonctionnalités de base, la version Pro est disponible à 56 640 FCFA pour un accès illimité à toutes les fonctionnalités → <https://classpoint.io/>

2. Utiliser l'IA pour optimiser l'apprentissage

2.3 ChatGPT : Un assistant IA au service de l'apprentissage

Pour le cas pratique, nous allons explorer l'utilisation de **ChatGPT**, une IA qui repose sur un algorithme avancé basé sur le modèle Transformer, qui fonctionne comme un **cerveau artificiel** capable de **comprendre le contexte des phrases et de fournir des réponses cohérentes**.

- Il peut adapter ses réponses en fonction du niveau de l'élève, de l'étudiant ou du besoin de l'enseignant, offrant ainsi un soutien personnalisé.
- Pour atteindre son niveau de performance, ChatGPT a été entraîné sur des milliards de pages issues d'Internet.

2. Utiliser l'IA pour optimiser l'apprentissage

2.4 Les GPTs personnalisés : Créez votre propre IA sur mesure

Un GPTs est une version personnalisée d'un modèle GPT (Generative Pre-trained Transformer), adaptée à des besoins spécifiques grâce à des instructions et des données sur mesure. Il permet aux utilisateurs de créer des intelligences artificielles optimisées pour des tâches précises.

Par exemple, vous pouvez concevoir un GPT spécialisé :

- Mathématiques
- Sciences Naturelles
- Codage
- Développement logiciel
- Analyse de données
- Philosophie
- Médecine
- Anglais, et bien d'autres domaines.

2. Utiliser l'IA pour optimiser l'apprentissage



2.5 Comment accéder à ChatGPT ?

Méthode 1 : Via un navigateur

- Rendez-vous sur <https://chat.openai.com>.
- Créez un compte avec votre e-mail.
- Testez gratuitement **GPT-3.5** ou optez pour **GPT-4** (payant, environ **12 000 F CFA/mois**).

Méthode 2 : Via les applications mobiles et PC

- Sur mobile : iOS (iPhone/iPad) : sur l'App Store et Android sur Google Play Store.
- Sur ordinateur : Téléchargez l'application pour Windows et Mac depuis le site officiel d'OpenAI.

Méthode 3 : La plus simple – Utiliser ChatGPT sur WhatsApp

 Ajoutez ce numéro : **+1 (800) 242-8478** sous le nom **“ChatGPT”** dans vos contacts, ouvrez WhatsApp et commencez à discuter avec ChatGPT !

2. Utiliser l'IA pour optimiser l'apprentissage

2.6 Exercices pratiques :

- **Mathématiques** : *Je suis un élève en terminale. Peux-tu me donner un plan de révision détaillé avec les notions essentielles à maîtriser et des exercices types pour le chapitre sur les nombres complexes ?*
- **Médecine** : *Je suis étudiant en médecine et je veux approfondir mes connaissances en anatomie humaine. Peux-tu me proposer une check-list des systèmes du corps humain ?*
- **Philosophie** : Explique la notion de justice selon Platon et Aristote en comparant leurs visions. Donne des exemples concrets pour illustrer leurs différences.
- **Informatique** : *Je suis étudiant en informatique et je veux apprendre la programmation en Python. Peux-tu me donner un parcours d'apprentissage progressif avec les concepts essentiels à maîtriser ainsi que des exercices pratiques pour chaque étape ?*

3. Les erreurs à éviter avec les LLM

- **Dépendance excessive et absence d'esprit critique** : Encourager les étudiants à utiliser les LLM sans développer leur esprit critique peut nuire à leur capacité d'analyse et de réflexion autonome.
- **Informations erronées ou biaisées** : Les LLM peuvent générer des réponses inexactes ou biaisées.
- **Langue et contexte culturel** : Beaucoup de modèles sont entraînés sur des données non adaptées aux réalités culturelles et linguistiques du Niger, ce qui peut entraîner des incompréhensions.
- **Plagiat et manque de créativité** : L'usage abusif des LLM pour la rédaction d'examens ou de devoirs peut réduire la capacité des étudiants à produire un travail original.

CAS PRATIQUE CYBERSÉCURITÉ : BONNES PRATIQUES ET OUTILS





1. Bonnes pratiques

1. Outils

1. Bonnes pratiques

"À mesure que les développeurs continueront d'inventer de meilleures mesures de sécurité, rendant l'exploitation des systèmes plus difficile, les attaquants se tourneront toujours vers l'humain, en utilisant l'ingénierie sociale (Kevin D. Mitnick). "

"Les amateurs piratent des systèmes, les professionnels piratent les gens (Kevin D. Mitnick). »

1.1 Détectez les tentatives d'hameçonnage

- **L'objet de l'email:** Le pirate envoie souvent un mail avec un objet alarmiste.
- **La demande d'informations personnelles.**
- **Adresses d'expéditeur suspectes :** L'e-mail de l'expéditeur ne correspond pas au domaine.
- **Liens douteux :** Vérifiez toujours l'URL des liens dans l'e-mail avant de cliquer.
- **Pièces jointes inattendues.**

Exemple d'un email d'hameçonnage :

Expéditeur: info@votrecole.com

Objet : «Urgent»

Message : Pour des raisons de sécurité, votre école invite l'ensemble de ses Étudiants à modifier leur code d'accès dans un délai de 24 h sous peine de ne plus pouvoir se connecter à leur espace personnel. Vous devez cliquer sur le lien ci-dessous et entrez vos informations de connexion pour modifier votre code d'accès :

[lien pour modifier vos accès](#)

1. Bonnes pratiques

1.2 Utilisation des mots de passe robustes

La majorité des piratages sont dus à des mots de passe soit trop faciles à deviner, soit volés.

- **Les attaques possibles sur les mots de passe :**
 - **Attaque par Force Brute :** L'attaquant essaie toutes les combinaisons possibles.
 - **Attaque par Dictionnaire :** L'attaquant crée une liste de mots possibles.
 - **Attaque par Keyloggers :** L'attaquant installe un petit logiciel espion sur votre appareil (ordinateur ou téléphone) qui enregistre tout ce que vous tapez, y compris vos mots de passe.
 - **Attaque par Ingénierie Sociale :** Manipulation psychologique pour vous faire divulguer vos mots de passe.

1. Bonnes pratiques



- **Créer des mots de passe complexes :**

Minimum 8 à 12 caractères et Mélanger des lettres, chiffres et caractères spéciaux (%,@,\$, etc.).

Exemple : Création d'un mot de passe complexe avec une méthode simple

« J'aime le café chaque matin à 7h ! » : On va transformer cette phrase en un mot de passe :

- 1) Prenons les premières lettres de chaque mot, ça donne : "Jalccma7h!".
- 2) On va encore ajouter des variations en remplaçant des lettres par des chiffres ou des symboles :
 - Le "a" devient "@" et ça donne : "J@lccm@7h!"
 - Remplacez "7h" par "07H" pour ajouter une majuscule, et on a : "J@lccm@07H!"
- 3) Résultat: Le mot de passe "J@lccm@07H!" est très complexe tout en étant mémorable grâce à la phrase d'origine.

1. Bonnes pratiques

- **Respectez quelques précautions essentielles et activez des solutions complémentaires :**
 - Activez l'authentification à double facteurs (2FA) si disponible.
 - Utilisez un gestionnaire de mot de passe.
 - Créez des mots de passe uniques pour chaque compte.
 - Ne partagez jamais vos mots de passe, même avec des collègues.
 - Ne stockez pas vos mots de passe dans un fichier non sécurisé.
 - Ne cliquez jamais sur "se souvenir de moi" surtout sur des ordinateurs publics.
 - Activez l'Authentification par la Biométrie.
 - Protégez vos connexions: Utilisez toujours des connexions HTTPS.
 - Évitez les Wi-Fi publics : Jamais du Wi-Fi public pour accéder à vos comptes sensibles. Si ça s'impose, utilisez un VPN

LE TEMPS POUR HACKER UN MOT DE PASSE EN 2024

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombre, lettres majuscules & minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241k ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans

Source : Hive Systems

2. Outils

1.3 Le Framework OSINT

C'est un ensemble d'outils et de méthodes pour la collecte des informations disponibles publiquement. Présenté sous forme de carte mentale (Mind Map), il facilite l'organisation et l'analyse des données pour obtenir des renseignements exploitables dans divers contextes, tels que la cybersécurité, les enquêtes ou même pour un usage personnel.

Il existe nombreux outils dans le Framework, nous allons juste explorer quelques-uns :

1. <https://osintframework.com/>
2. Opsec → Anonymous Browsing → NoScript (T)
3. Opsec → Privacy / Clean Up → Just Delete Me
4. Opsec → Privacy / Clean Up → Social Media Fingerprint
5. Opsec → Privacy / Clean Up → Privacy Tools
6. Malicious File Analysis → Malware Analysis Tools → Online Scanners → Virus Total

CONCLUSION



L'intégration de **l'Intelligence Artificielle** et de la **Cybersécurité** dans **l'éducation au Niger** représente une **opportunité stratégique** mais présente énormément des **défis**.

❑ **L'IA offre des solutions innovantes :**

- Apprentissage personnalisé et automatisation des tâches.
- Meilleure accessibilité aux ressources pédagogiques.
- Possibilité d'intégration des langues locales dans l'apprentissage.

Cependant, des défis subsistent, notamment le **manque d'infrastructures, de compétences et de financement** pour une adoption efficace.

❑ **La cybersécurité est un impératif :**

- Protection des données
- Protection des réseaux et systèmes.

Toutefois, le **manque de sensibilisation, de réglementation stricte et d'investissement** fragilise les établissements face aux menaces numériques.

L'intégration de **l'Intelligence Artificielle** et de la **Cybersécurité** dans **l'éducation au Niger** représente une **opportunité stratégique** mais présente énormément des **défis**.

❑ **L'IA offre des solutions innovantes :**

- Apprentissage personnalisé et automatisation des tâches.
- Meilleure accessibilité aux ressources pédagogiques.
- Possibilité d'intégration des langues locales dans l'apprentissage.

Cependant, des défis subsistent, notamment le **manque d'infrastructures, de compétences et de financement** pour une adoption efficace.

❑ **La cybersécurité est un impératif :**

- Protection des données
- Protection des réseaux et systèmes.

Toutefois, le **manque de sensibilisation, de réglementation stricte et d'investissement** fragilise les établissements face aux menaces numériques.

« L'Afrique a raté la révolution industrielle, elle ne doit pas rater la révolution numérique. »

« La cybersécurité, c'est comme l'assurance : soit on paie avant, soit on paie après... mais après, c'est toujours plus cher. »

Merci!

Avez-vous des questions?