CIBEROBS

MAKEAFRICASAFE

Livre blanc

Le cyberespace africain à l'épreuve de l'Intelligence Artificielle (IA) : enjeux, défis et opportunités

Novembre 2023

En partenariat avec

CAF CYBER AFRICA FORUM

CIBEROBS CONSULTING

Auteurs

Sylvestre KABORE
Brice-Yves KOFFI
Amadou Tidiane DIAWARA
Alassane FANNY
Issa LASSISSI
Kevin AMLAMAN

Remerciements

Les auteurs tiennent à remercier l'ensemble de l'équipe Ciberobs Make Africa Safe et toutes les personnes qui ont contribué à la rédaction de ce livre blanc.

Avant-Propos

Créée en 2019 par Franck KIÉ, Managing Partner du cabinet panafricain de conseil Ciberobs Consulting, Ciberobs Make Africa Safe est une plateforme dédiée à la cybersécurité en Afrique, visant à être le principal relais d'informations sur les risques cybernétiques touchant le continent.

Pour concrétiser cette ambition, Ciberobs Make Africa Safe propose une variété de contenus tels que des articles, des analyses d'actualités et des interviews, en collaborant avec des experts, des institutions, des entreprises et des médias. Pour renforcer son action, elle a fusionné avec Africa Security Partners, une organisation spécialisée dans la sensibilisation à la cybersécurité en Afrique, permettant ainsi une mutualisation des efforts.

Ciberobs Make Africa Safe est également à l'origine du Cyber Africa Forum, un événement annuel réunissant les acteurs les plus influents de la sécurité numérique en Afrique. Cette rencontre offre une plateforme d'affaires propice aux échanges sur les enjeux, opportunités et perspectives du secteur dans la région.

Plus d'information sur : www.ciberobs.com

Table des matières

Partenaire Thought Leadership du Cyber Africa Forum (CAF) 2023

Mastercard is passionate about powering economies and empowering people, building a sustainable and inclusive digital economy where everyone prospers. It is both our business strategy and our social responsibility to ensure that people, businesses and organizations have access to the networks, tools and solutions that can help them reach their potential, achieve financial security, and grow. Our unique B2B2C model allows us to advance innovation and digitization to simplify the way people pay. By harnessing the potential of technology, Mastercard continues to work with partners in the public and private sector to ensure a more connected future.

Jean-Charles YALLET
Vice President, Country Lead, Sub Saharan Francophone Africa (FSSA)

Introduction

Dans le paysage numérique actuel, l'Afrique de l'Ouest se distingue comme un hub technologique émergent, où la cybersécurité et l'Intelligence Artificielle (IA) occupent une place prépondérante dans la révolution en cours. Selon Verified Market Research, cabinet mondial de recherche et de conseil, la taille du marché de l'IA dans le domaine de la cybersécurité était de 17 milliards de dollars en 2022, et devrait dépasser les 100 milliards de dollars d'ici 2032[1]. La croissance exponentielle des technologies de l'information et de la communication, conjuguée à la diversité culturelle et à la vigueur économique de la région, positionnent l'Intelligence Artificielle comme un catalyseur potentiel de la croissance économique et du développement social. Cependant, cette rapide avancée se heurte à des menaces cybernétiques grandissantes, compromettant la sécurité tant des individus que des entreprises et des gouvernements.

Dans ce contexte, assurer la protection des données sensibles et des infrastructures critiques devient impératif pour préserver la souveraineté nationale. La convergence entre la cybersécurité et l'Intelligence Artificielle ouvre des perspectives exceptionnelles : les systèmes d'IA peuvent non seulement détecter, mais également prévenir les cyberattaques, renforçant ainsi la résilience des réseaux numériques régionaux. De surcroît, l'innovation dans le domaine de l'Intelligence Artificielle peut catalyser le développement de solutions de cybersécurité adaptées aux besoins spécifiques de l'Afrique de l'Ouest.

Face à ce défi colossal, une coopération étroite entre les gouvernements, le secteur privé, la société civile et les institutions académiques est impérative. La création d'un écosystème propice à l'innovation, associée à des investissements dans la formation, s'avère cruciale pour relever les défis de la cybersécurité et maximiser les avantages de l'Intelligence Artificielle.

Ce livre blanc explore en profondeur les spécificités de la cybersécurité et de l'Intelligence Artificielle en Afrique de l'Ouest, mettant en lumière les défis uniques de la région et proposant des recommandations concrètes. En mettant l'accent sur la collaboration régionale, l'innovation et l'inclusion numérique, il encourage à tracer ensemble la voie vers un avenir numérique plus sûr, plus intelligent et plus prospère pour l'Afrique de l'Ouest et au-delà.

[1] · Artificial Intelligence (AI) In Cybersecurity Market 2032, Precedence Research, 2023.

1 Paysage actuel de la Cybersécurité en Afrique de l'Ouest

Partenaire Thought Leadership du Cyber Africa Forum (CAF) 2023

“ La cybercriminalité est une menace en constante évolution à l'ère du numérique, avec des conséquences dévastatrices pour toute entreprise notamment les pertes financières, la compromission de la confidentialité des données, l'impact négatif sur la réputation et bien d'autres. À ce titre, maintenir les compétences en cybersécurité, se doter d'outils d'infrastructures de sécurité modernes, constituent pour GUCE CI, des enjeux majeurs pour faire face aux menaces actuelles et émergentes.

GUICHET UNIQUE DU COMMERCE EXTERIEUR | COTE D'IVOIRE

www.guce.gouv.ci

1.1. Analyse de l'impact financier des cyberattaques

Selon les projections du rapport annuel du cabinet de conseil américain Cybersecurity Ventures, les coûts liés à la cybercriminalité devraient connaître une augmentation de 15 % par an au cours des trois prochaines années, atteignant 8 000 milliards de dollars cette année et estimés à 10 500 milliards de dollars par an d'ici 2025, contre 3 000 milliards de dollars en 2015[2].

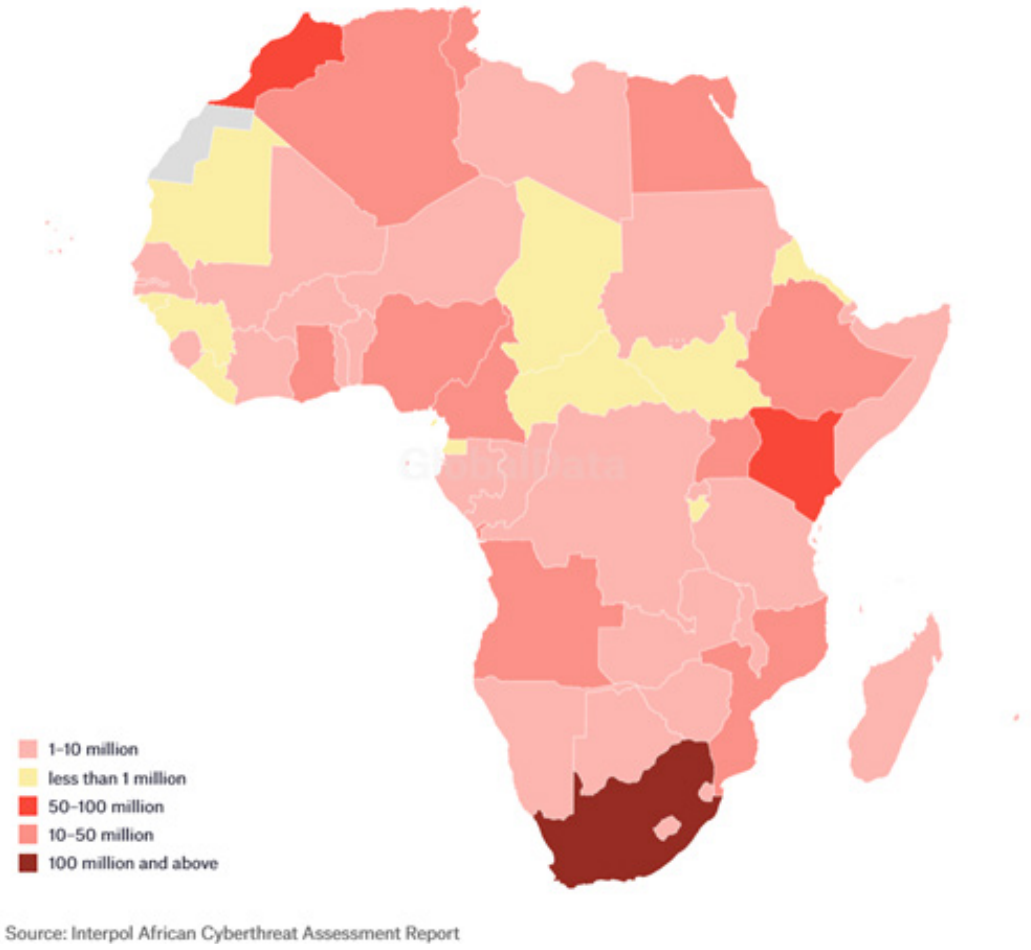


Figure 1. Aperçu des détections de menaces cyber en Afrique entre 2020 et 2021

Par ailleurs, le nombre total de cyberattaques réussies a plus que doublé au cours des cinq dernières années. Avec la rapide expansion du numérique en Afrique, les risques de sécurité pour les gouvernements et les entreprises connaissent une croissance exponentielle, les plaçant comme des cibles privilégiées des cybercriminels. Ces risques sont exacerbés par la sophistication croissante des méthodes employées par les auteurs de cyberattaques. Au deuxième trimestre de 2023, l'Afrique a enregistré le plus grand nombre moyen de cyberattaques par semaine et par organisation, avec une augmentation de 23 % par rapport à la même période en 2022[3] . Ces cyberattaques ont engendré des coûts estimés à environ 10 % du PIB[4] des pays africains.

[2] « 2023 Official Cybercrime Report », Cybersecurity Ventures, 2023.

[3] « Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research », sur Check Point Blog [en ligne], 2023.

[4] Donnée publiée par la Commission Économique pour l'Afrique, 2022.

En 2023, les cyberattaques ont coûté près de 5,9 millions de dollars au secteur financier, ce qui les place en deuxième position en termes de coûts les plus élevés par rapport à d'autres secteurs selon les chiffres de IBM Security[5]. En effet, les banques et les institutions financières sont des cibles privilégiées des cybercriminels, étant donné la nature très sensible des données que ces entités possèdent sur leur clientèle et de l'opportunité financière qui s'y rattache. Entre 2018 et 2022, le groupe de cybercriminels OPERA1ER a mené plus de 35 attaques réussies et a détourné pas moins de 11 millions de dollars auprès de banques et d'entreprises de télécommunications, à travers de multiples pays notamment en Afrique. Les pertes totales liées à ces attaques sont estimées à 30 millions d'USD[6].

Les institutions gouvernementales et les entreprises opérant dans le secteur public sont des cibles privilégiées des cybercriminels, en raison du stockage de données sensibles et personnelles sur les citoyens. Au printemps 2022, le siège de l'Union Africaine a été victime d'une attaque, entraînant la paralysie du réseau interne de l'organisation quelques jours seulement après la conclusion du sommet annuel réunissant les chefs d'État du continent[7]. Les cybercriminels ont également ciblé des entités gouvernementales de grande envergure, notamment la Banque de Zambie, plusieurs ministères en Ouganda, ainsi que des institutions gouvernementales en Éthiopie et au Sénégal[8].

Le secteur privé ne fait pas exception. Quelle que soit leur taille, les entreprises demeurent vulnérables aux cyberattaques, susceptibles de perturber leurs opérations et de ternir leur réputation. En 2023, des entreprises telles que Flutterwave, TransUnion, le siège de Porsche en Afrique du Sud, ainsi que les compagnies d'électricité du Ghana (ECG) et d'Afrique du Sud (Eskom) ont été victimes d'attaques informatiques[9].

Au-delà des conséquences sur les entreprises touchées, les cyberattaques peuvent avoir des répercussions sur le quotidien des populations lorsqu'elles ciblent des infrastructures critiques[10].

1.2. Analyse des menaces sur les infrastructures critiques

Ces dernières années, l'Afrique a connu une accélération significative de sa transformation numérique. En conséquence, la cybersécurité a émergé en tant que préoccupation majeure pour tous les États du continent. Dans son rapport 2023 sur les grands risques mondiaux auxquels nous pourrions être confrontés au cours de la prochaine décennie, le Forum économique mondial a souligné que la cybercriminalité et la cybersécurité, font désormais partie des questions primordiales à résoudre pour la prochaine décennie au même titre que le changement climatique et les migrations involontaires. C'est dire à quel point la question de la cybersécurité revêt une importance capitale[11]. Elle est désormais considérée comme un pilier essentiel de nos nations, compte tenu des risques potentiels en cas d'attaques informatiques.

Les attaques cybernétiques qui émergent en Afrique de l'Ouest sont un défi majeur pour la sécurité et le développement de la région. Ces attaques peuvent avoir des conséquences graves sur la sécurité publique, la santé publique, l'éducation et l'économie. Les cybercriminels ciblent désormais des secteurs qui étaient auparavant considérés comme moins vulnérables. Les entreprises et les gouvernements d'Afrique de l'Ouest doivent être conscients des nouveaux risques afin de se préparer efficacement à faire face à ces nouvelles menaces.

---

[5] « Cost of a Data Breach Report 2023 », IBM Security, 2023.

[6] « OPERA1ER: Ceux qui jouent à Dieu sans y avoir été autorisés », Group-IB, 2022.

[7] « Vent de panique à l'Union africaine après une nouvelle cyberattaque », Le Monde.fr, 25 avril 2023.

[8] « Cybersecurity Threatscape of African Countries 2022–2023 », Positive Technologies, 2023.

[9] *Ibid.*

[10] Une infrastructure critique fait référence à des installations, systèmes, et services essentiels au fonctionnement d'une société et dont la perturbation ou la destruction pourrait avoir un impact grave sur la sécurité nationale, l'économie, la santé publique, ou d'autres aspects vitaux de la vie quotidienne. Ces infrastructures peuvent inclure des secteurs tels que l'énergie, les télécommunications, les transports, l'eau, la santé, la finance, et d'autres services gouvernementaux.

[11] « Global Risks Report 2023 », Forum économique mondial, 2023.

Pour illustrer les conséquences potentielles de ces attaques, l'analyse se concentrera sur les menaces qui pèsent sur les infrastructures critiques et les répercussions qui pourraient en découler.

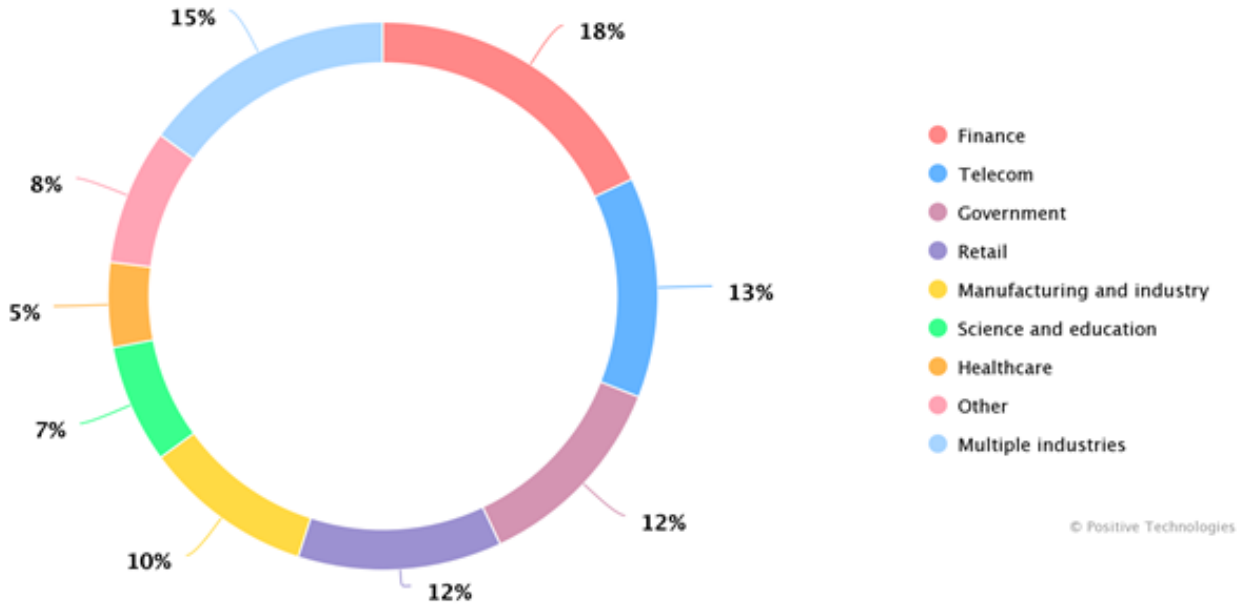


Figure 2. Les principaux secteurs victimes de cyberattaques en Afrique – Positive Technologies

— Au niveau du secteur industriel

Le domaine industriel est confronté aux cyberattaques qui visent à perturber le fonctionnement normal des activités industrielles, à saboter les infrastructures critiques ou à voler les secrets commerciaux.

Les réseaux de distribution de nourriture, d'eau et d'énergie sont désormais informatisés et reposent en quasi-totalité sur des systèmes de contrôle et de communication (SCADA)[12]. Les cyberattaques visant ce type d'infrastructures critiques, telles que les centrales électriques, les systèmes de transport et les réseaux de télécommunications sont de plus en plus répandues. Selon les conclusions de l'étude menée par Cyentia Institute, centre de recherche spécialisé en cybersécurité, les cyberattaques visant les infrastructures critiques ont augmenté de 60 % en 2023[13]. Ces attaques peuvent avoir un impact dévastateur sur les infrastructures essentielles, telles que l'alimentation, l'approvisionnement en eau, les transports et les communications.

Alors que les cyberattaques contre les infrastructures maritimes se multiplient, les experts craignent que les ports et les industries maritimes africains ne soient la cible d'une attaque qui perturberait gravement les échanges commerciaux, comme ce fut le cas lors de la cyberattaque contre Transnet en juillet 2021. L'attaque de Transnet, en charge des principaux ports du pays et de la plupart des réseaux ferroviaires, a eu des conséquences majeures sur les opérations portuaires en Afrique du Sud.

[12] SCADA : Supervisory Control and Data Acquisition

Les attaquants ont employé une tactique de ransomware[14], bloquant ainsi l'accès aux données et aux systèmes de contrôle des ports. Cette perturbation a impacté significativement les opérations de conteneurs aux ports de Cape Town et Durban, mettant en lumière les risques émergents liés aux cyberattaques dans le domaine des infrastructures critiques[15].
Il est donc crucial pour les États de mettre en place des plans d'accompagnement visant le renforcement de la sécurité, en particulier pour les entreprises considérées comme ayant un intérêt vital pour la nation. En collaborant étroitement avec le secteur privé, les gouvernements peuvent élaborer des politiques et des initiatives qui favorisent la cybersécurité, partageant des bonnes pratiques, fournissant des ressources et encourageant l'adoption de mesures de protection avancées. Une approche coordonnée est essentielle pour faire face aux menaces cybernétiques qui peuvent avoir des répercussions sur la sécurité nationale, l'économie et la stabilité générale.

— Au niveau de l'administration publique

Depuis le début de l'année 2022, plusieurs gouvernements africains se sont engagés à relever les défis de la numérisation liés à la bonne gouvernance, à la croissance économique et à la performance de leurs pays respectifs. Ils ont entamé une course à la modernisation des services de l'État.

Cependant, il est important de rappeler que même si la transformation numérique ouvre de nouvelles perspectives, elle ouvre également de nouvelles portes aux cybercriminels. L'attaque du 26 mai 2023 qui a mis hors service une dizaine de site web officiels sénégalais[16], prouve que les institutions gouvernementales ne sont pas à l'abri de telles attaques. Elles doivent donc reconnaître et atténuer les risques de cyberattaques dans leur stratégie de transformation numérique.

— Au niveau du secteur de la santé

Selon une étude menée en 2023 par l'entreprise Fortified, les données de plus de 40 millions de personnes ont été compromises lors de cyberattaques, soit une hausse de 60% par rapport à l'année précédente [17]. Les cyberattaques visant les hôpitaux et les cliniques peuvent provoquer d'importantes perturbations de leurs systèmes informatiques, entraînant des retards dans les soins aux patients, la perte de données médicales sensibles, voire des décès. C'est ce qu'illustrent les cyberattaques contre le groupe hospitalier sud-africain Life Healthcare, qui ont eu des répercussions sur les services d'admission, le traitement des dossiers des patients et les serveurs de courrier électronique, entre autres opérations critiques. Il convient de noter que les soins aux patients n'ont pas été affectés, bien que les hôpitaux et les bureaux administratifs fonctionnaient au ralenti[18].

[13] CYENTIA INSTITUTE, « Cybersecurity Incidents in Industrial Operations Report », Rockwell Automation, 2023.
[14] Un rançongiciel ou ransomware est un logiciel malveillant qui bloque l'accès à un ordinateur et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
[15] « Case Study 17: Port of Durban, South Africa », in Building Capacity to Manage Risks and Enhance Resilience, UNCTAD 2022.
[16] « Au Sénégal, l'État ciblé par une cyberattaque », JeuneAfrique.com, 2023.
[17] « 2023 Mid-Year Horizon Report: The State of Cybersecurity in Healthcare », Fortified Health Security, 2023.
[18] « Afrique du Sud - Life Healthcare frappé par des cyberattaques », sur Businessfrance.fr, 2020.

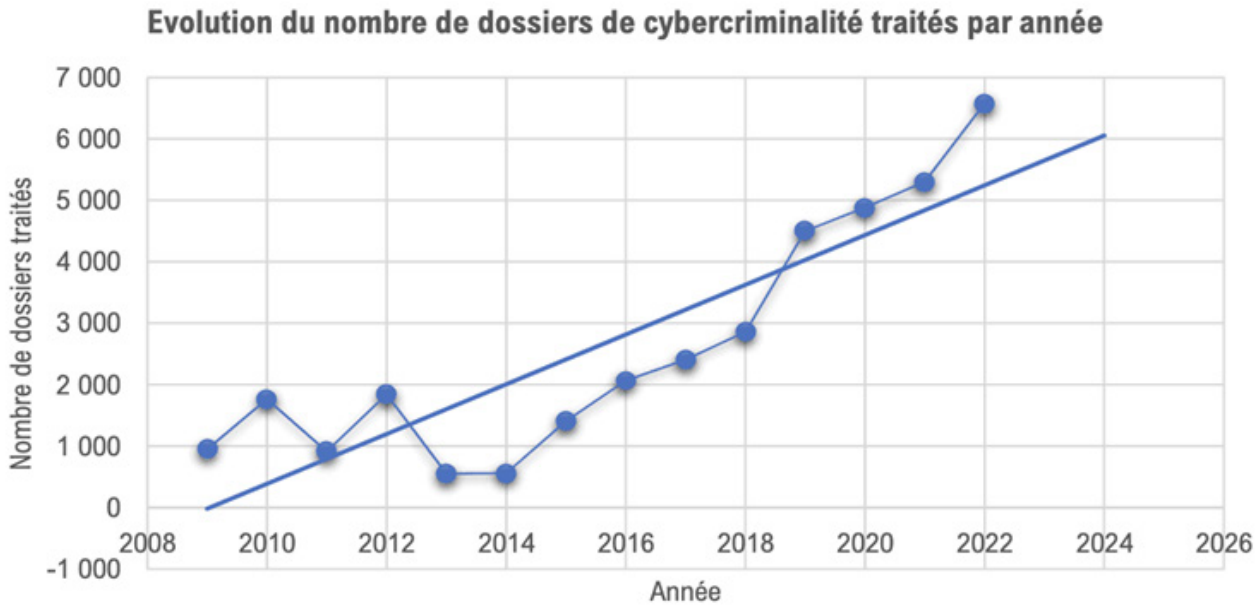


Figure 3. Courbe d'évolution des dossiers de cybercriminalités traités entre 2009 et 2023 en Côte d'Ivoire

1.3. Évolution du cadre règlementaire relatif à la Cybersécurité

Le cadre règlementaire en matière de cybersécurité en Afrique de l'Ouest est en cours de développement. Les initiatives régionales et nationales prises ces dernières années constituent une étape importante pour renforcer la cybersécurité dans la région. Cependant, il reste encore beaucoup à faire pour sensibiliser les entreprises et les particuliers aux risques des cyberattaques et pour les aider à mettre en place des mesures de protection efficaces.

En Afrique de l'Ouest, plusieurs pays ont adopté des lois et des réglementations en matière de cybersécurité en 2023. Ces mesures visent à renforcer la protection des données personnelles et des infrastructures critiques. Les États de la CEDEAO travaillent conjointement depuis 2010 à l'harmonisation de la règlementation en matière de cybersécurité[19], notamment grâce à :

- L'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.
- L'acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO.
- La Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

La CEDEAO offre également un accompagnement à ses États membres dans le renforcement de la cybersécurité à travers des actions de partage d'information, de sensibilisation et de formation. Ces efforts ont pour objectif principal de renforcer les coopérations entre les gouvernements, les acteurs de la cybersécurité et avec les institutions régionales. Il est question de soutenir la croissance économique de ces États à travers des mesures visant à garantir la résilience et la sécurité des opérateurs d'importance vitale (OIV)[20].

[19] Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité, CEDEAO, 2021.

[20] Opérateurs d'importance vitale (OIV) : Organisations essentielles à la survie ou à la sécurité nationale.

Il incombe maintenant aux États concernés de les décliner au niveau national à travers des réformes. La Côte d'Ivoire, le Bénin et le Togo peuvent être cités comme bons élèves en la matière avec la création d'agences spécialisées notamment : l'Agence Nationale de la Cybersécurité (ANCy) au Togo, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) du Bénin et du Sénégal et l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI). En outre, un projet supplémentaire de mise en œuvre d'une agence nationale de sécurisation des systèmes d'information visant à accompagner les institutions publiques et entreprises privées est en cours en Côte d'Ivoire.

Par ailleurs, des textes de lois visant à encadrer l'exploitation des données personnelles et les activités dans le domaine cyber ont également vu le jour dans plusieurs pays Ouest-africains. Le Nigeria Data Protection Act (NDPA) de 2023 établit un cadre juridique pour la règlementation des données personnelles au Nigéria[21]. Le Ghana a adopté une loi sur la cybersécurité en 2020. Dans le cadre de la préparation à la mise en œuvre de la loi, l'Autorité de la cybersécurité (CSA) a été créée pour règlementer l'écosystème de la cybersécurité dans le pays[22]. En Côte d'Ivoire, un projet de loi a été soumis en 2022 dans l'optique de durcir la répression de la cybercriminalité. La modification des articles 17, 33, 58, 60, 62 et 66 de la loi relative à la lutte contre la cybercriminalité instaure des peines maximales d'emprisonnement liées à toutes utilisations illicites des TIC[23].

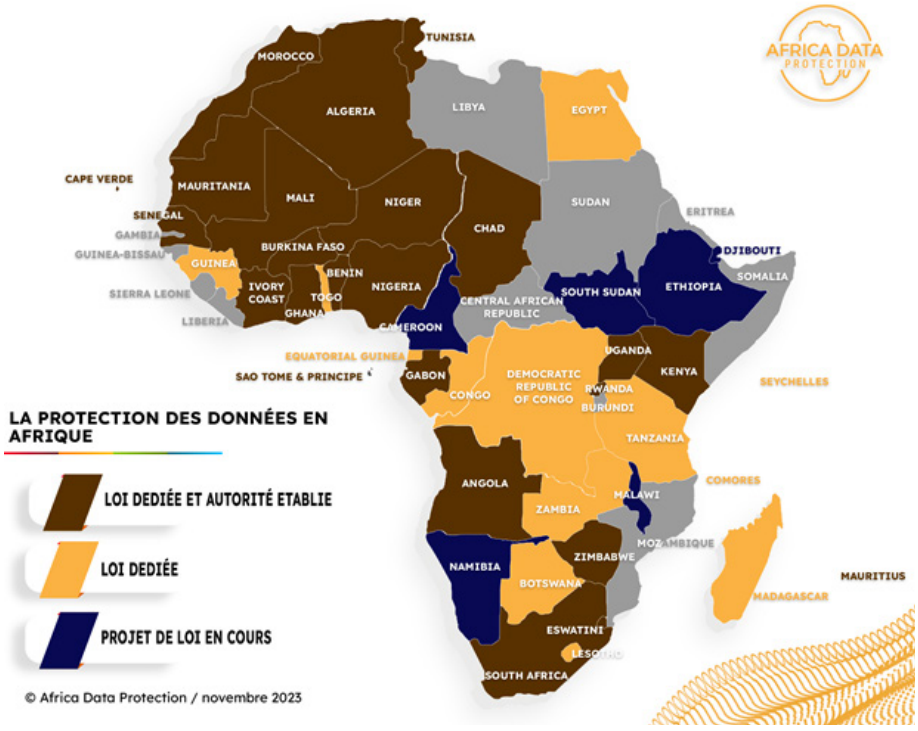


Figure 4. La protection des données en Afrique

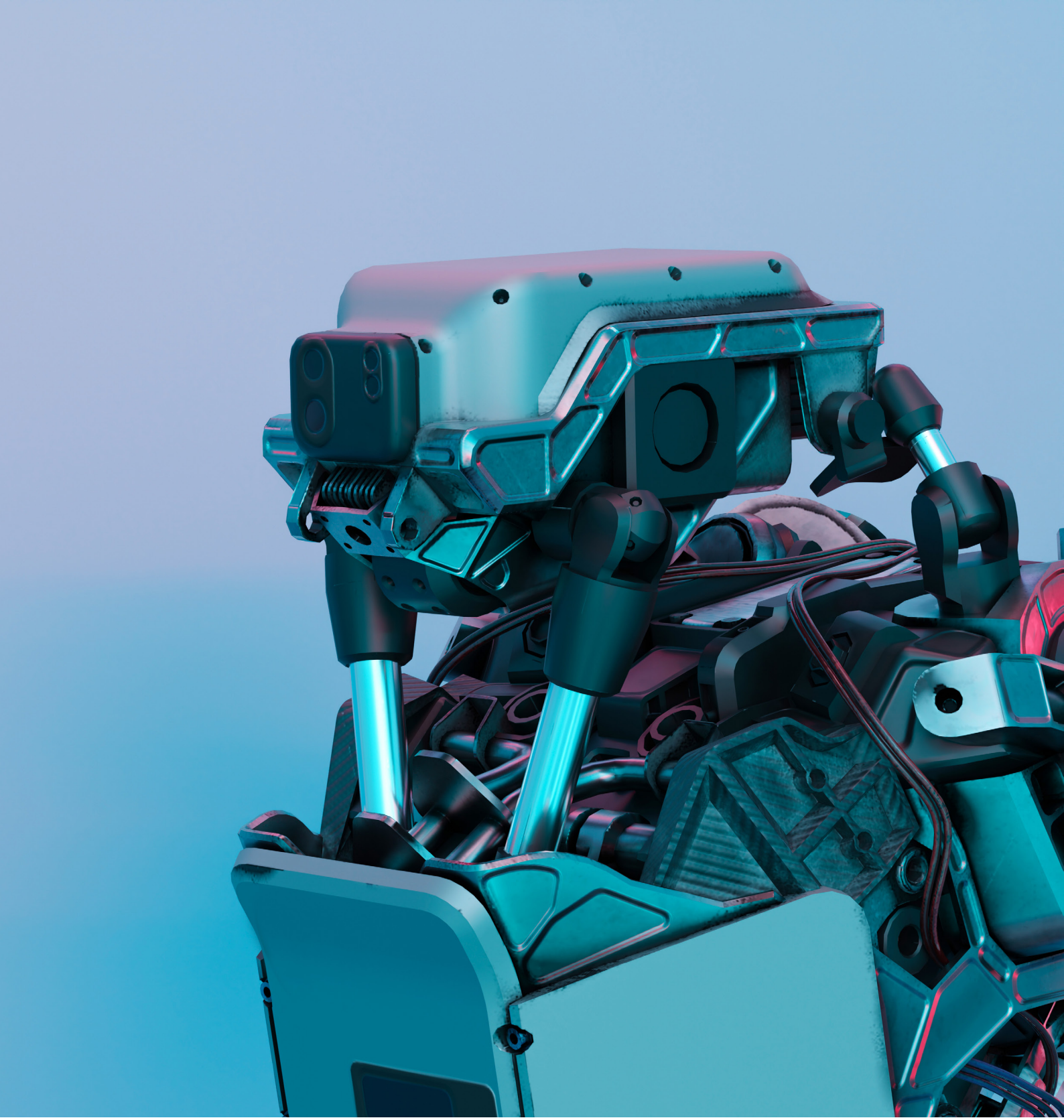
Au vu des nouvelles menaces qui pèsent sur le paysage numérique africain, force est de constater que la législation peine encore à s'adapter à l'évolution constante de la sphère cybernétique, notamment face à la démocratisation de l'Intelligence Artificielle. Pour emprunter les mots de l'expert en cybersécurité singapourien Barry Greene, les cybercriminels opèrent à la vitesse de la lumière tandis que les autorités agissent à la vitesse de la loi. Cette disparité entre les moyens de protection et les capacités des acteurs malveillants, exacerbée par la montée en puissance de l'Intelligence Artificielle dans le domaine de la sécurité numérique, place les acteurs du numérique du continent face à des défis colossaux.

---

[21] AJAYI Wale, « The Nigeria Data Protection Act, 2023 - KPMG Nigeria », sur KPMG, septembre 2023.

[22] « CSA, Chamber of Telecommunications collaborate on cyber security regulations », sur MyJoyOnline, 2023.

[23] « Côte d'Ivoire : Nouvelle loi sur la cybercriminalité, toute image à caractère de pornographie infantile désormais punie d'un à six ans et jusqu'à 40 millions d'amende », sur KOACI [en ligne], 2022.



2 Défis et opportunités de l'Intelligence Artificielle en matière de Cybersécurité

Partenaire Thought Leadership du Cyber Africa Forum (CAF) 2023

> La cybersécurité est au cœur de nombreux domaines du droit et des affaires sur lesquels nous intervenons, qu'il s'agisse de questions de règlementation bancaire, de produits fintech ou de startups naissantes sur les marchés africains. À ce titre, c'est un sujet auquel nous sommes attentifs.

ASAFO & CO.

www.asafoandco.com

La croissance de l'adoption de l'IA en Afrique est un facteur clé qui contribuera à l'amélioration de la cybersécurité dans la région. L'IA est déjà utilisée par de nombreuses entreprises et gouvernements africains pour des applications non liées à la cybersécurité, telles que la reconnaissance faciale, la traduction automatique et la surveillance des réseaux. À mesure que l'adoption de l'IA se poursuit, les entreprises et les gouvernements africains seront plus susceptibles de déployer des solutions d'IA pour la cybersécurité.

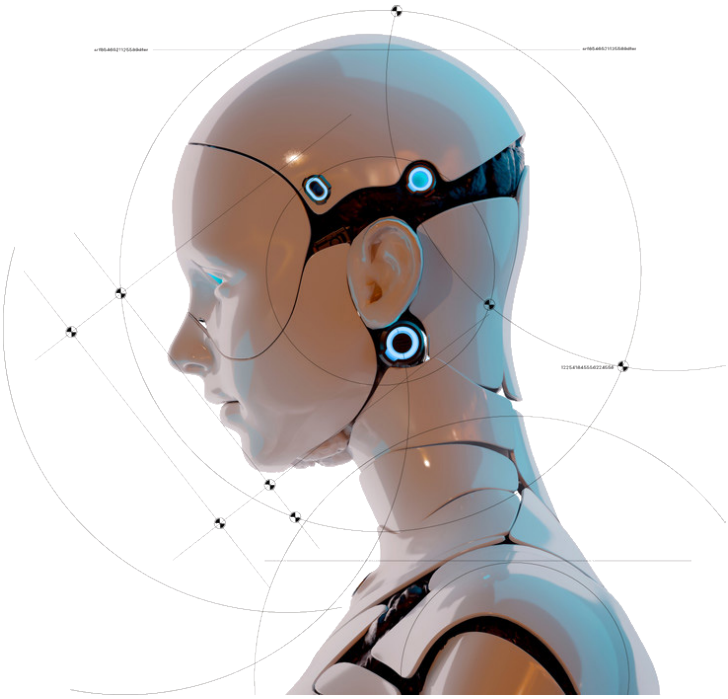
L'Intelligence Artificielle est utilisée à la fois par les cybercriminels pour mener des attaques sophistiquées et par les différentes entreprises dans la protection de leur système d'information contre ces menaces. Nous assistons à une course à l'armement technologique entre les cybercriminels et les professionnels de la cybersécurité.

2.1. Impact de l'IA sur la cybersécurité

Le paysage de la cybersécurité a subi des transformations majeures avec la démocratisation de l'Intelligence Artificielle, suscitant des préoccupations croissantes face aux défis en matière de sécurité en résultant. En effet, l'IA, facilite l'entrée dans le monde de la cybersécurité et offre aux acteurs malveillants une force de frappe plus importante.

Les cybercriminels adoptent désormais des techniques avancées, intégrant l'IA pour rendre leurs attaques plus persuasives et difficiles à détecter en s'adaptant aux habitudes et comportements spécifiques des utilisateurs ciblés. Ceci souligne l'impératif croissant pour les entreprises de développer des solutions de cybersécurité alimentées par l'IA afin de contrer ces menaces en constante évolution.

L'IA a le potentiel de transformer la cybersécurité en Afrique. Elle peut aider à relever les défis spécifiques de la région et à protéger les entreprises, les gouvernements et les citoyens africains contre les cyberattaques. Cependant, les organisations doivent également être conscientes que les cybercriminels adaptent leurs méthodes pour résister aux outils de cybersécurité classiques. Les cybercriminels utilisent également l'IA pour créer des attaques avancées, déployer des formes nouvelles et actualisées de logiciels malveillants pour cibler à la fois les systèmes traditionnels et les systèmes améliorés par l'IA.



2.2. Défis liés à l'utilisation de l'IA en matière de cybersécurité

L'Afrique se trouve confrontée à des défis substantiels dans l'adoption de l'Intelligence Artificielle, le premier étant le coût initial de déploiement. Bien que les coûts des infrastructures informatiques aient diminué avec l'avènement du cloud computing, la migration de cette infrastructure vers des modèles plus avancés demeure onéreuse. Pour appréhender les implications financières de l'IA, il est impératif de plonger dans la complexité de son infrastructure et les ressources nécessaires. Les coûts élevés découlent essentiellement de la nécessité d'une puissance de calcul massive, notamment des processeurs haute performance et des unités de traitement graphique. Cette réalité devient d'autant plus préoccupante dans le contexte africain où les ressources financières sont souvent limitées.

Un deuxième défi réside dans une infrastructure technologique insuffisante, amplifiée par une couverture Internet encore insuffisante. L'accès au haut-débit, essentiel pour les applications basées sur l'IA, demeure marginal, accentuant l'écart entre la demande croissante et la capacité d'infrastructure. De surcroît, la question du coût de connexion demeure un enjeu majeur, nécessitant une accessibilité accrue compte tenu des revenus médians modestes.

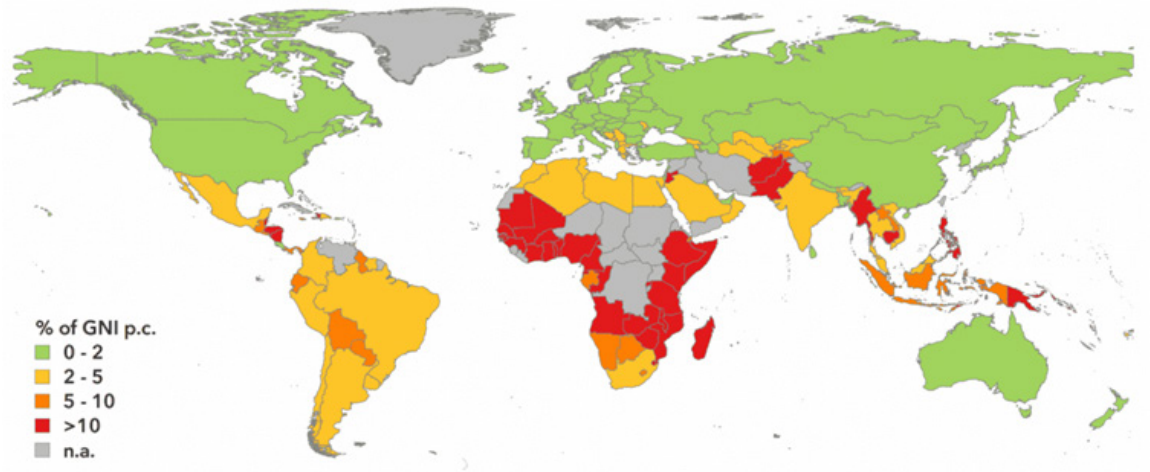


Figure 5. Accessibilité du coût de l'internet haut débit fixe par rapport au revenu national brut par habitant - Union Internationale des Télécommunications (UIT) [24]

Outre ces défis majeurs, la pénurie de talents qualifiés constitue un troisième obstacle significatif. La fuite des cerveaux, résultant de la difficulté pour la recherche universitaire de rivaliser avec les institutions étrangères, compromet la rétention des esprits innovants au niveau local. Cette situation crée un déséquilibre, obligeant certains à dépendre de géants internationaux, engendrant ainsi un appauvrissement pour les acteurs locaux engagés dans la formation des jeunes talents.

Selon un rapport de 2017 de PwC[25], l'IA a le potentiel de contribuer à 15,7 % du PIB africain, d'ajouter une valeur de 1,2 milliard de dollars et de créer jusqu'à 20 millions d'emplois en Afrique d'ici 2030. Ces chiffres illustrent la manière dont l'IA peut servir de catalyseur à l'innovation et à la croissance en Afrique, soulignant par la même occasion l'importance d'encourager l'adoption de l'IA et de développer les compétences requises pour tirer pleinement parti de son potentiel.

Enfin, la cybersécurité émerge comme une préoccupation cruciale. Malgré l'augmentation des cyberattaques, seules 4% des entreprises en Afrique francophone disposent d'un budget spécifiquement alloué à la cybersécurité. Ces budgets, souvent insuffisants, présentent une répartition non-optimale, avec seulement 35% dédiés à la sécurité des infrastructures IT et 5% à la sécurité des données, à la détection des incidents, à la surveillance des menaces, ainsi qu'à la gestion des identités et des accès selon une étude menée par Deloitte[26]. Cette lacune de préparation expose les acteurs à des risques considérables, soulignant l'urgence de renforcer les mesures de protection face à l'évolution rapide du paysage cybernétique.

[24] Global Connectivity Report 2022, Union internationale des télécommunications (UIT), 2022.

[25] « Sizing the prize : What's the real value of AI for your business and how can you capitalise? », PwC, 2017.

[26] « Maturité cybersécurité 2021 afrique francophone », Deloitte, 2021.

2.3. Opportunités offertes par le déploiement de l'IA

Par ailleurs, malgré de nombreux défis, l'Intelligence Artificielle offre des opportunités stratégiques pour renforcer la cybersécurité, notamment à travers des domaines clés. L'analyse des risques constitue l'une de ces perspectives, où l'IA peut scruter de vastes volumes de fichiers à intervalles réguliers, identifiant ainsi les risques potentiels et décelant de nouvelles menaces en assimilant les données acquises au cours de cyberattaques antérieures.

De fait, l'IA s'avère être un outil de choix dans la détection des vulnérabilités, permettant de fortifier les défenses contre les cybercriminels et la cybercriminalité. En effet, elle offre une capacité proactive en surveillant en temps réel les activités réseau, permettant ainsi une détection, une prévention et une riposte efficaces face aux menaces numériques émergentes.

Développer des systèmes de détection des intrusions plus efficaces. Les systèmes de détection des intrusions traditionnels utilisent des règles prédéfinies pour identifier les menaces. L'IA peut être utilisée pour développer des systèmes plus intelligents, qui peuvent apprendre et s'adapter aux nouvelles menaces. La détection basée sur le deep learning[27] permet en l'occurrence aux entreprises d'ajuster de façon continue les paramètres de détection en utilisant l'analyse comportementale pour identifier les anomalies dans les systèmes informatiques.

— L'amélioration du processus de prévention des cybermenaces

Grâce à l'analyse préventive et à l'utilisation d'algorithmes d'apprentissage automatique, l'IA peut traiter de grandes quantités de données pour identifier des modèles et tendances qui peuvent ensuite être utilisées pour prédire les risques de sécurité futurs. L'association de la cybersécurité et de l'IA permet une collecte plus rapide des données. Cela rend la réponse à la gestion des incidents plus dynamique et plus efficace. Les professionnels de la sécurité n'ont plus besoin d'effectuer des tâches manuelles et chronophages, ce qui leur permet de se concentrer sur des activités plus stratégiques qui ajoutent de la valeur à l'entreprise.

Cette démarche permet aux entreprises de prendre des mesures proactives pour atténuer ces menaces en amont. Alors que les cybercriminels conçoivent des vecteurs d'attaque de plus en plus sophistiqués, les organisations sont vulnérables aux menaces inconnues qui pourraient causer des dommages massifs aux réseaux. L'IA fournit une solution pour cartographier et prévenir les menaces inconnues, y compris les vulnérabilités qui n'ont pas encore été identifiées ou corrigées par les fournisseurs de logiciels. Cette approche défensive proactive est essentielle pour garder une longueur d'avance sur les cybercriminels.

[27] Le deep learning est une méthode qui permet aux ordinateurs d'apprendre à partir de données, en utilisant des structures appelées réseaux de neurones.

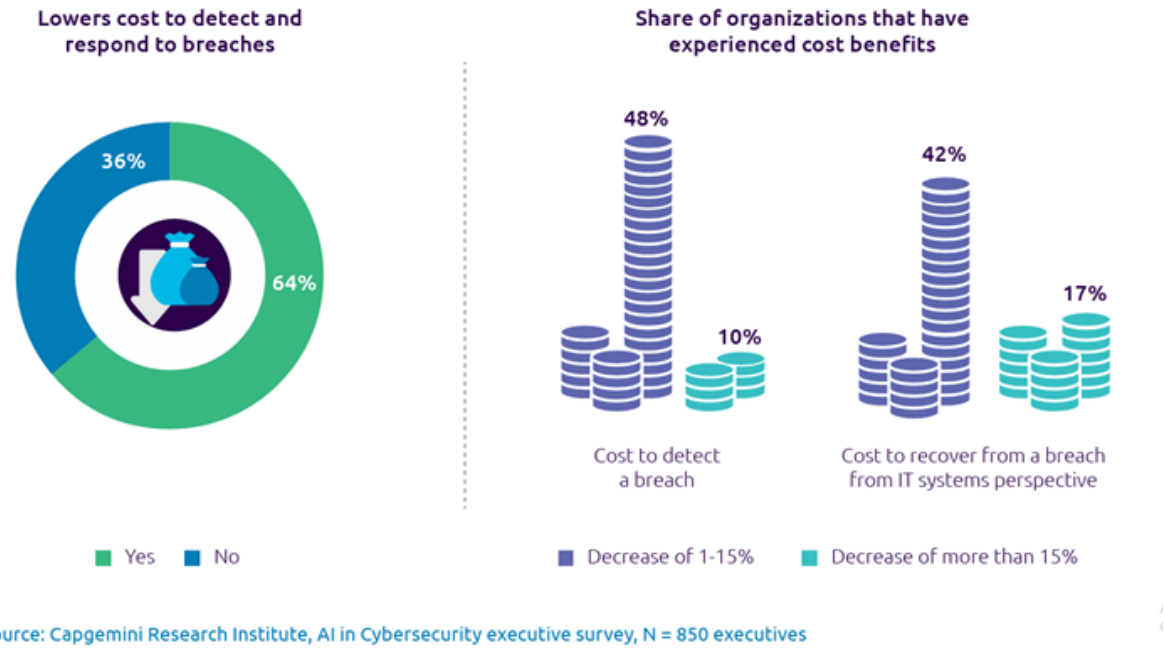
— La réduction du temps de réponse aux cybermenaces

Les solutions de cybersécurité traditionnelles peuvent être coûteuses pour les entreprises et les gouvernements africains. Ces solutions peuvent nécessiter des investissements importants en capital et en ressources humaines.

L'IA peut aider à réduire les coûts de la cybersécurité en automatisant les tâches et en améliorant l'efficacité des opérations. Grâce à la rapidité de l'IA dans le traitement de gros volumes de données et l'automatisation des processus de détection, les entreprises peuvent identifier les vulnérabilités plus rapidement, raccourcissant considérablement le temps de réponses des équipes de sécurité aux cyberattaques.

— La réduction des coûts liés à la cybersécurité

La mise en œuvre de l'IA dans ce contexte présente une panoplie d'avantages significatifs pour les organisations cherchant à gérer efficacement leurs risques, mais l'impact le plus visible à moyen et long terme sera celui de la réduction des coûts d'opération liés à la cybersécurité. Elle émerge comme une solution prometteuse pour réduire considérablement les coûts liés à la cybersécurité en améliorant l'efficacité opérationnelle des équipes de sécurité face aux cyberattaques. Cette rapidité dans le traitement de données massives permet non seulement une détection plus précoce des menaces, mais elle contribue également à minimiser les dépenses en ressources humaines et en investissements technologiques, offrant ainsi une approche rentable pour renforcer la sécurité des entreprises et des gouvernements face aux cybermenaces.

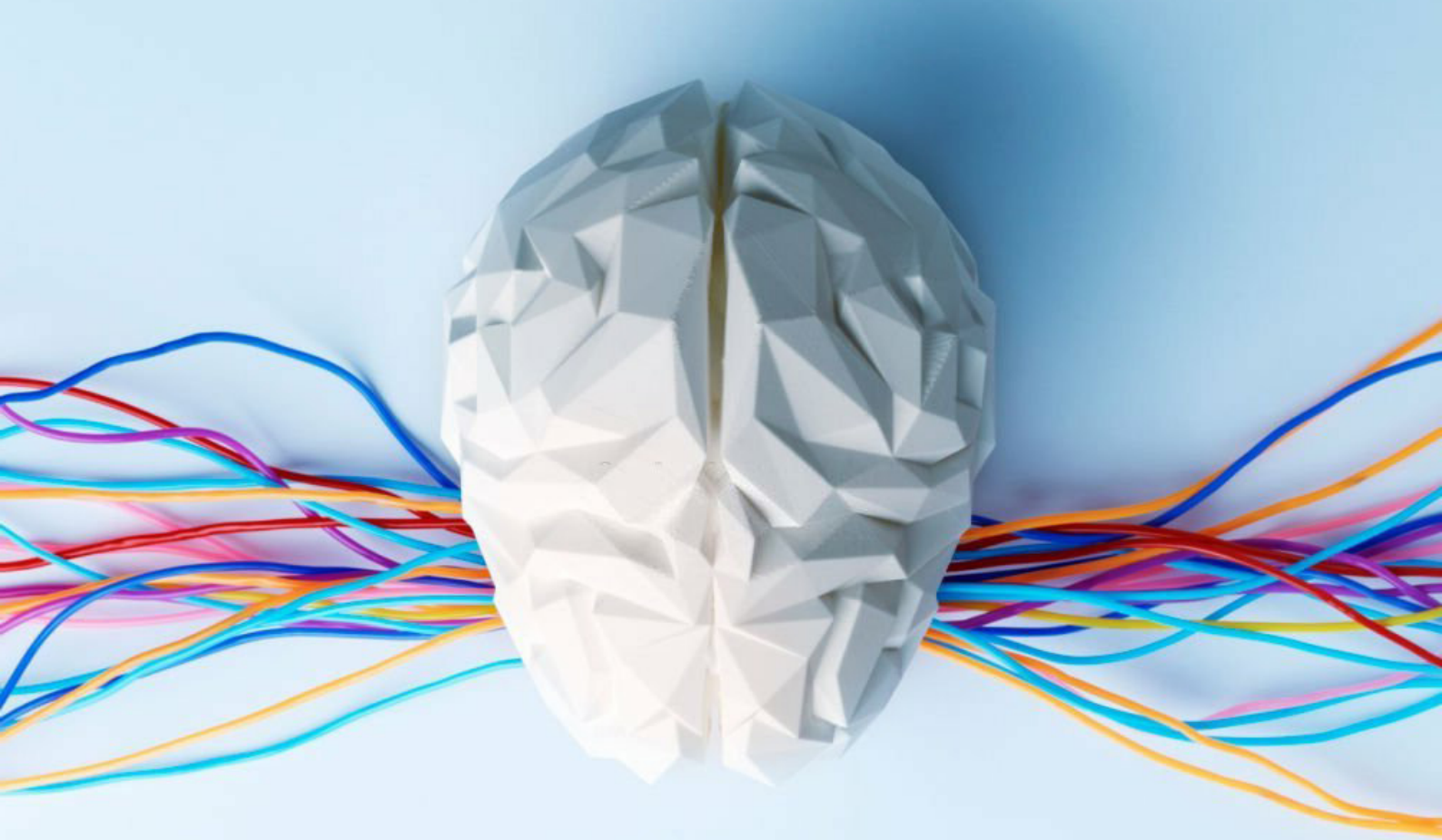


Source: Capgemini Research Institute, AI in Cybersecurity executive survey, N = 850 executives

Figure 6. Le recours à l'IA dans le domaine de la cybersécurité réduit le coût de détection et de réponse aux failles de sécurité

L'utilisation judicieuse des systèmes d'Intelligence Artificielle se révèle être un atout considérable dans le domaine de la cybersécurité, offrant des capacités avancées de détection automatique des cybermenaces, d'alerte précoce, de reconnaissance de nouveaux logiciels malveillants et de protection accrue des données sensibles au sein des entreprises.
Dans cette dernière partie, des propositions seront faites pour permettre à l'Afrique sur le long terme de saisir les opportunités qu'offre l'Intelligence Artificielle.

3 Perspectives futures en matière d'Intelligence Artificielle et de Cybersécurité en Afrique



Partenaire Thought Leadership du Cyber Africa Forum (CAF) 2023

Eviden (an Atos business) propose une approche unique et cohérente, liant sécurité et business, centrée sur la protection des données et la prévention. Vous bénéficierez d'une expertise fondée sur des années d'expérience, s'appuyant sur des solutions et des services de sécurité répondant aux exigences de vos organisations.

Partenaire de confiance, Eviden conçoit, développe, exploite et maintient des solutions numériques de pointe alliant puissance de calcul, sécurité et intégration de systèmes.

Avec sa forte expertise technologique et plus de 6500 spécialistes cybersécurité dans le monde, Eviden est l'une des seules ESN mondiale à proposer un portfolio cybersécurité alliant expérience et innovation avec les technologies cryptographique post-quantum et GenAI, son intelligence artificielle générative.

85 % des cyberattaques peuvent être évitées avec des mesures appropriées de gestion des risques.
Detect early. Respond swiftly.

Atos

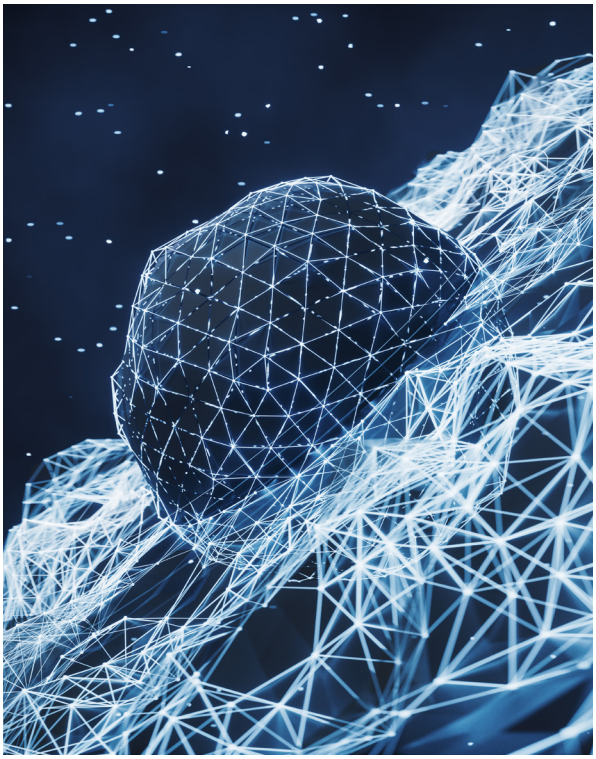
www.atos.net

En Afrique, l'IA et la cybersécurité ont de beaux jours devant eux. L'IA a le potentiel de transformer la cybersécurité en Afrique, en aidant à relever les défis spécifiques de la région et à protéger les entreprises, les gouvernements et les citoyens africains contre les cyberattaques.

L'avenir de l'Intelligence Artificielle et de la cybersécurité en Afrique se profile à travers plusieurs axes stratégiques cruciaux. Dans une interview donnée au magazine Forbes Afrique en 2022, Nathalie KIENGA, présidente d'honneur de Ciberobs – Make Africa Safe a identifié les problèmes de gouvernance, les failles de l'infrastructure et les failles humaines comme les trois principaux maillons faibles des entreprises africaines face aux cyberattaques[28].

3.1. Mise en place de normes règlementaires pour une utilisation responsable de l'IA

Tout d'abord, la mise en place de normes réglementaires émerge comme un impératif majeur afin d'encadrer l'utilisation de l'IA de manière responsable. Cette démarche vise à établir des fondements éthiques et juridiques, indispensables pour guider le développement technologique tout en préservant les valeurs sociétales. Les organisations développant et déployant des systèmes d'IA devraient intégrer des principes tels que la transparence, la responsabilité et la confidentialité dans leurs politiques et leurs pratiques.



La transparence joue un rôle clé, en exigeant que les systèmes d'IA soient compréhensibles et explicables. Les développeurs devraient documenter le processus de prise de décision des algorithmes, permettant ainsi une évaluation externe de leur équité et de leur fiabilité. De plus, la responsabilité doit être intégrée dès la conception, en identifiant clairement les parties prenantes responsables de la conception, du déploiement et de la maintenance des systèmes d'IA.

La confidentialité des données est un autre aspect crucial. Les organisations doivent garantir des pratiques de collecte, de stockage et de traitement des données respectueuses de la vie privée. Cela implique souvent la mise en œuvre de mesures de sécurité robustes pour éviter tout accès non autorisé.
Sur le plan légal, l'établissement de cadres réglementaires clairs est essentiel. Les gouvernements Africains et les organismes de réglementation devraient élaborer des lois spécifiques encadrant l'utilisation de l'IA, définissant les droits et responsabilités des parties prenantes. Ces réglementations pourraient couvrir des domaines tels que la protection des consommateurs, la responsabilité civile et l'utilisation éthique des données.

Enfin, la mise en place de mécanismes de gouvernance et de supervision est cruciale pour garantir le respect des principes éthiques et des réglementations. Cela peut impliquer la création d'organismes indépendants chargés de surveiller l'utilisation de l'IA, d'auditer les systèmes existants et de conseiller sur les meilleures pratiques.

[28] « La cybercriminalité a coûté à l'Afrique 4,12 milliards de dollars en 2021 », Forbes Afrique, 2022.

En somme, garantir l'utilisation de l'Intelligence Artificielle dans un cadre éthique et respectueux exige une collaboration étroite entre les gouvernements, l'industrie et la société civile. Les principes éthiques, les normes légales et les mécanismes de gouvernance doivent travailler de concert pour façonner un avenir où l'IA contribue positivement à la société tout en préservant les valeurs fondamentales.

3.2. Renforcement des infrastructures pour faciliter le déploiement de l'IA

Parallèlement, le renforcement des infrastructures constitue une composante essentielle pour l'implantation de l'Intelligence Artificielle. La création d'une base solide favorise le déploiement efficace de l'IA à travers le continent africain. Cela englobe non seulement la connectivité, mais également la modernisation des réseaux et des systèmes, créant ainsi un environnement propice à l'émergence et à la croissance des technologies intelligentes.

En investissant de manière stratégique dans ces domaines, les pays africains peuvent créer un écosystème propice à l'innovation, à la croissance économique et à l'inclusion numérique, positionnant ainsi le continent en tant qu'acteur majeur dans le paysage mondial de l'IA. Ces investissements peuvent également favoriser le développement de l'Internet des Objets (IoT)[29] et des technologies connexes, créant ainsi une base solide pour les applications d'IA axées sur la collecte et l'analyse de données en temps réel.

Par ailleurs, le déploiement réussi de l'IA en Afrique dépend également de la sécurité des données. Des infrastructures robustes en matière de cybersécurité sont essentielles pour protéger les informations sensibles traitées par les systèmes d'IA. Investir dans des technologies de sécurité de pointe et former des experts en cybersécurité garantit que les données personnelles et professionnelles sont protégées contre les menaces potentielles, renforçant ainsi la confiance des utilisateurs et des entreprises dans l'utilisation de l'IA.

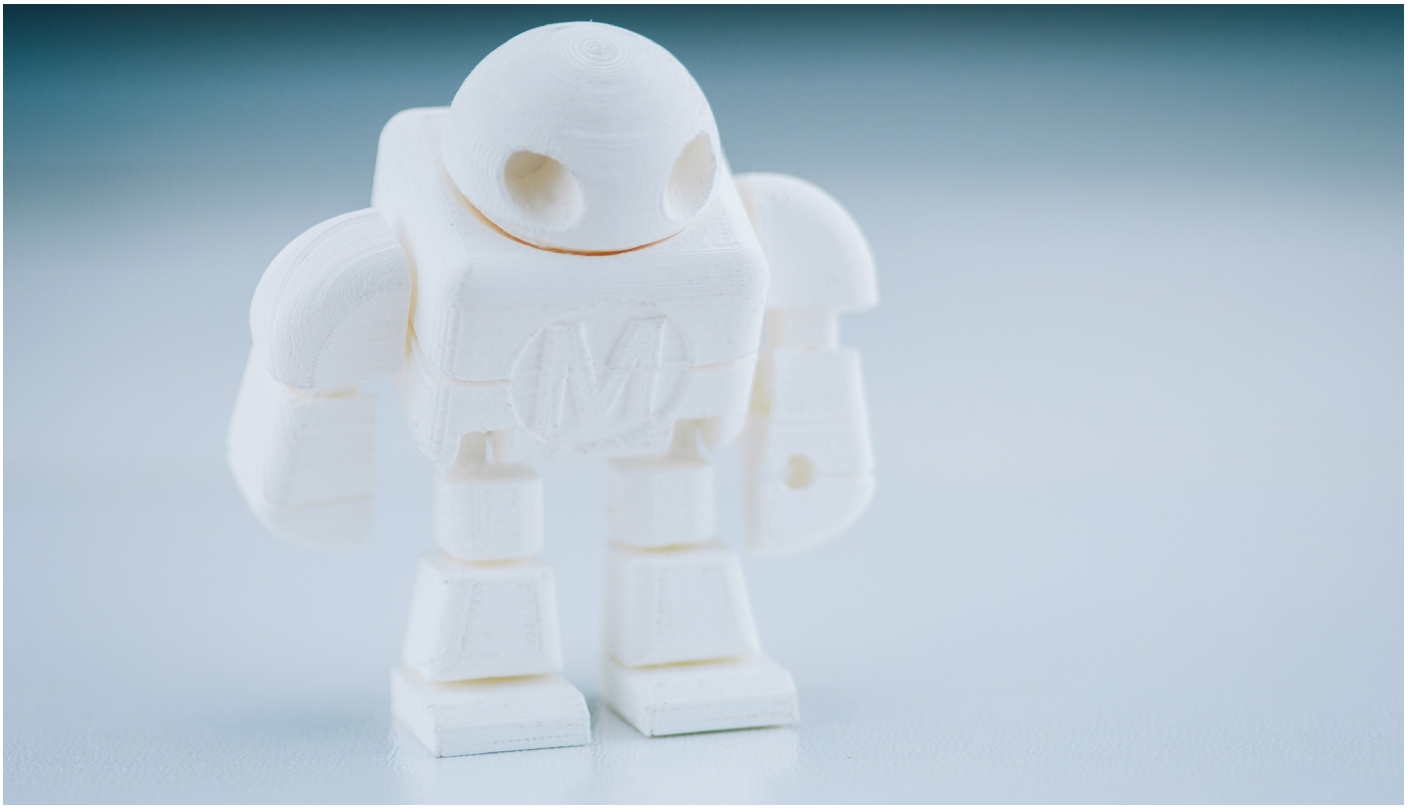
3.3. Formation du capital humain sur l'inclusion de l'IA dans la sécurité numérique

En marge de tout cela, il faut rappeler que l'éducation et la formation demeurent des aspects cruciaux du renforcement des infrastructures pour l'IA en Afrique. En établissant des programmes de formation spécialisés et en facilitant l'accès à des ressources éducatives de qualité, les pays peuvent développer une main-d'œuvre compétente et prête à relever les défis technologiques de l'IA. Cela stimule non seulement la croissance de l'industrie de l'IA, mais encourage également l'innovation locale en permettant aux talents africains de jouer un rôle actif dans le développement et l'application de nouvelles solutions.

La formation du capital humain demeure incontournable, particulièrement en ce qui concerne l'inclusion de l'IA dans la sécurité numérique. La montée en compétences des acteurs clés, qu'ils soient professionnels de la sécurité informatique ou décideurs politiques, devient impérative. Cette formation vise à garantir une compréhension approfondie des enjeux liés à l'IA, tout en insistant sur la nécessité de concilier innovation technologique et préservation de l'intégrité numérique.

Tout d'abord, les professionnels de la cybersécurité doivent acquérir des compétences spécialisées pour comprendre et contrer les menaces émergentes liées à l'IA. Cela inclut la maîtrise des techniques de détection des attaques basées sur l'IA, la compréhension des vulnérabilités spécifiques aux systèmes d'IA, et la mise en œuvre de stratégies de protection efficaces.

[29] Interconnexion d'objets intelligents qui échangent des données via internet.



D'autre part, sensibiliser les utilisateurs finaux revêt une importance cruciale. Les programmes de formation en sécurité numérique doivent s'efforcer d'informer les individus sur les meilleures pratiques relatives à la sécurité en ligne, couvrant divers aspects tels que la gestion des mots de passe et la reconnaissance des tentatives de phishing. En ce qui concerne l'Intelligence Artificielle, il est impératif que les utilisateurs acquièrent une compréhension fondamentale des technologies sous-jacentes, ainsi que de leurs avantages et risques, afin de prendre des décisions éclairées.

Cette sensibilisation est également promue par des initiatives telles que Ciberobs Make Africa Safe, qui se positionne en tant que premier observatoire de la cybersécurité en Afrique avec son évènement Cyber Tour qui consiste à faire la sensibilisation dans les établissements sur la cybersécurité et les dangers liés au numérique et le Cyber Africa Forum (CAF) organisé par Ciberobs Consulting, un rendez-vous incontournable traitant des enjeux de sécurité et de confiance numérique en Afrique.

Les formations devraient également accorder une importance particulière à l'éthique de l'IA. Il est essentiel que les professionnels de l'informatique et les décideurs soient instruits sur les implications éthiques de l'utilisation de l'IA, en mettant spécifiquement l'accent sur des valeurs telles que la transparence, la responsabilité et l'équité. Cela favorise la création d'une culture organisationnelle intégrant des considérations éthiques de manière intrinsèque dans le développement et le déploiement des systèmes d'IA. Des initiatives telles que l'Agence Afria, qui vise à rendre l'IA accessible à tous, s'inscrivent également dans cette perspective éthique en cherchant à étendre les bénéfices de cette technologie de manière inclusive.

En outre, les programmes de formation peuvent encourager l'innovation responsable en stimulant la créativité tout en sensibilisant aux risques potentiels. Les développeurs d'IA devraient être formés à concevoir des systèmes qui minimisent les biais, protègent la vie privée et sont conformes aux réglementations en vigueur.

La collaboration entre les institutions éducatives, les organismes gouvernementaux et l'industrie est essentielle pour élaborer des programmes de formation complets et actualisés. Ces formations peuvent être dispensées à travers des ateliers, des cours en ligne et des certifications, fournissant ainsi des ressources accessibles à tous les niveaux de compétence.

Partenaire Thought Leadership du Cyber Africa Forum (CAF) 2023

“

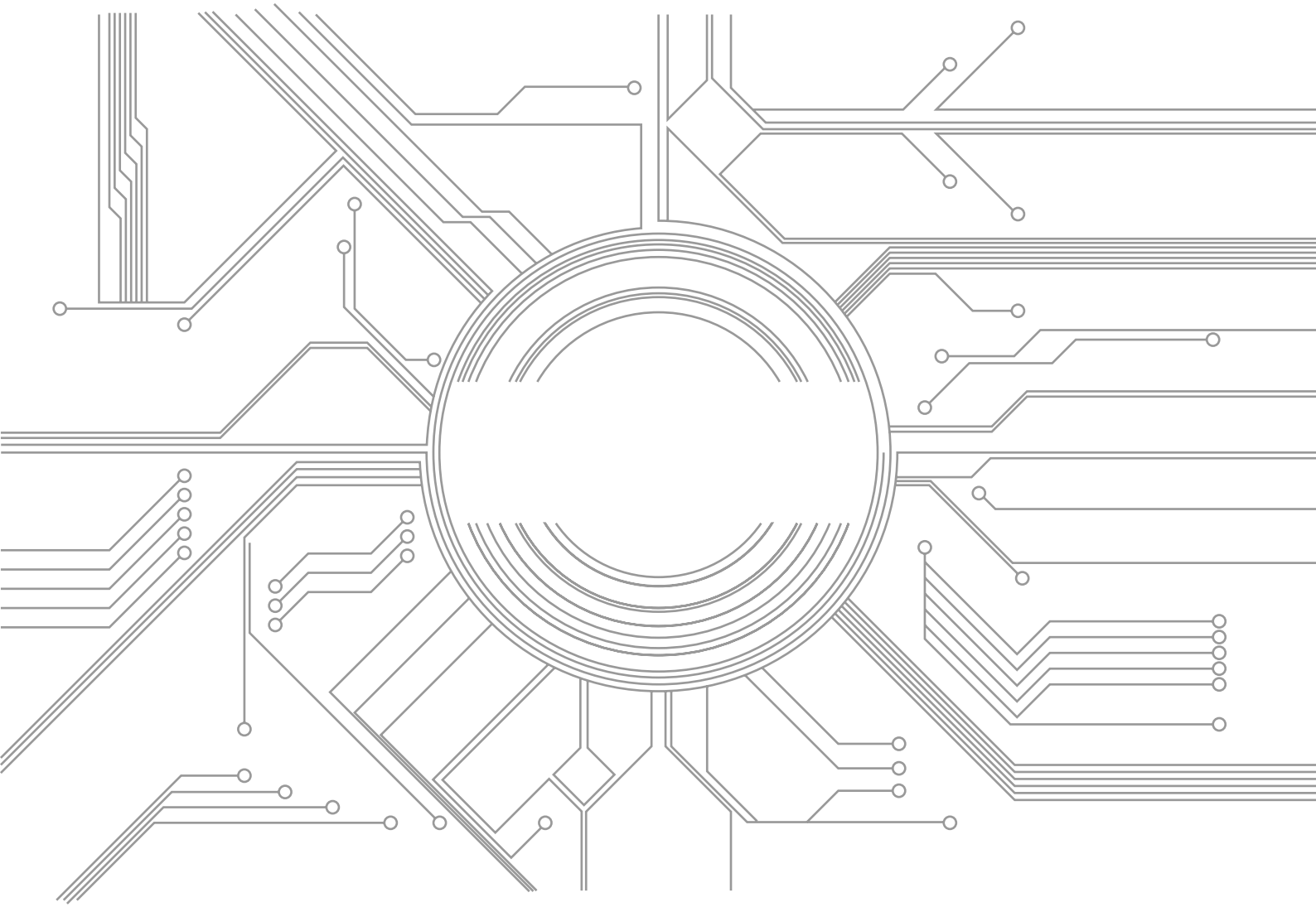
La collaboration étroite entre les acteurs du secteur public et privé revêt une importance cruciale. Il est essentiel de reconnaître que seul, il est impossible de faire face efficacement aux cyberattaques et aux nouvelles menaces qui émergent chaque jour. Il devient incontestable qu’une réforme s’impose, favorisant la synergie entre les différents intervenants pour renforcer notre capacité collective à répondre de manière efficace.

fygytech

Conclusion

L'inclusion de l'Intelligence Artificielle dans la cybersécurité en Afrique de l'Ouest offre des opportunités significatives, mais aussi des défis cruciaux. Le paysage actuel révèle des cyberattaques impactant financièrement la région et des menaces complexes contre les infrastructures critiques. Cependant, l'IA peut atténuer ces risques en renforçant la détection et la réponse aux menaces. L'édification d'un avenir durable en matière d'IA et de cybersécurité en Afrique requiert donc une approche holistique, intégrant des normes réglementaires, un renforcement des infrastructures et une formation ciblée du capital humain. Ces piliers convergent vers l'établissement d'un écosystème technologique robuste et éthique, propice au développement durable du continent.

In fine, le succès de la cybersécurité en Afrique de l'Ouest dépend de l'approche équilibrée de l'intégration de l'IA. Les défis ne doivent pas décourager, mais plutôt inspirer des actions concertées. Avec une réglementation adéquate, le renforcement technique et la formation, la sous-région pourrait réussir à relever les enjeux liés à la cybersécurité grâce à l'IA. Cette tendance renforcerait ainsi sa position dans le monde numérique en constante évolution.



Bibliographie

CYENTIA INSTITUTE, « Cybersecurity Incidents in Industrial Operations », Rockwell Automation, 2023. https://www.rockwellautomation.com/en-us/campaigns/cyentiareport.html

« Cybersecurity Threatscape of African Countries 2022–2023 », Positive Technologies, 2023. https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/

« Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research », sur Check Point Blog [en ligne], publié le 13 juillet 2023. https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

« Cost of a data breach 2023 », IBM Security, 2023. https://www.ibm.com/reports/data-breach

« OPERA1ER: Ceux qui jouent à Dieu sans y avoir été autorisés », Group-IB, 2022. https://www.group-ib.com/resources/research-hub/opera1er-fr/

« Global Connectivity Report 2022 », Union internationale des télécommunications (UIT), 2022. https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022

« Maturité Cybersécurité 2021 Afrique Francophone », Deloitte, 2021. https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/articles/maturite-cybersecurite-2021-afrique-francophone.html

« 2023 Official Cybercrime Report », Cybersecurity Ventures, 2023. https://www.esentire.com/resources/library/2023-official-cybercrime-report

« Global Risks Report 2023 », sur World Economic Forum [en ligne], [consulté le 20 novembre 2023]. https://www.weforum.org/publications/global-risks-report-2023/

« Artificial Intelligence (AI) In Cybersecurity Market 2032 ». https://www.precedenceresearch.com/artificial-intelligence-in-cybersecurity-market

« 2023 Mid-Year Horizon Report: The State of Cybersecurity in Healthcare », Fortified Health Security. https://fortifiedhealthsecurity.com/healthcare-cybersecurity-report-annual-horizon-reports/

« Sizing the prize : What's the real value of AI for your business and how can you capitalise? », PwC. https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

Articles de presse

« Au Sénégal, l'État ciblé par une cyberattaque » [en ligne], JeuneAfrique.com, mai 2023. https://www.jeuneafrique.com/1448977/politique/au-senegal-letat-cible-par-une-cyberattaque/

AJAYI Wale, « The Nigeria Data Protection Act, 2023 - KPMG Nigeria », sur KPMG [en ligne], publié le 12 septembre 2023. https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023.html

KOACI, « Côte d'Ivoire : Nouvelle loi sur la cybercriminalité, toute image à caractère de pornographie infantile désormais punie d'un à six ans et jusqu'à 40 millions d'amende », sur KOACI [en ligne]. https://www.koaci.com/article/2022/11/24/cote-divoire/societe/cote-divoire-nouvelle-loi-sur-la-cybercriminalite-toute-image-a-caractere-de-pornographie-infantile-desormais-punie-dun-a-six-ans-et-jusqua-40-millions-damende_164951.html

« Vent de panique à l'Union africaine après une nouvelle cyberattaque » [en ligne], Le Monde.fr, 25 avril 2023 https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvelle-cyberattaque_6170976_3212.html

« CSA, Chamber of Telecommunications collaborate on cyber security regulations » [en ligne], MyJoyOnline, avril 2023. https://www.myjoyonline.com/csa-chamber-of-telecommunications-collaborate-on-cyber-security-regulations/

« Afrique du Sud - Life Healthcare frappé par des cyberattaques », sur BusinessFrance.fr [en ligne]. https://www.businessfrance.fr/afrique-du-sud-life-healthcare-frappe-par-des-cyberattaques

Divers

« Significant Cyber Incidents | Strategic Technologies Program | CSIS ». https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

« Case Study 17: Port of Durban, South Africa », Building Capacity to Manage Risks and Enhance Resilience, UNCTAD, 2023. https://resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa

Membres de l'association Ciberobs
Ensemble nous pouvons #MakeAfricaSafe

Franck KIÉ
Président

Nathalie KIENGA
Présidente d'honneur

Yena KIGNAMAN-SORO
Vice-présidente

Mohamed KABA
Secrétaire général

Sylvestre KABORE
Secrétaire général
adjoint - Trésorier

Amadou T. DIAWARA
Responsable des programmes et contenus

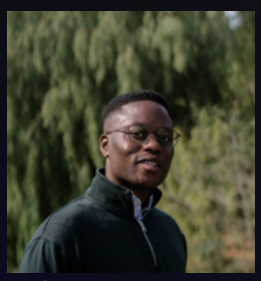
Ansah Y. KAMARA
Responsable de la communauté

Driss GHARMOUL
Responsable de l'orientation stratégique

Karl-Hervé SEHR
Responsable communication

Brice KOFFI
Responsable adjoint des programmes et contenus

Mariam A. TRAORE
Responsable adjointe de la communauté



Axel NDILO
Responsable adjoint de l'orientation stratégique

Alassane FANNY
Membre de la communauté

Marie-Eve LIDA
Chargée de communication

Radiatou OURO-GBELE
Chargée de communication

Issa LASSISSI
Membre de la communauté