Journal de Recherche
Multidisciplinaire
ISSN : 3088-5205
https://jorep.net

Volume : 1
Numéro : 3
Année : 2025
Mois : 5

Évolution des cybermenaces et stratégies de défense pour les entreprises et institutions en Afrique de l'Ouest

Sawadogo Guéswendé Samuel Junior
Doctorant, Département de Sciences et technologies, option : Intelligence artificielle, Université Lisala, RDC

RÉSUMÉ

L'essor des technologies de l'information a offert de nombreuses opportunités aux entreprises et aux institutions. Il a transformé la manière dont les citoyens accèdent à l'information et aux services, créant ainsi des opportunités économiques. Cependant, cette expansion rapide s'accompagne de défis, tels que les cyber menaces, qui évoluent elles aussi. Pour garantir la sécurité des services et des informations aux utilisateurs, les entreprises et les institutions doivent prendre des mesures pour y faire face. Dans cet article, nous étudions les cyber menaces dans le cyberespace ouest-africain, la cybercriminalité associée et ses effets, ainsi que les stratégies de défense des entreprises et des institutions. Notre étude utilise l'analyse de contenu comme principale source de données pour analyser la cybercriminalité en Afrique de l'Ouest, les menaces et les stratégies de défense des institutions publiques. La sécurité étant un domaine très sensible, nous n'avons pas trouvé d'études spécifiques sur les stratégies de défense des entreprises privées. Cependant, il existe des recommandations pour la protection de leurs infrastructures et de leurs données.

Mots clés : cyber menace ; cyberespace ; Internet des objets ; cyber sécurité

ABSTRACT

The expansion of the usage of information technologies brought a lot of opportunities for companies and institutions. It has transformed the way people access information and services creating economic opportunities as well. On the other hand, this rapid expansion has its challenges such as cyber threats, which are evolving as well. To procure a safe services and information to the users, companies and institutions must take action to face these challenges. In this article, we study the cyber threats in the west African cyberspace, the related cybercrime and their effects and the defense strategies for companies and institutions. Our study uses content analysis as a primary source of data to go through cybercrime in west Africa, the threats and the defense strategies used by public institutions. As security is a very sensible domain, we didn't find studies specifically about defense strategies used by private companies however there are some recommend measures they can take for protecting their infrastructures and data.

Keywords: cyber threat; cyberspace; Internet of things; cyber security

Soumis le : 05 mai, 2025
Publié le : 20 mai, 2025
Auteur correspondant : Sawadogo Guéswendé Samuel Junior
Adresse électronique : samcorpbig5@gmail.com

1. INTRODUCTION

Ces dix dernières années, l'Afrique de l'ouest a fait des avancées significatives dans le domaine des technologies de l'information et de la communication (TIC) portés par des initiatives des secteurs publics et privés visant à améliorer l'infrastructure, la connectivité et les services.

En Novembre 2023, la banque mondiale a approuvé le programme régional d'intégration numérique pour l'Afrique de l'Ouest (DTfA/WARDIP), allouant 266.5millions de dollars pour améliorer l'accès à Internet en Gambie, en Guinée, en Guinée-Bissau et en Mauritanie. Cette initiative vise à promouvoir un marché numérique unique, à rendre les services Internet plus abordables et à favoriser la concurrence entre fournisseurs. Le programme devrait bénéficier à environ 1.3 million de personnes, en mettant l'accent sur la réduction des inégalités entre les sexes en matière de compétences numériques et d'entrepreneuriat. [1]

Des initiatives pour le développement et l'intégration du numériques sont faites non seulement au niveau régional mais aussi au niveau national. C'est le cas du Burkina Faso qui en 2017 a bénéficié d'un financement de 20millions de dollars pour moderniser les services gouvernementaux et améliorer la qualité des ressources humaines. D'autres parts, en Janvier 2024, la Banque Mondiale a approuvé le projet d'accélération numérique avec une dotation de 150millions de dollars pour l'amélioration de l'accès aux infrastructures numériques, en ciblant les populations vulnérables telles que les personnes déplacées internes (PDI) et les communautés rurales. [2]

Dans le secteur privé on peut citer de grandes initiatives telles que celles des entreprises de fintech comme Moniepoint basé au Nigéria qui a pour vision de booster le domaine des paiements digitaux et la banque digitale dans toute l'Afrique [3]

Toutes ces initiatives visent à répondre aux demandes de plus en plus croissantes en matière de digitalisation et de facilité d'accès aux services et aux informations et elle permet également aux entreprises et institutions d'atteindre un très grand nombre de personnes plus efficacement.

Ces innovations nécessitent également des mesures de cybersécurité conséquente pour faire face aux multiples cybermenaces qui existent et qui ne cessent d'évoluer.

La cybersécurité désigne l'ensemble des technologies, pratiques et politiques visant à prévenir les cyberattaques ou à en atténuer l'impact. Elle vise à protéger les systèmes informatiques, les applications, les appareils, les données, les actifs financiers et les personnes contre les rançongiciels et autres logiciels malveillants, les escroqueries par hameçonnage, le vol de données et autres cybermenaces. [4]

Les sociétés et les gouvernements emploient diverses mesures, tels que des mesures de cybersécurité, des cadres juridiques et des campagnes d'éducation et de sensibilisation pour promouvoir un comportement éthique et décourager les intentions malveillantes. La cybersécurité est la protection des individus, des sociétés, des organisations, des systèmes et des technologies contre les activités anormales, elle permet d'assurer le maintien de la confidentialité, de l'intégrité et de la disponibilité des ressources informatiques appartenant à une organisation ou connectées au réseau d'une autre organisation [2].

Dans la suite de notre travail nous explorerons les cybermenaces connues, les tendances en Afrique de l'Ouest et les stratégies de défenses pour les entreprises et les institutions.

1.1 Problématique

La digitalisation et les différentes innovations ne sont pas sans contre-partie. Les entreprises et institutions font face à plusieurs défis tels que :

- L'adoption généralisée du cloud computing qui peut accroître la complexité de la gestion du réseau et augmenter le risque de mauvaises configurations du cloud, d'API mal sécurisées et d'autres voies que les acteurs malveillants peuvent exploiter. [4]
- L'augmentation du travail à distance, du travail hybride et des politiques BYOD (apportez votre propre appareil) signifie davantage de connexions, d'appareils, d'applications et de données que les équipes de sécurité doivent protéger. [4]
- L'Internet des objets (IoT) et les appareils connectés en pleine prolifération, dont beaucoup ne sont pas sécurisés ou mal sécurisés par défaut, peuvent être facilement détournés par des acteurs malveillants. [4]
- L'essor de l'intelligence artificielle (IA), et plus particulièrement de l'IA générative, crée un paysage de menaces entièrement nouveau, que les pirates informatiques exploitent déjà par injection rapide et autres techniques. Selon une étude récente de l'IBM Institute for Business Value, seulement 24 % des initiatives d'IA générative sont sécurisées.[4]

Rendre Internet plus sûr et protéger les internautes est devenu l'un des enjeux de sécurité les plus critiques au monde. Alors que le paysage numérique continue de s'étendre et d'intégrer presque tous les aspects de notre vie, garantir un environnement en ligne sécurisé a des implications considérables pour les particuliers, les entreprises et les nations en matière d'amélioration de la cybersécurité [2].

Les entreprises et institutions adoptent déjà des stratégies de protections pour leurs infrastructures numériques. Toutefois, il est important de connaitre d'une part les cybermenaces existantes et les tendances en Afrique de l'Ouest et d'autres parts les stratégies de défenses pour y faire face.

1.2 Questions de recherche

1.2.1 Question générale

Face à l'évolution rapide des technologies digitales et à l'expansion de l'utilisation d'internet, quelles sont les cybermenaces auxquelles doivent faire face les entreprises et institutions et quelles sont les stratégies de défense ?

1.2.2 Questions spécifiques

- Quelles sont les menaces les plus courantes dans le cyberespace Ouest Africain ?
- Quelles stratégies de défenses sont adoptées ? Cette question explore les innovations en matière de cyberdéfense.

1.3 Objectifs de la recherche

1.3.1 Objectif général

Cette étude a pour objectif général d'étudier les différents types de cybermenaces particulièrement en Afrique de l'Ouest et les stratégies de défenses afin de permettre aux entreprises et institutions d'avoir une vue sur les cybermenaces principales dans la région, les autres cybermenaces connues et d'avoir des recommandations sur les mesures possibles pour une sécurité efficace.

1.3.2 Objectif spécifiques

Nous aurons pour objectifs spécifiques :

- Observer cybermenaces principalement rencontrées en Afrique de l'Ouest
- Etudier les autres cybermenaces connues
- Etudier l'état de la cybersécurité dans la région
- Faire des recommandations de stratégies de défense.

1.4 Hypothèses de la recherche

- Il y aurait un lien entre l'expansion de l'utilisation d'internet et les menaces de cyber sécurités en Afrique de L'Ouest.
- Les entreprises et institutions peineraient à s'adapter à l'évolution des cyber menaces liées à l'expansion rapide de l'utilisation des technologies de l'informations et de la communication.

1.5 Justification de la recherche

Cette recherche s'inscrit dans un contexte où l'évolution des innovations technologiques fait apparaitre de nouveaux défis de cybersécurité auxquelles les entreprises et institutions doivent faire face. Elle répond à un besoin de mise à jour des pratiques de cybersécurité et des stratégies de cyberdéfense face aux cybermenaces qui ne cessent d'évoluer.

2. REVUE DE LA LITTÉRATURE

2.1 Définitions des concepts clés

- Cyber menace: une menace de cybersécurité, ou cybermenace, est une indication qu'un pirate informatique ou un acteur malveillant tente d'obtenir un accès non autorisé à un réseau pour lancer une cyberattaque.
- Cyber espace: Le cyberespace désigne l'environnement virtuel créé par le réseau interconnecté de systèmes informatiques, Internet, les réseaux de télécommunications, les logiciels et autres technologies numériques. 1 C'est le domaine non physique où se déroulent la communication en ligne, l'interaction sociale, l'échange de données, le commerce, le divertissement et diverses activités numériques.
- Internet des objets: L'Internet des objets (IoT) fait référence à un réseau d'appareils physiques, de véhicules, d'appareils et d'autres objets physiques dotés de capteurs, de logiciels et d'une connectivité réseau, leur permettant de collecter et de partager des données.
- Cybersécurité: La cybersécurité désigne l'ensemble des technologies, pratiques et politiques visant à prévenir les cyberattaques ou à en atténuer l'impact. Elle vise à protéger les systèmes informatiques, les applications, les appareils, les données, les actifs financiers et les personnes contre les rançongiciels et autres logiciels malveillants, les escroqueries par hameçonnage, le vol de données et autres cybermenaces.

2.2 Croissance du pourcentage d'utilisation de l'Internet en Afrique de l'Ouest entre 2000 et 2021

Ci-dessous, nous avons un tableau qui donne le pourcentage de la croissance de la connectivité dans la sous-région [5]

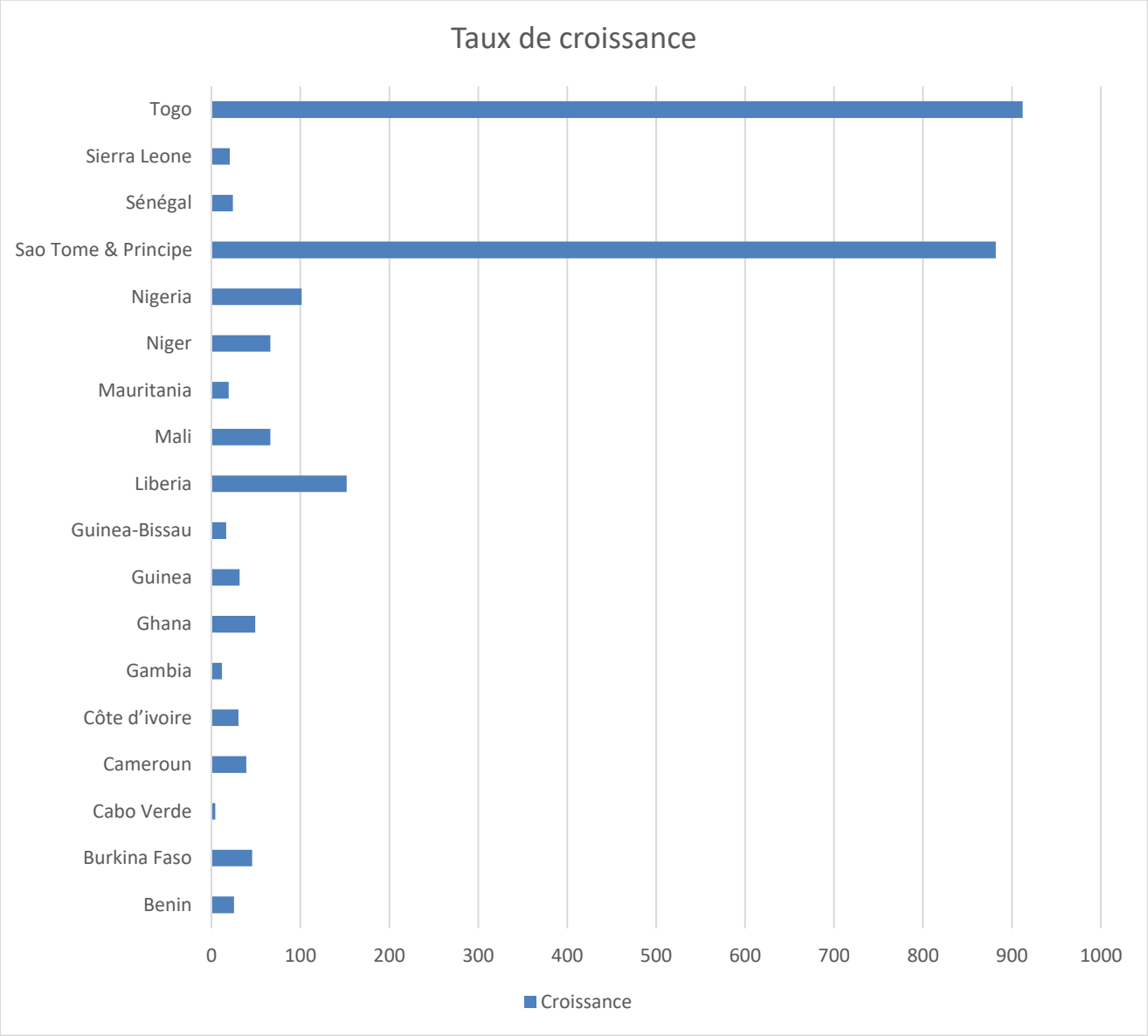

Figure 1: Croissance du pourcentage d'utilisation de l'Internet en Afrique de l'Ouest entre 2000 et 2021. [5]

Ce tableau nous montre que de plus en plus de personnes en Afrique de l'Ouest utilisent internet, ce qui veux dire parallèlement qu'il y a de plus en plus d'informations et d'applications qui sont utilisés et qui nécessitent une sécurité.

2.3 Les menaces et la cybercriminalité en Afrique de l'Ouest

2.3.1 Les principales menaces

La cybercriminalité est plus répandue en Afrique de l'Ouest. Le Nigeria est l'un des pays les plus touché selon des études récentes. Les Cybercriminels ont été en mesure de cibler des personnes et des entreprises au Nigéria grâce à l'expansion des TICs ce qui a eu une grave influence sur les finances, la réputation et la croissance de la région. Il faut noter que les cyberattaques impliquent souvent des collaborateurs de pays extérieurs tels que l'Afrique du Sud et le Cameroon.

Les attaques les plus fréquentes sont les arnaques par imitation et les rançongiciels (ransomware).

Au Nigeria par exemple, les attaques au rançongiciel sur les entreprises ont eu une croissance de 22% en 2020 à 71% en 2021 [6].

A la lumière de cet article nous pouvons dire que les menaces les plus récurrentes en Afrique de l'Ouest sont :

1. Le phishing : C'est un type de cyber attaque basé sur l'utilisation d'email frauduleux, de messages textes, d'appels téléphoniques ou de site webs douteux pour inciter les victimes à partager des données sensibles, télécharger des logiciels malveillants (malwares) ou s'exposer autrement à la cybercriminalité [7]. Il y a trois types de phishing :

- Le spear phishing : Une attaque très ciblée qui manipulent un individu spécifique, en utilisant souvent les détails des profils publics de la victime sur les réseaux sociaux pour rendre l'arnaque plus convaincante.
- Le whale phishing : C'est une attaque de spear phishing visant les dirigeants d'entreprise ou les particuliers fortunés
- Business Email Compromising (BEC) : Arnaques dans lesquelles les cybercriminels se font passer pour des dirigeants, des fournisseurs ou des associés commerciaux de confiance pour inciter les victimes à transférer de l'argent ou à partager des données sensibles [8].

2. Le rançongiciel (ransomware) : C'est un type de logiciel malveillant qui prend en otage les données de la victime en menaçant de les garder inaccessible ou les supprimer à moins que la victime ne paie une rançon au cybercriminel(s). [9]

2.3.2 Autres menaces connues

Selon un article de IBM [8], on peut citer d'autres cybermenaces tels que :

- Les logiciels malveillants aussi appelés malware : Désigne un logiciel créé dans l'intention de compromettre un system informatique ou des utilisateurs. Dans cette catégorie de cybermenace, on peut compter le rançongiciels (ransomware), le cheval de troie, le logiciel espion, et les vers informatiques.
- L'attaque Man-in-the-middle (MITM): Qui consiste pour le cybercriminel à écouter clandestinement sur un réseau afin d'intercepter et relayer des messages entre deux partie et de voler des données. Cette attaque est fréquente sur les réseaux wifi non sécurisés.
- Le déni de service (DoS) : Il consiste à submerger frauduleusement un site web, une application ou un système informatique avec un énorme volume de requêtes pour ralentir le service ou le rendre inaccessible aux bénéficiaires légitimes.
- L'exploit zero-day : C'est un type de cyberattaque qui consiste à exploiter une vulnérabilité inconnue ou pas encore corrigé dans un système informatique.
- Les attaques sur les objets connectés (IoT) : Elles consistent à exploiter les vulnérabilités de certains objets connectés tels que les appareils de maisons intelligentes et de système de contrôle industriels pour prendre contrôle de l'appareil, voler des données ou les utiliser en tant que nœud d'un réseau pour des activités malveillantes.

2.4 Stratégies de cyberdéfenses en Afrique

Dans les pays d'Afrique de l'Ouest, notamment au Nigéria et au Ghana, des législations ciblant la cybercriminalité ont été mises en vigueur. Ces structures juridiques sont essentielles pour orienter la réglementation des cyberactivités. Néanmoins, l'application pratique de ces systèmes juridiques présente des complexités et des obstacles pour les organismes chargés de l'application de la loi. [6]

Selon un article de Yasmine Abdillahi, directrice exécutive des risques de sécurité et de la conformité et responsable de la sécurité chez Comcast, certaines mesures simples peuvent être adoptées par les organisations africaines pour diminuer considérablement et efficacement le volume des cyberattaques. Ces mesures fondamentales définie par le rapport d'investigation des violations de données de Verizon et le rapport de défense digital de Microsoft.[10]

- Créer un inventaire complet des actifs : Le fondement d'une cybersécurité efficace réside dans la connaissance des éléments à protéger. Les organisations doivent répertorier tous leurs systèmes, appareils et données. Elles doivent documenter les éléments de données pertinents afin de faciliter la catégorisation, l'évaluation des risques et la priorisation. Les systèmes obsolètes ou non autorisés sont fréquents dans les bureaux distants, d'où l'importance cruciale d'un inventaire complet.
- Limiter l'accès : Les organisations devraient limiter l'accès aux systèmes au personnel essentiel et appliquer l'authentification multi facteur. En Afrique, où les appareils mobiles constituent souvent le principal moyen d'accès à Internet, l'authentification sécurisée est particulièrement importante.
- Mettre en place une liste d'applications autorisées (whitelist) : Il est important de n'autoriser que les logiciels approuvés dans les systèmes, car cela empêche l'exécution de programmes non autorisés ou malveillants. Ceci est particulièrement utile dans les régions d'Afrique où le piratage de logiciels est répandu et où les utilisateurs pourraient être tentés d'installer des applications non autorisées en raison de contraintes de ressources. Autoriser uniquement les logiciels approuvés réduiraient également les risques associés aux logiciels non autorisés ou obsolètes.
- Normaliser les configurations de sécurité (créer des standards) : les organisations doivent appliquer des paramètres de sécurité uniformes sur tous les systèmes, ce qui minimiserait les vulnérabilités et simplifierait la gestion, garantissant une protection cohérente même dans des emplacements distants.
- Déploiement proactif des correctifs : Il est essentiel de corriger rapidement et systématiquement les vulnérabilités logicielles à l'aide de correctifs. Dans les zones à connectivité limitée, des solutions créatives de distribution et d'application des correctifs

(comme l'utilisation de serveurs de mise en cache locaux ou la programmation des mises à jour en dehors des heures de pointe) peuvent garantir leur application.

- Élaborer des plans de sauvegarde et de récupération robustes : Développer, mettre à jour régulièrement et tester des plans de récupération adaptés aux scénarios de menaces les plus critiques est essentiel pour minimiser les temps d'arrêt en cas de perturbation. Les organisations doivent envisager des solutions de sauvegarde sur site et hors site, en tenant compte des réglementations locales et des enjeux de souveraineté des données susceptibles d'affecter le lieu de stockage des données.

Anastasia Bezborodko,[11] a mené une étude sur la cybercriminalité en Afrique dans la période du premier trimestre de 2023 au troisième trimestre de 2024. Selon l'auteur, le développement rapide des technologies du digital et l'expansion de l'accès à internet a créé plus d'opportunités pour les utilisateurs mais aussi pour les cybercriminels.

En utilisant une approche quantitative dans son article, elle examine les statistiques des cyberattaques en Afrique, les méthodes principales d'attaques, leurs conséquences et donne des solutions possibles pour renforcer la sécurité informatique.

Wasyihun Sema Admass et al. [2], ont publié en 2024 un article concernant l'état de l'art de la cybersécurité, les défis et les orientations futures. Dans cette publications une étude systématique a été menée afin d'identifier les dernières tendances, les défis et l'état de l'art en matière de cyber sécurité.

Yasmine Abdillahi [10], dans un article publié sur Atlantic Council, a donné des recommandations pour rendre plus efficace la cybersécurité en Afrique. L'auteur a détaillé les stratégies qui peuvent être implémentées rapidement pour protéger l'infrastructure digitale des entreprises et institutions. Ces stratégies étant basiques, permettent de protéger efficacement les ressources digitales et faciliter la prise en charge en cas d'attaque informatique.

Victor Adewopo et al. [6], ont publié un article qui explore la cybercriminalité en Afrique de l'Ouest. Cet article fait une revue systématique de littérature sur la prévalence de la cybercriminalité et donne des stratégies de prévention pour les institutions en Afrique de l'Ouest.

3. MATERIEL ET METHODE

3.1 Site de l'étude

L'étude concerne l'Afrique en générale et l'Afrique de l'Ouest en particulier. Les documents analyses sont :

- Les articles et publications web sur les cybermenaces et la cybersécurité en Afrique et en Afrique de l'Ouest si existant.
- Les articles sur les cybermenaces connues
- Les articles sur la cybercriminalité en Afrique et en Afrique de l'Ouest si existant

3.2 Méthodologie

Comme méthode de recherche, nous avons utilisé l'analyse de contenu. Elle consiste à analyser systématiquement des contenus textuels, visuels ou multimédias afin d'en dégager des tendances, des thèmes ou des significations. Cette méthode peut être appliquée aussi bien qualitativement que quantitativement.

3.3 Type d'étude

Il s'agit d'une étude exploratoire qui nous permet d'identifier les cybermenaces et les stratégies de défenses.

4. RESULTATS

Cette étude met en évidence les défis que posent les cybermenaces en Afrique. Selon l'article de Anastasia Bezborodko,[11] le nombre de cyberattaques exécutées avec succès à l'encontre des organisations est de 89% et ceux sur les individus (les particuliers) de 11%. Les institutions publiques et les organisations financières sont les cibles principales dans la région avec des taux d'attaques réussies de 29% et 22% respectivement.

Nous avons ci-dessous, nous avons une figure qui présente les cyberattaques affectant les entreprises et institutions ainsi que les individus :

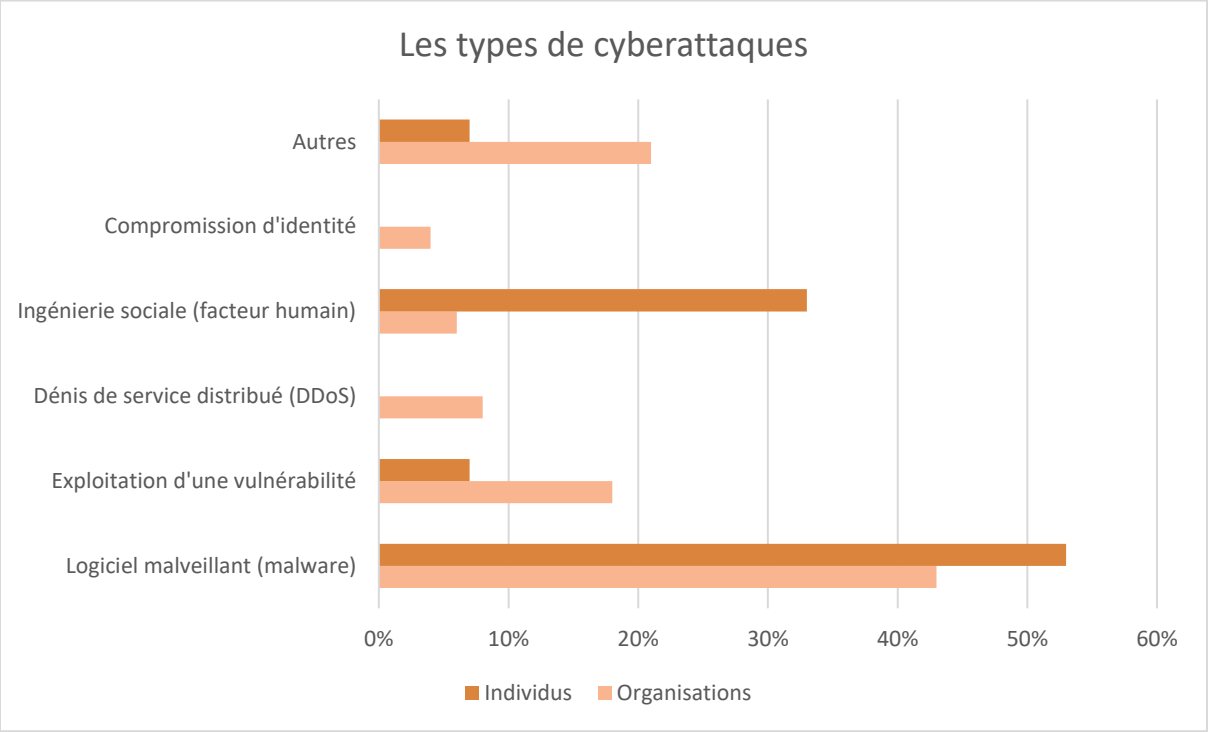

Figure 2: les cyberattaques affectant les entreprises et institutions ainsi que les individus

5. DISCUSSION DES RESULTATS

Notre étude nous a montré que l'utilisation d'internet en Afrique de l'Ouest a connu une expansion rapide qui a transformé la manière dont les usagers accèdent à l'information et aux services. Cette expansion a créé des opportunités telles que les e-commerces, les transactions en lignes etc. A côté de cette expansion de l'utilisation d'internet, nous avons vu aussi que la cybercriminalité est de plus en plus grande et de plus en plus grave dans la région Ouest Africaine. Ce qui vérifie notre première hypothèse selon laquelle il y a un lien étroit entre l'expansion de l'utilisation d'internet et l'évolution des cyber menaces.

Nous avons aussi vu que les cybercriminels ont pu exploiter les vulnérabilités et faire des dégâts notamment au Nigeria. Ce qui vérifie notre seconde hypothèse selon laquelle les entreprises ont du mal à s'adapter à l'évolution de ces cyber menaces.

Enfin, notre dernier diagramme nous donne un aperçu de la situation de la cybercriminalité en Afrique. Cela montre que les cybermenaces évoluant rapidement permettent aux agents malveillants de compromettre les organisations et les individus. Il est donc impératif de continuellement mettre à jour les pratiques de sécurité pour y faire face d'une part et d'autre part, avoir des protocoles qui permettent d'anticiper les vecteurs d'attaques.

6. CONCLUSION

Ces dix dernières années, les technologies de l'information et de la communication font partie de plus en plus du quotidien des usagers en Afrique de l'Ouest. Cela a permis de pouvoir donner un accès facile aux informations et aux services. Cela a aussi permis aux entreprises et institution de se moderniser. Toutefois, ces évolutions viennent avec leurs défis.

Nous avons vu que l'expansion de l'utilisation d'internet veut aussi dire plus d'équipements à protéger, un grand volume d'informations sensibles à sécuriser. Il est donc impératif pour les entreprises et institutions de mettre en place des stratégies de défense pour rendre les services et les ressources plus sûres pour les usagers.

Malgré les stratégies d'adaptation et les mesures de sécurité des entreprises, des vulnérabilités apparaissent suivant l'évolution. En Afrique de l'Ouest, ces vulnérabilités ont pu être exploités par les cyber criminels et on fait beaucoup de dégât en terme de finances et de destruction de réputation. Notre étude nous a permis de faire le point de l'évolution des menaces et des stratégies de défense pour les entreprises et institutions.

En conclusion, nous pouvons affirmer que des propositions sont faites et des cadres légaux sont mis en place par les états pour rendre le cyber espace Ouest africain plus sûr.

7. RECOMMANDATIONS

Les stratégies de défense proposées par Yasmine Abdillahi que nous avons décrit plus haut permettent d'avoir une infrastructure informatique robuste, résiliente et facile à prendre en charge en cas de cyberattaques.

A cela, nous pouvons ajouter les recommandations suivantes :

- Mettre en place un protocole de sécurité qui devra être déployer pour chaque micro service et équipement ajouté à l'infrastructure informatique.
- Sensibiliser et former le personnel afin de les équiper à se protéger des cyberattaques exploitant le facteur humain.
- Les équipes de sécurités doivent régulièrement faire un suivi des systèmes et une révision des protocoles de sécurité au moins une fois par an.
- Mettre en place un protocole pour la gestion des BYOD (bring your own device) pour le personnel qui travaillent avec leur propre matériel informatique.

CONFLITS D'INTÉRÊTS

Aucun conflit n'est signalé dans notre travail.

RÉFÉRENCES BIBLIOGRAPHIQUES

- World Bank Group, (2023). Accelerating Digital Transformation in West Africa, consulté le 02 Avril 2025, https://www.worldbank.org/en/news/press-release/2023/12/01/accelerating-digital-transformation-in-west-africa
- Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro (2024), Cyber security: State of the art, challenges and future directions
- Reuters, (2024). Google among investors putting $110 million into Nigeria's Moniepoint, consulté le 02 Avril 2025, https://www.reuters.com/technology/google-among-investors-putting-110-million-into-nigerias-moniepoint-2024-10-29/
- IBM, (2024), What is cybersecurity?, consulté le 02 Avril 2025, https://www.ibm.com/think/topics/cybersecurity
- Statista, (2022), Percentage change in internet usage in West Africa between 2000 and 2021, by country, consulté le 05 Avril 2025, https://www.statista.com/statistics/1139345/internet-growth-in-west-african-countries/
- Victor Adewopo et al., (2024). A Comprehensive Analytical Review on Cybercrime in West Africa
- IBM, (2024), What is phishing?, consulté le 09 Avril 2025, https://www.ibm.com/think/topics/phishing
- IBM, (2024), Types of cyberthreats, consulté le 09 Avril 2025, https://www.ibm.com/think/topics/cyberthreats-types
- IBM, (2024), What is ransomware?, consulté le 09 Avril 2025, https://www.ibm.com/think/topics/ransomware
- Atlantic Council, (2024), Effective cybersecurity in Africa must start with the basics, consulté le 10 Avril 2025, https://www.atlanticcouncil.org/blogs/africasource/effective-cybersecurity-in-africa-must-start-with-the-basics/
- Anastasia Bezborodko, (2024), Cybersecurity threatscape for African countries: Q1 2023–Q3 2024, consulté le 02 Mai 2025, https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024