Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 3, No. 3, Mai 2025

Enjeu de l'intelligence artificielle dans la cybersécurité : L'intelligence artificielle représente-t-elle un risque ou une opportunité dans la cybersécurité ?

ELIFA Fehmi

Abstract: AI and cybersecurity can go hand in hand. AI can be used to strengthen cybersecurity, but it also represents a risk when exploited by attackers.

Keywords: **AI, cybersecurity, Attack, hacking, incident.**

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**15373396**

1 Introduction

Aujourd'hui, le monde est devenu un village global et interconnecté par la technologie. Cette dernière joue également un rôle très important en répondant aux besoins de l'être humain. On parle notamment des nouvelles technologies de l'information et de la communication (NTIC), qui englobent divers domaines comme l'intelligence artificielle, le cloud, l'IoT (Internet des objets), la 5G, la cybersécurité, ...

Les NTIC font partie intégrante de la vie courante de tous les acteurs (États, organisations, entreprises et individus).

Dans ce chapitre, nous allons découvrir deux domaines : l'intelligence artificielle et la cybersécurité, en répondant aux questions :

- **Qu'est-ce que la cybersécurité?**
- **Quels sont les types d'attaques cyber?**
- **Quels sont les domaines dans lesquels l'intelligence artificielle intervient?**
- **Quel est l'enjeu de l'intelligence artificielle dans la cybersécurité?**

2 Qu'est-ce que la cybersécurité?

2.1 Le Mot cybersécurité:

Le terme cybersécurité est construit à partir du préfixe « **cyber »** et du mot **« sécurité ».**

Cyber (d'origine grecque) : Qui est un préfixe qui participe à la construction de beaucoup d'autres concepts liés à l'informatique et aux activités rendues possibles par les technologies du numérique et de l'Internet.

Sécurité : Quant à elle renvoie aux procédés permettant de la garder secret. [1]

2.2 Définition de la cybersécurité:

La cybersécurité est la pratique qui consiste à défendre les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. Elle est également connue sous le nom de sécurité des technologies de l'information ou de sécurité de l'information électronique. Le terme s'applique à divers contextes, des entreprises à l'informatique mobile, et peut être divisé en quelques catégories communes. [2]

2.3 L'éthique de la cybersécurité:

L'objectif principal de la cybersécurité est de sécuriser les données, les systèmes informatiques et les réseaux (logiciels et matériels) qui ont certainement une valeur économique. Grâce à cette valorisation, les pratiques de la cybersécurité visent avant tout à garantir l'intégrité, la fonctionnalité et la fiabilité des institutions humaines qui s'appuient sur ces données, systèmes et réseaux.

On peut même évoquer le bonheur de l'être humain en utilisant ses propres données en toute sécurité. Prenons l'exemple d'un hôpital qui utilise les DMI (dossiers médicaux informatisés). Le responsable de la sécurité est chargé de protéger le réseau et les données critiques contre les attaques. La vie des patients, leur santé, voire leur survie, peuvent dépendre de votre succès ou de votre échec.

Cet exemple est très particulier, mais les professionnels de la cybersécurité sont également primordiaux pour la protection des électeurs, des investisseurs, des utilisateurs de cartes de crédit, etc.

Le responsable de la sécurité n'intervient pas pour protéger uniquement les données des individus. Il peut aussi assurer la prévention des attaques cyber et contre les menaces afin de protéger les données confidentielles des entreprises et des sociétés (les grands projets, les inventions, ...) ainsi que celles des organisations de l'État (les élections, les données des habitants, ...).

Malheureusement, dans ce domaine, il n'est pas évident d'avoir les bonnes valeurs. Il y a les sollicitations, les tendances politiques et sociales qui poussent les attaquants à aborder les informations confidentielles de leurs victimes.

2.4 Concept de la cybersécurité :

La cybersécurité est différente de la sécurité informatique. Il s'agit d'un domaine plus complexe et plus vaste qui nécessite de solides connaissances. Elle présente des enjeux économiques, stratégiques et politiques qui dépasse la sécurité des systèmes d'information. Ainsi, l'identification des vulnérabilités et la prévention des cyberattaques ne sont pas les seuls objectifs de la cybersécurité. Les principes de base de la cybersécurité comprennent également la gestion des accès, la sécurité des systèmes, des réseaux et des applications, ainsi que la protection des données. Au sein de chaque organisation, il est possible de définir une politique de sécurité pour garantir la sécurité des flux de données. Cette politique met en œuvre les mesures de sécurité au sein de l'organisation afin de protéger la confidentialité, la disponibilité et l'intégrité des données et des ressources sensibles. Elle dépend de la taille et de la hiérarchie de l'organisation. Évidemment, tous les employés, sans exception, doivent être conscients de leur responsabilité et s'en acquitter.

En effet, dans certaines entreprises, la responsabilité de la sécurité peut être confiée à toute une équipe composée d'un directeur de la sécurité, ***d'un responsable de la sécurité*** **(CSO : CHIEF SECURITY OFFICER)** ou ***d'un responsable de la sécurité et de l'information*** **(CISO : CHIEF INFORMATION SECURITY OFFICER).** Dans les grandes entreprises et les compagnies, on trouve également le ***système des opérations de sécurité*** **(SOC : SECURITY OPERATIONS SYSTEM)**, lieu où travaillent les professionnels de la sécurité, divisés en deux équipes **(RED TEAM et BLUE TEAM)** ou trois équipes **(RED TEAM, BLUE TEAM et PURPLE TEAM)**.

- **RED TEAM** (l'équipe rouge) est l'équipe offensive, qui réalise des attaques sur le système et le réseau pour découvrir les défaillances et les points faibles du système.
- **BLUE TEAM** (l'équipe bleue) est l'équipe défensive qui cherche les nouvelles vulnérabilités pour anticiper les attaques et les menaces.
- **PURPLE TEAM** (l'équipe violet) est un mélange des deux équipes précédentes.

Tout ce qui est mentionné ci-dessus concerne la cybersécurité interne. Il existe aussi une autre équipe, indépendante et externe, spécialisée dans la réponse aux incidents cybernétiques. Elle s'appelle ***équipe de réponse aux incidents cybernétiques*** **(CIRT** : **CYBER INCIDENT RESPONSE TEAM)** ou ***équipe d'intervention en cas d'urgence informatique*** **(CERT : COMPUTER EMERGENCY RESPONSE TEAM)**. Elle intervient en cas d'attaque et de vulnérabilité qui a dépassé les capacités du SOC de l'entreprise. C'est comme la protection civile. Mais avant cela, lors du développement des systèmes d'information et dans les nouveaux cabinets de développement, on utilise de nouveaux termes comme :

- **DevOps** : Ce terme est né de l'union de deux mots, « développement » et « opérations ». L'objectif de ce poste est de favoriser la collaboration entre les équipes de développement et les équipes opérationnelles. Il permet effectivement de réaliser des économies, mais il offre surtout un gain de temps considérable, notamment au niveau des tests unitaires. [3]
- **DevSecOps** : dans le DevOps, la sécurité est prise en charge à la fin du processus de développement. Dans le DevSecOps, les pratiques de sécurité sont appliquées tout au long du processus, du début à la fin. [4]

3 Les types d'attaques:

Il n'existe pas de liste finale des types d'attaques cybernétiques, mais voici tous les types connus à ce jour :

3.1 Logiciels malveillants (MALWARE):

Le terme « malware » désigne un logiciel nuisible, comme les **virus (VIRUSES)**, les **vers (WORMS)**, **les chevaux de Troie (TROJAN)**, **les logiciels publicitaires (ADWARE)** et **les logiciels d'espionnage (SPYWARE).**

- Les virus et les vers se répliquent et se propagent eux-mêmes, soit en modifiant, soit en détruisant des données.
- Les chevaux de Troie se déguisent en logiciels légitimes afin de tromper les utilisateurs à installer des logiciels malveillants.
- Les logiciels de publicité et d'espionnage, quant à eux, collectent des informations sur les utilisateurs sans leur consentement et peuvent perturber l'expérience utilisateur en affichant des publicités indésirables.

3.2 Déni de service (DoS : DENIAL OF SERVICE) et Déni de service distribué (DDoS : DISTRIBUTED DENIAL OF SERVICE) :

C'est la méthode la plus efficace et la plus simple. Les stratégies **DoS** et **DDoS** figurent parmi les meilleures stratégies offensives. L'objectif de cette attaque – DoS – est de surcharger la machine victime (souvent un serveur) ou le réseau par un trafic volumineux, ce qui rend la ressource indisponible. Le DDoS est une attaque Dos, mais elle est souvent générée par des machines infectées appelées **botnets (zombies)**. Ce qui rend le service indisponible pour ces utilisateurs.

3.3 Hameçonnage (PHISHING) :

L'hameçonnage consiste à accéder aux données confidentielles de la victime via des e-mails frauduleux. Ces e-mails semblent légitimes pour tromper les utilisateurs et les inciter à divulguer ces informations, comme leurs mots de passe, leurs numéros de carte de crédit ou leurs données bancaires. Ils peuvent contenir des pièces jointes infectées par des malwares ou des liens vers des sites malveillants. Il existe plusieurs types d'attaques de ce type :

3.3.1 Hameçonnage de lance ou ciblé (SPEAR PHISHING):

C'est l'hameçonnage instantané pour une cible bien déterminée.

3.3.2 Hameçonnage baleinière (WHALE PHISHING) :

C'est l'hameçonnage par lance, mais la cible diffère. Dans cette attaque, on cible une baleine à titre d'exemple, un directeur ou un manager.

3.3.3 Hameçonnage avec SMS (SMS PHISHING) :

C'est l'hameçonnage par SMS.

3.3.4 Hameçonnage vocal (VISHING) :

C'est l'hameçonnage, mais réalisé par voix. On peut utiliser l'intelligence artificielle pour imiter la voix d'une telle personne afin de piéger la victime.

3.4 Attaque de l'Homme au milieu (MitM : MAN IN THE MIDDLE):

Cette attaque consiste tout simplement à intercepter et à modifier les communications entre deux parties. C'est un type d'espionnage numérique qui exploite les réseaux non sécurisés comme les Wi-Fi publics.

3.5 Logiciels Rançons (RANSOMWARE) :

Il s'agit de chiffrer les données ou les fichiers d'une victime, ce qui les rend inaccessibles jusqu'à ce que celle-ci paie une rançon.

3.6 Mise à jour malveillante (MALICIOUS UPDATE) :

Cette attaque se produit lors de la visite d'un site malveillant par l'intermédiaire de plug-ins ou de publicités.

Elle peut se produire lors d'un téléchargement de fichier ou de données depuis un site infecté, ou bien lors du téléchargement de la mise à jour du système d'exploitation.

3.7 Scripts intersites (CROSS-SITE SCRIPTING (XSS)) :

L'attaquant exploite des vulnérabilités dans des applications Web en insérant des codes malicieux, ce qui infecte l'utilisateur de cette application en faisant exécuter ces scripts dans son navigateur.

3.8 Injection SQL :

Dans l'objectif d'exploiter les failles de sécurité dans les applications de bases de données, l'attaquant injecte un code SQL malicieux pour modifier la logique de programmation de cette base.

3.9 Jour zéro (ZERO-DAY) :

Cette attaque correspond aux nouvelles vulnérabilités qui ne sont pas connues et qui ne sont pas encore découvertes. Ils n'ont pas de signatures.

3.10 DNS, usurpation (SPOOFING) et creusement de tunnel (TUNNELING) :

L'attaque DNS consiste à intercepter des données ou à rediriger les utilisateurs vers des sites malveillants.

La DNS usurpation permet à l'attaquant de détourner la requête DNS afin de correspondre un nom de domaine à une adresse IP malveillante.

Le DNS creusement de tunnel utilise les requêtes et les réponses DNS pour y passer discrètement des données malveillantes qui lui permettent d'y accéder.

3.11 Menaces Internes (INSIDER THREATS) :

Ce sont des menaces internes déclenchées par des individus au sein de l'entreprise.

3.12 Usurpation d'identité (IDENTITY SPOOFING) :

L'attaquant cherche à tromper la victime en imitant des sources fiables. Elle peut prendre plusieurs formes telles que l'usurpation d'emails, l'usurpation d'adresse IP et l'usurpation ARP.

3.13 Force brute (BRUTE FORCE) :

Il parvient à deviner les mots de passe en effectuant plusieurs tentatives. Il est efficace contre les mots de passe faibles.

3.14 Écoutes clandestines (EAVESDROPPING ATTACKS) :

L'écoute clandestine (interception des communications) a pour objectif de capturer et d'écouter les échanges de données entre deux parties.

3.15 Détournement d'URL (URL INTERPRETATION) :

L'attaquant essaie de manipuler les requêtes envoyées vers un serveur web en modifiant l'URL afin d'accéder à des pages non autorisées. Par la suite, il redirige les utilisateurs vers des sites malveillants.

3.16 Chaîne d'approvisionnement (SUPPLY CHAIN) :

Les attaquants insèrent des logiciels malveillants dans le code des produits des fournisseurs afin de déborder les données de leurs clients.

3.17 Attaques Web (WEB ATTACK) :

Les vulnérabilités Web **(CROSS-SITE SCRIPTING (XSS) et CROSS-SITE REQUEST FORGERY (CSRF))** représentent des menaces pour la sécurité des applications Web.

Les attaques XSS exploitent des applications web en permettant à des scripts malveillants de s'intégrer dans les requêtes reçues par les utilisateurs (au niveau du navigateur). Les attaques CSRF trompent l'utilisateur d'une application web pour qu'il exécute des actions malveillantes dans l'application à laquelle il est authentifié (au niveau serveur).

3.18 CRYPTOJACKING :

L'attaquant utilise discrètement les ressources informatiques de la victime pour miner des crypto-monnaies (BITCOIN, ETHEREUM, ...). Il ralentit ainsi le système tout en consommant beaucoup d'électricité.

3.19 Détournement de session (SESSION HIJACKING) :

Il s'agit d'une technique permettant à un attaquant de prendre le contrôle de la session Web d'un utilisateur. Elle exploite ainsi des vulnérabilités et des menaces pour la gestion des sessions afin de profiter des identifiants de la victime.

Cette attaque intercepte les cookies de sessions via l'écoute clandestine (**SNIFFING**) en cas d'absence du protocole HTTPS pour chiffrer les données échangées.

3.20 Attaques d'Anniversaire (BIRTHDAY ATTACKS) :

Cette attaque est inspirée du paradoxe des anniversaires : on cherche la probabilité de collisions. Lors d'un anniversaire, on cherche à identifier les personnes qui ont la même date d'anniversaire. On cherche ainsi à trouver dans l'entrée (des données légitimes et malveillantes) deux éléments ayant le même résultat dans la sortie afin de générer des collisions et tromper par la suite les systèmes avec des messages malveillants contenant des données malveillantes.

4 Domaines de l'intelligence artificielle :

L'intelligence artificielle est une technologie qui offre de nombreuses possibilités d'exploitation dans plusieurs domaines de notre vie. Elle joue un rôle de plus en plus important dans de nombreux aspects de notre vie et de notre société. Grâce à l'émergence de nouvelles innovations, elle ne cesse de se développer et de s'améliorer. Voici les domaines dans lesquels l'intelligence artificielle intervient :

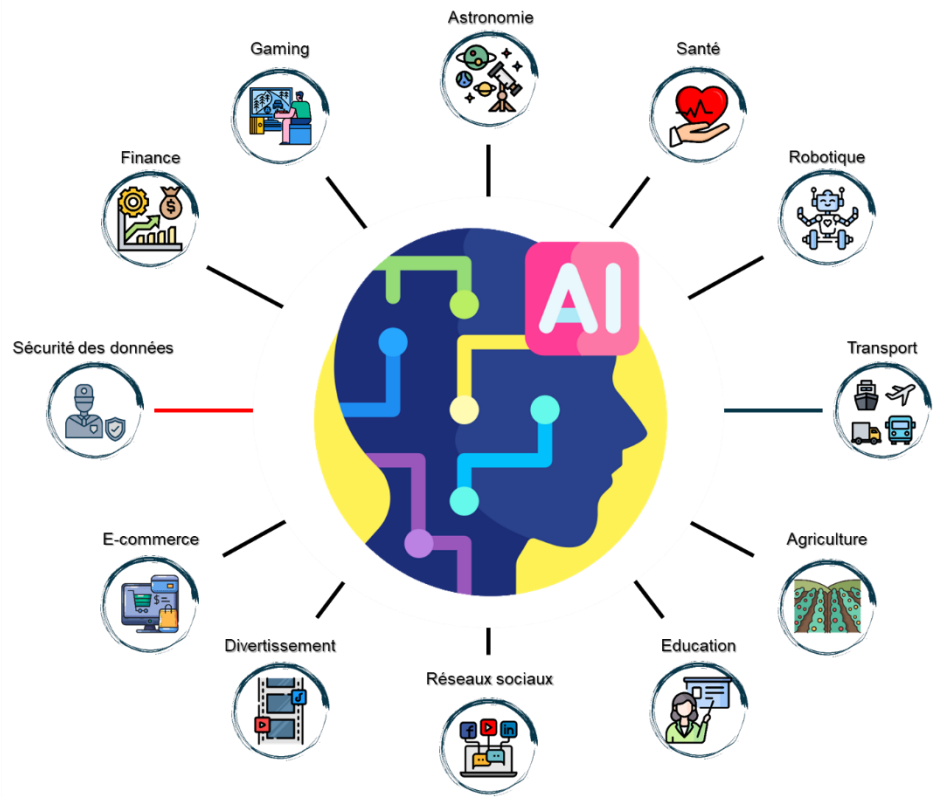

Figure. Domaines de l'Intelligence Artificielle.

- **Finance:** L'intelligence artificielle permet d'améliorer la prise de décision et de mieux réduire les risques dans les transactions bancaires et boursières. Elle est efficace dans l'analyse des données financières afin de déterminer les opportunités d'investissement. Elle garantit la satisfaction des clients en leur fournissant, grâce à l'intelligence artificielle, un service client personnalisé.
- **Gaming:** Les jeux vidéo permettent de développer des compétences sociales et d'apprentissage chez les joueurs de tout âge. Les nouveaux jeux font appel à des algorithmes et à des techniques très élaborées. L'intelligence artificielle peut simuler des comportements intelligents chez eux en lui facilitant la gestion dynamique de l'environnement afin de contrôler ces adversaires et d'adapter le niveau de difficulté.
- **Astronomie:** Les astronomes exploitent l'intelligence artificielle pour découvrir les secrets de la planète et étudier les corps étrangers, ce qui rend leur travail plus facile et plus rapide puisqu'il permet de traiter d'énormes quantités de données. L'intelligence artificielle aide donc à traiter les données par des systèmes automatisés afin de les rendre exploitables dans le cadre de recherches scientifiques. De plus, on utilise l'intelligence artificielle pour rechercher la vie extraterrestre.
- **Santé:** L'intelligence artificielle est utilisée dans le domaine de la santé pour améliorer le diagnostic et le traitement des maladies. Elle permet même l'analyse d'images médicales pour détecter plus efficacement les anomalies. On peut aussi prévenir les maladies. De nos jours, l'intelligence artificielle permet de dispenser des conseils de santé par le biais de consultations vidéos.
- **Robotique:** La robotique garde une place importante dans plusieurs domaines. Les robots sont utilisés aujourd'hui dans la quasi-totalité des industries ainsi que dans la vie domestique. Le développement majeur de la robotique est notamment rendu possible par l'intelligence artificielle. À titre d'exemple, les caméras 2D et 3D sont des outils utilisés dans de nombreux domaines. Les robots permettent ainsi d'automatiser les tâches de production et d'inspection dans l'industrie. On peut utiliser des robots pour optimiser les chaînes d'approvisionnement.
- **Transport:** La fameuse intervention de l'intelligence artificielle dans le domaine des transports concerne les systèmes de conduite autonome, qui visent à améliorer la circulation et à optimiser les réseaux de transport public. On parle aussi aujourd'hui de véhicules connectés qui peuvent utiliser l'intelligence artificielle pour communiquer avec l'infrastructure routière.
- **Agriculture:** Face aux défis de l'agriculture, notamment face à l'effet de serre et à l'augmentation exponentielle de la population mondiale, l'intelligence artificielle demeure une excellente solution. La technologie et la numérisation ont fortement évolué à l'aide de l'intelligence artificielle pour répondre à la demande mondiale. Celle-ci les aide en effet à optimiser leur travail. Grâce à la collecte et l'analyse des informations, à la gestion de l'eau et à l'augmentation des effectifs de production. On peut également parler d'agriculture intelligente en utilisant des drones de surveillance ou d'irrigation.
- **Education:** L'intelligence artificielle permet d'améliorer les méthodes d'éducation en proposant des méthodologies innovantes en matière d'apprentissage et d'évaluation. Elle offre également de nombreux outils qui aident l'apprenant à effectuer des recherches ciblées et à mieux comprendre en moins de temps.
- **Réseaux sociaux:** L'intelligence artificielle aide l'utilisateur de réseaux sociaux à mieux présenter ses données. Elle lui permet également de bien traduire ses données et d'améliorer en temps réel les résultats de ses recherches. L'intelligence artificielle aide également à créer du contenu ciblé et efficace.

- **Divertissement:** L'intelligence artificielle nous permet de découvrir de nouveaux endroits à visiter et de trouver des idées d'activités familières. Elle nous aide également à créer des œuvres d'art, comme de la musique ou de la littérature. Elle nous aide à faire le ménage et à améliorer la sécurité de la maison.
- **E-commerce:** L'e-commerce est l'un des domaines d'utilisation de l'intelligence artificielle. Il est possible d'apprendre grâce à l'expérience d'achat des clients et d'analyser leurs intérêts et leurs besoins. L'IA permet également d'automatiser les tâches commerciales tout en respectant la stratégie marketing de l'entreprise. En se basant sur les données commerciales, on peut créer des entreprises de publicité, surtout dans les réseaux sociaux.
- **Sécurité des données:**

5 L'enjeu de l'intelligence artificielle dans la cybersécurité?

Les domaines de l'intelligence artificielle et de la cybersécurité sont complémentaires, puisqu'on a besoin de l'intelligence artificielle dans la cybersécurité, que ce soit pour attaquer ou pour se défendre. Ainsi, un flux de données sur les menaces ne produit pas automatiquement des renseignements sur les menaces. En reliant les deux sources de renseignements, vous pouvez identifier les objectifs et les tactiques associés à ce groupe et utiliser des contrôles pour atténuer d'autres attaques. La plupart des plateformes de renseignement sur les menaces utilisent une sorte d'intelligence artificielle pour effectuer des analyses de corrélation. La question qui se pose ici est la suivante :

- **L'intelligence artificielle représente-t-elle un risque ou une opportunité dans la cybersécurité ?**

Tout d'abord, les premiers pas d'une attaque cyber commencent par l'ingénierie sociale, qui consiste pour l'attaquant à collecter des informations utiles sur la victime en se basant sur des outils sophistiqués d'intelligence artificielle. En d'autres termes, elle consiste à usurper une identité, à installer un logiciel malveillant ou à divulguer des informations privées ou confidentielles. Par conséquent, l'intelligence artificielle demeure un moteur de l'ingénierie sociale et permet d'améliorer l'efficacité des attaques. L'intelligence artificielle peut traiter un grand flux de données issues de sources diverses, comme les moteurs de recherche et les réseaux sociaux.

Ensuite, l'intelligence artificielle permet d'améliorer des techniques d'attaques déjà utilisées, comme l'hameçonnage (PHISHING), qui consiste à générer des données malveillantes dans des e-mails ou des messages SMS. De plus, comme déjà mentionné, il est possible d'usurper l'identité d'une personne en imitant sa voix et sa signature afin de la piéger et de lui voler ses données confidentielles. Par ailleurs, un hacker peut injecter un code malveillant à travers les textes générés par les outils d'intelligence artificielle, comme le ChatGPT et les chatbots.

D'une part, l'intelligence artificielle est un outil très important et indispensable pour le développement Web, notamment dans l'interfaçage graphique et la gestion des données. Elle aide le développeur à résoudre des problèmes complexes, améliore l'efficacité du code et optimise le développement. D'autre part, un hacker peut créer le même site que l'original afin de rediriger la victime et d'y voler ses données confidentielles. Ensuite, lors de la mise à jour d'un ordinateur portable, d'un smartphone ou d'un iPad, l'hacker peut, à travers cette mise à jour, injecter un code malveillant, soit l'App store, ou même dans l'appareil de la victime.

Par la suite, les hackers peuvent intercepter les communications entre deux internautes ; il s'agit de l'attaque « Homme au milieu » (Man in the Middle). Grâce aux outils développés par l'intelligence artificielle, l'attaquant s'approprie les données de ses victimes pour les exploiter par la suite. Il peut également rediriger une victime vers son propre serveur afin de pirater ce dernier et ainsi accéder à ses données bancaires, par exemple. Cependant, les attaques de rançon se multiplient avec les outils sophistiqués de l'intelligence artificielle.

L'intelligence artificielle nous offre plusieurs solutions avancées d'authentification, telles que l'empreinte digitale. Cependant, le principal problème des scanners d'empreintes digitales est qu'il est possible d'obtenir d'un utilisateur et de créer un moule qui trompent le scanner. Ces problèmes sont traités par des scanners de correspondance veineuse ou de la biométrie vasculaire, mais ceux-ci sont trop chers et nécessitent plusieurs contraintes, ce qui fait perdre beaucoup de temps. Nous avons donc eu recours à la reconnaissance faciale et vocale. Ces technologies peuvent fournir un haut niveau de sécurité par rapport aux mots de passe traditionnels et ainsi protéger nos sites contre les intrus. Dans ce but, les entrées et les sorties des locaux de l'entreprise seront équipées de reconnaissance faciale, et même rétinienne. D'autre part, un logiciel malveillant pirate la reconnaissance faciale depuis l'IPhone pour vider les comptes bancaires de la victime.

6 Conclusion

Pour continuer, l'intelligence artificielle nous aide à résoudre nos problèmes en imitant le raisonnement humain. Cependant, les attaquants profitent de ces faiblesses pour perpétrer des attaques cyber comme la brute force (BRUT FORCE), les scripts intersites (CROSS-SITE SCRIPTING (XSS)), les écoutes clandestines (EAVESDROPPING ATTACKS) et surtout le déni de service distribué (DDOS).

Enfin, l'intelligence artificielle nous aide à développer des outils de sécurité plus efficaces pour lutter contre les menaces et les nouvelles vulnérabilités (ZERO DAY), comme les firewalls de nouvelle génération et les nouveaux **SIEM** (systèmes de gestion des événements et des informations de sécurité). Grâce aux machines d'apprentissage (Machine Learning), il est possible d'étudier le comportement du système afin de capter chaque transaction suspecte ou chaque suspicion de menaces.

REFERENCES

[1] https://www.studocu.com/row/document/universite-pedagogique-nationale/nouveaux-medias/cybersecurite-le-cours-de-nouveaux-medias-presente-aux-etudiants-levolution-des-medias-traditionnels/45989576
[2] https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security
[3] https://www.skills4all.com/metiers/devops-ingenieur/
[4] https://www.crowdstrike.fr/cybersecurity-101/cloud-security/devops-vs-devsecops/