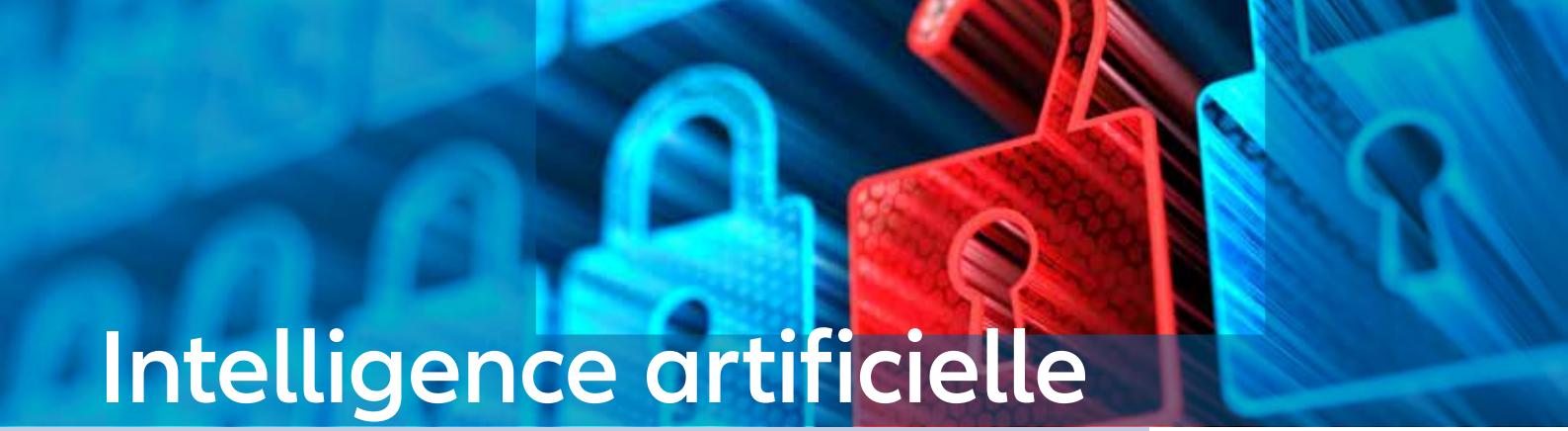

Intelligence artificielle et cybersécurité
Entrez dans une nouvelle ère

fr.allianzgi.com

Active is: ouvrir de nouvelles perspectives

Principales idées

À mesure qu'une part plus importante de nos vies est passée au numérique, la cybersécurité joue un rôle essentiel dans la protection des données et de nos actifs.

L'intelligence artificielle (IA) est parfaitement adaptée à la défense des cybermenaces les plus néfastes dans un environnement en rapide évolution.

Les gouvernements et de nouvelles législations devraient accorder une priorité élevée aux dépenses en cybersécurité des entreprises.

La nouvelle ère de la cybersécurité

La cybersécurité est la pratique consistant à protéger les ordinateurs, les dispositifs mobiles et les autres actifs numériques contre des attaques malveillantes. Au cours de ces dernières décennies, les cyberattaques sont devenues un danger évolutif pour les entreprises et les particuliers. Le développement de la technologie a entraîné une plus forte interconnectivité des systèmes des entreprises ainsi qu'un accroissement de la présence individuelle en ligne. Les cybercriminels capitalisent sur ce changement dans la mesure où les opportunités d'accès ou de destruction de données sensibles sont plus nombreuses. Par voie de conséquence, une cybersécurité efficace devient une nécessité pour les entreprises, toutes tailles et secteurs confondus[1].

Impact de la COVID-19 sur la cybersécurité

La COVID-19 a jeté la lumière sur le manque de préparation des entreprises dans la gestion des problèmes liés à la cybersécurité. Le passage au télétravail et la recrudescence de l'utilisation des canaux numériques ont entraîné un nombre croissant de problèmes liés à la cybersécurité.

De nombreuses entreprises et particuliers se précipitent pour actualiser leurs systèmes et protéger leurs données. Cette très forte augmentation des menaces a accru le besoin de contrôles de sécurité et les tests de vulnérabilité. Les entreprises se tournent de plus en plus vers l'Intelligence artificielle (IA) afin de contribuer à mettre en échec les menaces croissantes de cyberattaques. Il est mathématiquement impossible, même pour les grandes équipes de sécurité informatique des entreprises, de contrôler l'ensemble des menaces et de passer au crible des centaines de milliers de vulnérabilités[2]. C'est la raison pour laquelle l'automatisation par le biais de l'IA et l'utilisation des algorithmes d'apprentissage automatique ou *Machine Learning* sont désormais activement utilisés pour éliminer les menaces cybernétiques. La pandémie de Covid-19 entraîne des changements de comportement à l'égard de la cybersécurité et les entreprises bien positionnées et à même de résoudre certains des problèmes les plus pressants en matière de cybersécurité devraient enregistrer une croissance exceptionnelle.

Les coûts des dommages de la cybercriminalité devraient atteindre 6 000 milliards de dollars d'ici 2021 contre 3 000 milliards en 2015.

Le coût élevé de la cybercriminalité

Parmi les coûts de la cybercriminalité figurent notamment l'endommagement et la destruction de données, le vol de sommes d'argent, la violation de la propriété intellectuelle, le vol de données personnelles et financières, les détournements de fonds, la fraude, les dommages à la réputation et plus encore. Les coûts des dommages de la cybercriminalité devraient atteindre 6 000 milliards de dollars d'ici 2021 contre 3 000 milliards en 2015. Ce changement pourrait représenter le plus grand transfert de richesse économique de l'histoire et serait plus profitable que le commerce mondial des principales drogues illégales[3].

L'IA contribue au renforcement de la cybersécurité

Les entreprises à l'échelle mondiale travaillent d'arrache-pied pour trouver de nouvelles solutions destinées à combattre et à réduire la cybercriminalité. L'IA se révèle être la technologie la meilleure et la plus adaptée à la résolution d'une partie des problèmes les plus difficiles du secteur de la cybersécurité. En utilisant l'IA et le Machine Learning afin d'automatiser la détection des menaces, les entreprises peuvent réagir aux menaces de cyberattaques de manière plus efficace qu'en utilisant les approches logicielles traditionnelles.

Avant 2019, de l'ordre de 20 % seulement des prestataires de services de cybersécurité employaient l'Intelligence artificielle. D'ici la fin 2020, 63 % des sociétés spécialisées dans la cybersécurité envisagent de déployer l'IA au sein de leurs solutions[4].

L'automatisation permet aux entreprises de distinguer les bons des mauvais comportements en utilisant des modèles prédictifs et des données passées. Ces modèles sont suffisamment intelligents pour détecter et empêcher de nombreuses menaces de cybersécurité en temps réel. En éliminant le besoin d'une contribution humaine, les ingénieurs en cybersécurité sont capables de privilégier d'autres aspects de la protection qui pourraient mériter une attention plus particulière. L'IA peut également tirer profit des données sur les cyberattaques actuelles dans d'autres domaines et secteurs à l'échelle planétaire afin d'améliorer constamment les taux d'efficacité et de détection. Veuillez trouver ci-dessous quelques exemples de la manière dont l'IA est actuellement utilisée dans le domaine de la cybersécurité[5] :

Anti-spam : le « Machine Learning » permet de réaliser des filtres plus intelligents afin de détecter automatiquement les spams et les placer dans un « sandbox ».

Biométrie : les techniques d'authentification à l'image des scanners d'empreintes digitales, des visages et de l'iris des yeux sont de plus en plus utilisées au travail et au domicile. L'IA contribue à améliorer la précision de la reconnaissance et procure des informations comportementales destinées au renforcement de la sécurité.

Détection des menaces : la reconnaissance avancée des formes peut détecter les menaces et les virus en temps réel, renforçant ainsi les mesures de sécurité et permettant des réponses plus rapides.

Traitement du langage naturel : l'IA peut s'appuyer sur des informations provenant d'articles et de recherches afin d'apprendre les toutes dernières menaces de sécurité, techniques de hacking et stratégies de prévention.

Détection des bots : les modèles d'apprentissage en profondeur ou *Deep learning* sont en mesure de connaître le comportement des utilisateurs et de détecter les actions inhabituelles. Ces modèles peuvent détecter des bots plus tôt, les distinguer des comptes détenus par des humains et minimiser les menaces.

Confiance zéro : ce modèle de cybersécurité prend comme hypothèse un réseau hostile exposé à des menaces tant externes qu'internes. L'IA et le Machine Learning permettent un contrôle en temps réel des connexions des utilisateurs, de leur localisation, de leurs appareils, de leurs adresses IP et des applications provenant uniquement de sources de confiance.

Cybercriminalité et Internet des objets

Un dispositif basé sur l'Internet des objets (IdO) est un appareil informatique qui transmet des données d'un endroit à l'autre via Internet. Les appareils IdO ont été l'une des principales cibles de la criminalité informatique en 2018. En 2019, les cyberattaques visant ces dispositifs ont bondi de 300 % compte tenu de la prolifération d'appareils numériques dans nos vies[6]. Cette progression a été principalement attribuable aux dispositifs IdO qui étaient plus vulnérables en raison d'anciens firmwares qui n'avaient pas été mis à jour.

D'après Cisco, le nombre d'appareils IdO sera trois fois plus élevé que la population mondiale d'ici 2023[7].

La plupart des dispositifs de l'Internet des objets ont été fabriqués dans l'objectif de proposer une seule fonctionnalité. Ils disposent de très petits systèmes d'exploitation et leur sécurité n'est généralement possible qu'en ajoutant une extension. Dans ce contexte, les appareils IdO ont été extrêmement vulnérables aux cyberattaques par le passé. De nouvelles normes de cybersécurité dans le domaine de l'Internet des objets sont en phase de déploiement afin de mieux protéger ces appareils intelligents.

Une autre tendance qui met en lumière le besoin de cybersécurité est l'adoption rapide du cloud. Le montant total de données stockées dans le cloud, qui englobe les clouds publics opérés par des fournisseurs et les entreprises en charge de réseaux sociaux, les clouds détenus par les gouvernements et les clouds privés, sera 100 fois supérieur en 2021 par rapport à 2019[8]. Les entreprises nécessiteront davantage de solutions sophistiquées en matière de sécurité en raison de cette accélération de l'adoption du cloud.

Gouvernements et amendements législatifs

La législation, à l'image du Règlement général sur la protection des données (RGPD) au sein de l'Union européenne, constitue un moteur des dépenses de cybersécurité engagées par les entreprises. En vertu des règles du RGPD, les entreprises collectant des données sur les citoyens de l'Union européenne (UE) doivent se conformer aux exigences en matière de protection rigoureuse des données des clients même si elles ne disposent pas de présence au sein de l'UE[9]. Le non-respect de ces règles peut donner lieu à de lourdes amendes pouvant aller jusqu'à 4 % du chiffre d'affaires total de l'entreprise visée. D'autres pays à l'échelle mondiale devraient emboîter le pas de l'UE en adoptant des règles et des normes similaires.

Aux États-Unis, l'Association nationale des administrateurs de sociétés (« National Association of Corporate Directors » ou NACD) a appelé les Conseils d'administration des entreprises à renforcer leurs compétences et leurs capacités de gouvernance en matière de cybersécurité[10].

De nouvelles attentes voient le jour à l'égard des Conseils d'administration qui devraient avoir la capacité de comprendre et de gérer les problèmes liés à la cybersécurité. Ce point de vue est partagé par les actionnaires ; 36 % de l'ensemble des propositions actionnariales en 2018 visaient à appliquer des critères de performance sociale et environnementale, dont la cybersécurité et le respect de la vie privée, au calcul de la rémunération des dirigeants.

En outre, le projet de loi « Cybersecurity Disclosure Act of 2019 » est actuellement débattu au Congrès américain. S'il est voté, il imposera aux entreprises cotées d'acquérir une expertise en cybersécurité au sein du conseil d'administration ou de prouver à la Securities & Exchange Commission (SEC) américaine que cette expertise n'est pas nécessaire. 11 Les entreprises ne peuvent plus retarder leurs initiatives de cybersécurité et l'IA s'est avéré être la technologie la plus facile et la plus efficiente afin de contribuer à cette transformation.

Cybersécurité et révolution de l'IA

La sécurité a toujours été essentielle au bon fonctionnement de toute société. À mesure que nous évoluons vers un monde plus numérique, notre manière de mettre en œuvre des mesures de sécurité change et il existe de nombreuses entreprises qui commercialisent de nouvelles solutions pour aider à lutter contre ces menaces. *CrowdStrike** est une entreprise leader de la cybersécurité qui propose des services nouvelle génération dans les domaines de la sécurité des terminaux, de renseignements sur les menaces et de réponse aux cyberattaques. CrowdStrike fournit une plateforme cloud collectant des données sur les cyberattaques et exploite l'IA pour améliorer continuellement le profil de sécurité des dispositifs de ses clients. *Splunk** développe des logiciels qui permettent aux entreprises de rechercher, d'établir des corrélations, d'analyser, de contrôler et de publier des données en temps réel. La technologie Splunk peut représenter une composante clé permettant aux systèmes d'IA de digérer et d'analyser de larges volumes de données non structurées et structurées sur la cybersécurité. Okta* édite des logiciels de cybersécurité destinés à empêcher des usurpations d'identité au moyen de ses solutions d'authentification et d'identité fondées sur le risque qui utilisent le *Machine Learning* et l'IA pour obtenir des informations comportementales dans divers contextes.

Conclusion

Sous de nombreux aspects, l'IA est déjà utilisée pour améliorer la cybersécurité et combattre le cybercrime. Or compte tenu du développement technologique et du passage aux canaux digitaux, elle joue un rôle plus important que jamais. L'automatisation et la détection en temps réel sont primordiales car il s'agit des outils les plus efficaces que les entreprises peuvent adopter pour faire face au nombre croissant de cybermenaces. À l'avenir, la plupart des secteurs et des entreprises de toutes tailles nécessiteront une cybersécurité robuste. Par voie de conséquence, nous sommes d'avis que les investisseurs patients seront récompensés dans leur quête active d'entreprises vouées à jouer un rôle dans la lutte contre le cybercrime.

Allianz Global Artificial Intelligence

L'Intelligence artificielle transforme nos vies et bouscule des secteurs depuis des années. Pourtant, nous n'en sommes qu'aux prémices de ce vaste champ d'opportunités. Notre fonds Allianz Global Artificial Intelligence offre aux investisseurs une exposition mondiale et diversifiée à la thématique de l'Intelligence artificielle. Il n'est pas construit dans le but d'être un fonds investissant dans la technologie.

À noter par ailleurs qu'il investit dans l'ensemble des capitalisations boursières. Toutefois, il privilégie les moyennes et les grandes capitalisations au lieu de se concentrer principalement sur les méga-capitalisations. Plus important encore, nous investissons tout au long de la chaîne logistique, des entreprises technologiques qui développent des infrastructures et facilitent la mise en œuvre de l'IA aux entreprises de nombreux secteurs et industries qui appliquent l'IA à leurs produits, leurs solutions et leurs processus opérationnels. À l'avenir, l'Intelligence artificielle bouleversera chaque pan de l'économie et offrira un vaste champ d'opportunités d'investissement variées à ceux qui possèdent les connaissances et l'expertise nécessaires.

Notre équipe de gestion de portefeuille établie à San Francisco dispose d'un accès sans égal à la plupart des principaux acteurs de ce secteur. Elle peut de sorte engager un dialogue continu avec les acteurs établis et des start-ups et mieux comprendre comment l'IA s'est développée et multipliée. Par ailleurs, la plateforme de recherche mondiale (« Global Research ») d'Allianz Global Investors procure une vision mondiale et sectorielle transversale. Grâce à une connaissance exhaustive de la technologie et des entreprises sous-jacentes, notre équipe est idéalement placée pour comprendre les opportunités que représentent l'Intelligence artificielle dans tous les domaines de l'économie mondiale.

Les bouleversements provoqués par l'IA n'en sont qu'à leurs débuts

- L'IA est en phase rapide de développement et elle est vouée à demeurer un secteur à part entière de l'économie
- Les investissements annuels dans l'IA se sont multipliés par 6 entre 2015 et 2019[10]
- L'IA transforme les modèles économiques et les modes opératoires traditionnels
- Elle a le potentiel d'accélérer l'apprentissage humain et la productivité
- L'IA pourrait contribuer à hauteur de 15 700 milliards de dollars à l'économie mondiale d'ici 2030[11]

Opportunités de croissance sur le long terme

- Indépendamment du climat économique, les pays reconnaissent que leur prospérité future dépend des investissements dans l'innovation
- L'IA représentera un grand bouleversement qui contribuera à moderniser les industries et servira de moteur de croissance économique
- Les investisseurs peuvent participer aux opportunités de croissance à long terme dans l'IA dans l'objectif d'augmenter les performances

Un univers diversifié d'entreprises innovantes

- Notre plateforme de recherche analyse plus de 1 000 entreprises innovantes
- Nous sommes à la recherche d'entreprises vouées à bénéficier :
  a) du déploiement de l'infrastructure des IA,
  b) du développement de logiciels et d'applications en IA,
  c) de l'application de l'IA aux principaux processus opérationnels
- Nous avons construit un portefeuille diversifié composé de 40 à 100 positions dans les entreprises qui satisfont nos critères d'investissement

Pour plus d'informations, veuillez visiter notre site Web :
fr.allianzgi.com

Allianz Global Investors

[1] Digital McKinsey and Global Risk Practice, "Cybersecurity in a Digital Era," McKinsey & Company June 2020. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf

[2] Gauran Banga, "How to Create a Dream Team for the New Age of Cybersecurity." Dark Reading, February 2020. https://www.darkreading.com/cloud/how-to-create-a-dream-team-for-the-new-age-of-cybersecurity/a/d-id/1333849

[3] Cybersecurity Ventures Official Annual Cybercrime Report 2019.

[4] "Reinventing Cybersecurity with Artificial Intelligence," Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[5] Teju Shyamsundar, "AI Is Changing Security—Here's How," Okta Blog, January 2020. https://www.okta.com/blog/2020/01/ai-is-changing-security-heres-how/

[6] Zak Doffman, "Cyberattacks On IoT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims," Forbes, September 2019. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#281bde785892

[7] Cisco Annual Internet Report (2018–2023) White Paper, March 2020 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[8] "Cybersecurity CEO: The World Will Need to Cyber Protect 100X More Cloud Data by 2021," Cybersecurity CEO, Herjavec Group, October 2018. https://www.robertherjavec.com/cybersecurity-ceo-cyber-protect-100x-cloud-data/

[9] Micheal Nadeau, "General Data Protection Regulation (GDPR): What you need to know to stay compliant," CSO, June 2020. https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

[10] "Cyber-Risk Oversight Handbook For Corporate Boards," OAS.

[11] Chenxi Wang, "Corporate Boards Are Snatching Up Cybersecurity Talents," Forbes, August 2019. https://www.forbes.com/sites/chenxiwang/2019/08/30/corporate-boards-are-snatching-up-cybersecurity-talents/#615246a479f5

AdMaster: 1369261. CD 2681: Oct 2020