Intelligence artificielle : amie ou ennemie de la cybersécurité ?

Ludovic HAYE
Sénateur du Haut-Rhin

Par sa capacité à traiter de grands volumes de données [1], l'intelligence artificielle [2] peut être vue comme un allié au service des défenseurs du cyberespace, en particulier pour détecter des menaces émergentes et automatiser les réponses à y apporter. Mais l'IA peut aussi être mise à profit pour attaquer ce cyberespace.

En effet, si l'IA ne révolutionne pas les différents types d'attaques cyber existants, elle risque cependant d'en modifier sensiblement le nombre, mais aussi la sophistication et l'efficacité.
Grande consommatrice de données, l'IA permet désormais aux cyberattaquants de multiplier les vols de données et ainsi de s'auto-alimenter pour être encore plus performante. Un syndrome de Kessler de la donnée volée en quelque sorte.

La simple description de la situation actuelle des menaces dans le cyberespace suffit à comprendre l'intérêt que l'industrie de la cybersécurité porte à l'intelligence artificielle (IA) ; et, par conséquent, les espoirs que placent les entreprises dans ces solutions pour se protéger des cybercriminels et des assaillants voulant s'emparer de leurs données.

Du côté des entreprises, des collectivités et des organisations, ces dernières tentent d'échapper aux menaces, sans cesse plus nombreuses, en appliquant au plus vite des « rustines » logicielles et correctifs en tous genres.

Du côté des cybercriminels, les assaillants sont à l'affût de la révélation des failles affectant les multiples logiciels déployés en entreprise, avec une appétence particulière pour les failles 0-days (sans correctif), plus rares, plus chères mais terriblement efficaces, afin de mieux s'introduire dans les systèmes informatiques.

Concrètement l'IA peut être utilisée pour casser les captchas, ces tests requis pour accéder à certains services Internet et servant à différencier les utilisateurs humains d'éventuels robots malveillants, ou plus simplement pour perfectionner les techniques de phishing (ou hameçonnage par e-mail). En utilisant l'IA pour augmenter la personnalisation des messages malveillants, un chercheur est parvenu à passer d'un taux d'efficacité de 5 % à une proportion

[1] https://dataanalyticspost.com/Lexique/donnees/
[2] https://dataanalyticspost.com/Lexique/intelligence-artificielle-ia/

de 40 %. Autrement dit à tromper huit fois plus d'utilisateurs.

Ainsi, si l'IA peut s'avérer un facteur aggravant des cyberattaques que peuvent subir les entreprises, elle peut aussi s'avérer un allié tout aussi utile qu'efficace.

En effet, dans son fonctionnement intrinsèque, l'IA, par sa capacité à apprendre un contexte donné et donc à y détecter des anomalies, a tout pour être la nouvelle arme fatale des cyberdéfenseurs, en isolant efficacement les comportements anormaux révélateurs d'attaques.

L'intelligence artificielle est porteuse de beaucoup d'espoir grâce à sa capacité à détecter les vraies attaques dont l'entreprise peut être la cible, ainsi que les comportements à risque pour l'intégrité et la confidentialité des données. Sa capacité à traiter des volumes de données gigantesques confère à l'IA un second avantage non négligeable en matière de cyberdéfense.

Avec de telles promesses – capacité à détecter les vraies menaces dans le tumulte cyber ambiant – et un tel besoin du côté des entreprises, il n'est absolument pas étonnant de voir la quasi-totalité de l'industrie de la cybersécurité s'engouffrer dans la brèche. C'est une véritable aubaine marketing pour bon nombre d'éditeurs de logiciels qui, pour certains, appliquent un simple vernis marketing consistant à rajouter des couches d'IA sur des solutions anciennes.

L'IA a un énorme potentiel dans l'automatisation des détections, mais aussi, à court et moyen termes, dans l'optimisation des activités SOC (Security Operations Center) des entreprises, véritables centres opérationnels de cybersécurité, où est agrégé l'ensemble des alertes.

Bien que les attentes que placent les entreprises dans ces technologies soient fortes, parfois disproportionnées, mais somme toute légitimes, elles ne doivent cependant pas aboutir à des investissements hasardeux et donc à des déceptions. Malgré tous les espoirs portés sur l'IA et le Machine Learning[3], ces nouveaux concepts doivent, selon moi, être appréhendés comme des compléments efficaces aux technologies actuelles de détection de menaces, et non comme des moyens de substitution, du moins, à court ou moyen termes. Cette complémentarité représente une réelle plus-value dans l'analyse comportementale des menaces.

L'utilisation de l'IA doit venir en renfort des équipes de sécurité, sur les tâches où les règles manuelles atteignent leurs limites comme :
- la catégorisation de nouveaux scénarios d'attaques ;
- la détection de certains malwares ;
- le tri de faux-positifs (fausses alertes) ;
- la réduction du nombre d'alertes.

Enfin, en ce qui concerne la détection de fraudes inconnues jusqu'alors, de nombreux laboratoires de recherche parrainés pour certains par de grandes écoles voire la DGA elle-même (Direction Générale de l'Armement) par l'intermédiaire de la Cellule d'Innovation Défense (CID), travaillent sur une solution de détection de menaces basée sur l'IA. Ce sont des technologies qui peuvent donner des réponses lorsque les données sont incomplètes ou légèrement divergentes. Cependant, elles ne donnent des résultats probants que si le corpus de documents est

[3] https://dataanalyticspost.com/Lexique/machine-learning/

conséquent. Plus nous disposons d'échantillons, plus les décisions prises par l'IA sont pertinentes. Pour le chercheur, le savoir-faire autour des solutions d'IA réside notamment dans la faculté à « nettoyer » les données avant de lancer les algorithmes de Machine Learning.

Si les espoirs sont donc multiples pour les plus optimistes d'entre nous, l'IA a surtout fait ses preuves jusqu'à présent dans la détection de fraudes, un domaine connexe à la cybersécurité sans en faire toutefois partie stricto sensu.

Pour les plus pessimistes, la pertinence de l'IA comme solution de défense, peut aussi être vue comme le nouveau paradigme de la menace avec l'arrivée de malwares intelligents, capables de s'adapter à leurs environnements, permettant une meilleure propagation, une identification plus précise de la nature des machines sur lesquelles ils s'installent ou encore une exfiltration plus furtive des données, en se fondant dans le trafic réseau habituel d'une organisation.

Un ensemble de scenarii qui dessinent un avenir où des IA offensives et des IA défensives s'affronteraient pour le contrôle du cyberespace.