RÉFLEXIONS STRATÉGIQUES

PRÉOCCUPANTS, INSPIRANTS, PASSIONNANTS… DÉCOUVREZ À TRAVERS CES ARTICLES RÉFLEXIONS STRATÉGIQUES, LES SUJETS ET EXTRAITS DE MÉMOIRES RÉALISÉS PAR LES AUDITEURS DU MBA MANAGEMENT DE LA SÉCURITÉ.

#INTELLIGENCE ARTIFICIELLE #HUMAIN

Quelles sont les conséquences pour les humains de l'arrivée de l'intelligence artificielle dans la cyber-sécurité ?

AUTEUR : JOËL OLIVIER

JUIN 2019

Quelles sont les conséquences pour les humains de l'arrivée de l'intelligence artificielle dans la cyber-sécurité ?

Auteur : Joël OLIVIER, auditeur de la 5ème promotion

La sécurité informatique (1) reçoit un renfort de plus en plus important de l'Intelligence Artificielle et en particulier des Réseaux de Neurones. Toutefois, dans quelle mesure cet apport qui paraît irréversible impacte-t-il les humains ?
Les derniers succès de l'Intelligence Artificielle de DeepMind dans le monde du jeu de Go avec AlphaGo Zero, des échecs avec AlphaZero et plus récemment StarCraft II avec AlphaStar sont spectaculaires. Ils illustrent avec brio la capacité de l'IA à s'imposer sur des sujets toujours plus complexes (2) à partir de données initiales, souvent volontairement faibles, fournies par leurs créateurs humains : en l'occurrence dans les exemples précédents, les règles du jeu. Mais qu'est-ce vraiment que l'IA ? Nous le verrons dans la première partie de ce mémoire.
La cybersécurité est un enjeu de plus en plus important et le sera incontestablement de manière exponentielle dans les prochaines années. En effet, entre les attaques de virus, les vols de données, les usurpations d'identités, les botnets (3) , etc., les pirates informatiques ne manquent pas d'imagination. Côté organisations (entreprises, ONG, agences gouvernementales, etc.), un travail considérable de sécurisation reste encore à faire. Mais finalement, qu'est-ce que la sécurité informatique ? Nous le verrons dans la deuxième partie de ce mémoire.
Aujourd'hui, l'opportunité de l'arrivée de l'IA dans la sécurité ne fait aucun doute. Elle est d'ailleurs réellement présente dans un certain nombre de produits commerciaux ou libres de droits (« open source »), même si, malheureusement, pour nombre d'entre eux, on ne la trouve que dans les brochures publicitaires.
Lorsque l'on regarde du côté des équipes opérationnelles, on observe qu'elles sont surtout humaines, l'automatisation est somme toute assez faible. Toutefois, les succès de l'IA dans le domaine du jeu, mentionnés précédemment, laissent présager une arrivée plutôt spectaculaire dans la cybersécurité.
Pour certains experts, le temps des humains est même compté, nous serions des dinosaures à la fin du crétacé, prêts à être remplacés par des IA. Qu'en sera-t-il ? Nous considérerons ce sujet dans la troisième et dernière partie de ce mémoire.
Elle se basera sur une analyse reposant sur des faits et des arguments étayés par une large documentation, issue de vulgarisations, de présentations faites lors de conférences, d'articles scientifiques, d'ouvrages mais également de l'expérience de l'auteur du présent mémoire.

(1) Les termes « sécurité informatique » et « cybersécurité » seront utilisés comme synonymes dans ce document.
(2) En partant des règles et en jouant contre elle-même tout en faisant preuve de créativité dans des échelles de temps inhumaines (« quatre heures de pratique et 44 millions de parties [d'entraînement] pour vaincre Stockfish ») idem sur StarCraft avec la création d'une ligue composée de joueurs uniquement IA (cf. [20]).
(3) Un botnet est un ensemble de machines informatiques (caméras, ordinateurs, etc.) qui sont contrôlées de manière visible ou non par un cybercriminel pour son profit.