Impact de l'Intelligence Artificielle dans les métiers de la Cybersécurité

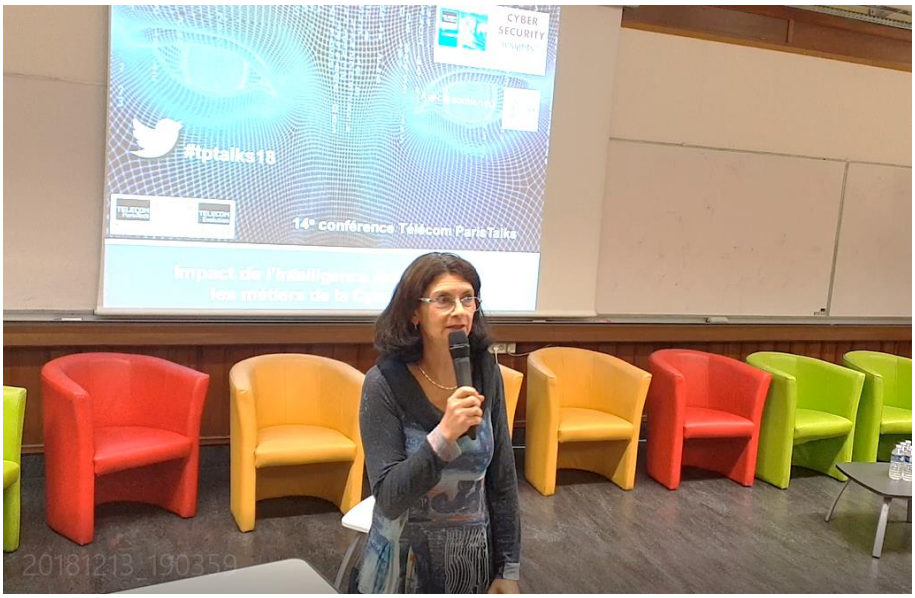
Compte rendu par Laura Peytavin

Les intervenants :

Accueil :

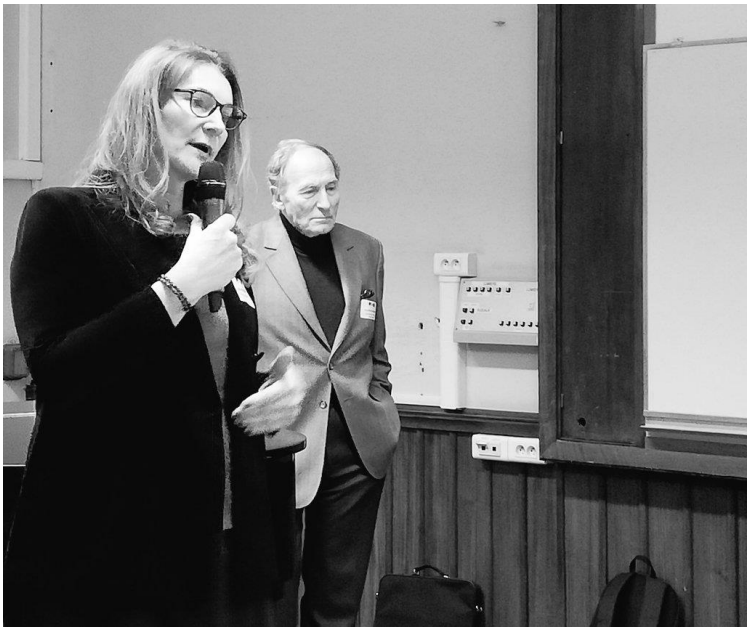
Geneviève Metz, Directrice de Telecom Evolution, souhaite la bienvenue aux nombreux participants, Elle rappelle les missions premières de Telecom Evolution, organisme de formation continue au sein de l'Institut Mines Telecom.

Telecom Evolution est aussi co-organisateur, depuis 2016, des conférences Telecom ParisTalks, en partenariat avec Telecom ParisTech Alumni, sur différents thèmes comme les réseaux et services de télécommunication, la santé, l'énergie, les transports, et ce soir la cybersécurité…



Introduction :

Laura Peytavin, vice-présidente de l'association Telecom ParisTech alumni et co-présidente de son groupe Cybersécurité, explique ce qui a présidé au sein du groupe Cybersécurité à l'approfondissement du thème croisé « IA & cybersécurité ». Travail qui a commencé début 2018, d'abord par le montage d'un dossier du même nom dans la Revue Telecom de septembre 2018, ainsi que d'une conférence menée en partenariat avec l'interclubs numérique des alumni des Grandes Ecoles G9+ en octobre. (Voir compte-rendu et enregistrement de la vidéo ici)



Le sujet de la conférence et de la table ronde se destine préférentiellement aux professionnels de la cybersécurité qui souhaitent aller plus loin que la simple évocation d'une IA marketée comme moteur principal de l'innovation dans leur secteur.

Partant certes d'un premier exemple très illustratif et qui marque les esprits , celui du combat réalisé de plusieurs intelligence artificielle entre elles en 2016 lors d'un Cyber Grand Challenge organisé par la DARPA aux Etats-Unis (voir détails dans l'article de Martin Descazeaux dans la Revue Telecom), elle évoque plutôt les nécessités nouvelles qui appellent l'Intelligence Artificielle à la rescousse de la cybersécurité, sur une terrain qui est construit aujourd'hui sur des architectures en nuage (les clouds) avec toujours plus de complexité logicielle (les SDN) , des APIs insuffisamment sécurisées aux effets systémiques en cas de panne, des tailles massives de données traités, des objets connectés déployés par milliards laissés sans protection, et d'autre part des utilisateurs de ces services numériques, nous les humains, toujours aussi faillibles, sujets à de l'ingénierie sociale qui cherchent à nous tromper – une société numérique où les « fake news ou infox » (pris dans son acception la plus large) desservies par des IA ou des outils d'IA sont destinées à élaborer les plus grandes des attaques possibles.

Les 2 principales questions auxquelles la conférence doit s'atteler à répondre sont :

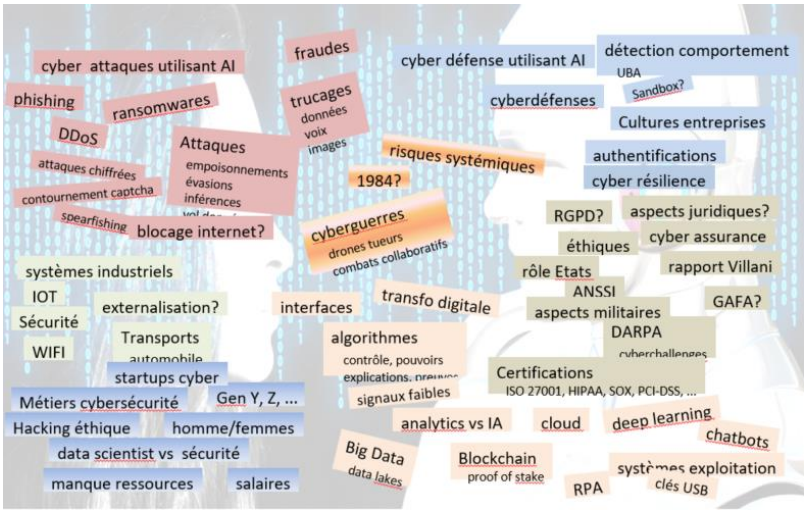
1. En quoi l'IA bouleverse les champs de la cybersécurité ? et en particulier est-ce que l'IA est plus au service de l'attaque que de la défense ?
2. Quels sont les impacts de l'IA sur les formations nécessaires aux futurs experts, et en général sur les métiers et les carrières en cybersécurité ?

Présentations :

Jean-François David qui a été choisi pour animer la table ronde à suivre se présente. Veilleur dans les domaines technologiques et organisationnels, il s'est intéressé récemment plus particulièrement aux domaines des avancées et applications des Intelligences Artificielles, et de leurs impacts sur les organisations et sur les métiers. Il est Enseignant à Dauphine et après une longue carrière très stimulante à IBM, il participe également à de nombreux think tanks.

Jean-François David, après les échanges préparatoires qu'il a eu avec les intervenants dresse le nuage des mots-clés qui seront débattus :

- Apport de l'IA dans un grand nombre de méthodes d'attaques
- Apport de l'IA pour l'outillage des experts en cyber-défense
- Aspect géopolitiques – rôle des états – importance des certifications
- L'impact grand public et risques systémiques et manipulation sur réseaux sociaux
- Impact sur les formations – réponse aux manques de ressources



François Charbonnier est chef adjoint de la coordination sectorielle à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) – chargé des secteurs privé et pilote des réglementations cyber ciblant les secteurs privés

François Charbonnier présente dans les grandes lignes les missions de l'ANSSI, agence nationale chargée de la cybersécurité et de la cyberdéfense. Visant à augmenter le niveau de cybersécurité de l'administration et des opérateurs privés, elle s'inscrit dans un large spectre d'action, notamment de sensibilisation, de cyberveille et d'assistance à l'administration et aux entreprises touchées par des cyber-attaques. De par ses laboratoires de recherche, ses travaux pour stimuler l'offre de solutions de qualité et son expertise reconnue au sein du gouvernement

en matière de systèmes d'information, l'ANSSI prête une grande attention au sujet, quand bien même il n'est pas son cœur de métier.

Tout d'abord, il est important de souligner des points généraux :

- Les avancées récentes présentées comme relevant de l'IA proviennent surtout du *machine learning* et en particulier du *deep learning*, mais les projets industriels qui s'en recommandent visent parfois simplement les dimensions de traitement d'un grand nombre de données (*big data*) et d'automatisation ;
- L'IA n'existe pas sans un volume significatif de données de qualité ;
- La thématique de l'explicabilité d'un algorithme IA est clé : par exemple, pour l'IA au service de la voiture autonome, il est important de comprendre ce qui va se passer et ce qui s'est passé (problématiques juridiques et assurantielles).

Concernant les apports de l'IA à la cybersécurité :

- Il y a une attente forte vis-à-vis de l'IA dans le domaine de la détection, notamment pour détecter les nouvelles menaces pour lesquelles on ne dispose pas encore de marqueurs techniques, et donc repérer ce qui n'est pas encore connu. L'apport sous l'angle du traitement d'un très grand nombre d'événements est également très appréciable ;
- Cependant, à ce stade, l'ANSSI défend une vision qui nécessite une supervision humaine de la détection, quand bien même elle s'appuierait sur des outils d'analyse basés sur l'IA ;
- Concernant l'IA dans les cyberattaques, à ce stade il n'y a pas d'exemple public connu, mais les capacités d'automatisation (souvent rapprochées de l'IA) et de latéralisation permettent l'élaboration d'outils (virus) de plus en plus sophistiqués ;
- Concernant les métiers, le rapprochement entre les data-scientistes / le monde académique « IA » et les experts cyber est un enjeu clé, sachant que la communauté IA est déjà très sollicitée sur beaucoup d'autres problématiques ;
- Un dernier mot sur l'initiative de la conférence CE&SAR 2018 en novembre 2018 à Rennes, une excellente démarche qui a permis justement de rapprocher les deux communautés ! Travaux à suivre…

Didier Cohen est Directeur de la stratégie de Wallix, éditeur français de solution de cybersécurité de plus de 100 personnes aujourd'hui, spécialiste dans le marché de la sécurisation des comptes à privilèges.

IA devient un enjeu dans le domaine de la cyberdéfense. Car il faut faire face au nombre d'attaques à traiter. Aujourd'hui 2 millions de malware par jour à détecter alors qu'ils n'étaient que 5 au début des années 2000. L'IA est d'abord une aide à la détection des menaces, elle soulage la tâche des cyber-analystes. Un exemple est pris par Didier sur une des techniques d'IA d'analyse comportementale « User behavior analytics » – qui permet dans les solutions Wallix de monitorer les usages qu'ont les utilisateurs de leur outil numérique, ceci afin d'y trouver des observations « déviantes » qui témoignent d'une activité malicieuse. Ainsi outillé, le cyber-analyste peut alors se concentrer sur les attaques vraisemblables et les faire bloquer.

En plus des comportements de l'utilisateur, Wallix cherche à pousser encore plus loin ces algorithmes et les faisant travailler sur des combinatoires de paramètres de sessions réseaux pour y trouver des comportements déviants.

Thierry Matusiak est architecte IBM et animateur du groupe de travail du CLUSIF sur la sécurité des objets connectés.

Il n'y a pas encore de groupe de travail IA au sein du CLUSIF, qui reste identifiée comme un sujet prospectif par les RSSI et qui ne porte pas encore une actualité à court terme. Mais c'est un sujet de demain qui motivera la création d'un groupe sans aucun doute.

Son propos liminaire résume bien les 3 rôles que joue l'intelligence artificielle dans la sécurité :

- Le bon : l'IA améliore les pratiques de sécurité informatique
- La brute : les applications reposant sur l'IA introduisent de nouvelles menaces – par exemple sur des médias (images et vidéos) qui rentrent dans la panoplie des données d'authentification des personnes grâce à la formidable capacité de reconnaissance des IAs en la matière
- Le truand : l'IA devient une arme pour les attaquants

En matière de défense (les bons) il évoque 3 grandes domaines d'introduction de l'IA dans les métiers des équipes de sécurité :

1. l'Analyse massive de données – car celle-ci n'est plus accessible à un opérateur humain qui ne serait outillé qu'avec des algorithmes classiques pour détecter de nouvelles menaces dans un flux d'information immense

2. le besoin d'Assistance - avec par exemple l'utilisation des assistants virtuels de type « chatbots » au service des administrateurs et des analystes

3. L'expertise – l'IA aide à assimiler un corpus de connaissance à partir de ces données de plus en plus massives et va contribuer à améliorer l'expertise globale.

Des exemples plus concrets sont brièvement décrits :

- Utilisation des UBA (User Behavior Analytics) pour compléter les moteurs de règles classiques
- Analyse de codes source – on constate ainsi que des solutions d'IA entrainées sur des jeux de données incluant des faux positifs en diminuent le nombre d'un facteur 20
- Déploiement de composants d'IA sous la forme d'assistant personnel en charge de faire respecter des règles de sécurité à l'utilisateur
- Réduction des temps d'analyse des attaques grâce à des composants d'IA qui assurent l'interrogation et la levée de doutes sur des bases de données orientées graphe de composants et documents malveillants
- Des outils de biométrie comportementale qui identifient tellement bien l'utilisateur sur son clavier et sur son écran que l'on pourrait remplacer les mots de passe pour l'accès au terminal (habitudes, vitesse, erreurs clavier…) – sauf que l'utilisateur s'inquiète.

Détection de création frauduleuse de comptes en ligne – qui utilise un moteur d'IA en prenant garde de renouveler régulièrement la base d'apprentissage, un fonctionnement volontairement positionné avec taux de faux négatifs non nul (pour limiter les risques de faux positifs), ainsi que des mécanismes encore supervisés ayant pour but de ne pas se faire repérer par l'attaquant.

Martin Descazeaux : est Manager cybersécurité chez Wavestone. Il participe à l'initiative interne au cabinet qui s'intéresse aux liens entre IA et cybersécurité, aussi bien du point de vue des nouvelles menaces que cela implique, que des opportunités offertes.

Martin témoigne du sentiment largement répandu dans les métiers cyber d'être dans une époque charnière : les solutions d'IA pour la cybersécurité sont nombreuses et très prometteuses, mais il est encore difficile pour les responsables sécurité de visualiser quels seront les cas d'usage concrets sur lesquels investir à court terme.

Pour autant, l'IA « métier » (chatbot, voitures autonomes, smart cities, …) est déjà bien amorcée, en sous-estimant malheureusement souvent le volet cybersécurité. La priorité est donc pour les responsables sécurité de sécuriser ces IA « métier », souvent vulnérables, et d'anticiper l'intégration de la sécurité dans les projets IA futurs.

Grégory Blanc est Maître de Conférences - enseignant chercheur en cybersécurité à Telecom SudParis, membre du laboratoire CNRS SAMOVAR.

Grégory témoigne lui-aussi que le sujet IA dans le monde académique des chaires Cybersécurité est d'actualité. Il cite un article du MIT Technology Review d'août 2018 qui explique que l'avènement de l'IA en cybersécurité est pour l'heure très directement motivé par le volume du travail de détection des menaces qui s'accroit et par le manque de compétence et ressources pour faire face à ces menaces, avec un objectif d'automatisation de la détection et de la réponse la plus complète possible, avec comme matière algorithmique principale les solutions d'apprentissage supervisée dans leur ensemble.

Au niveau recherche en France et en Europe, il y a encore une certaine dichotomie entre les communautés académiques en science des données (Big Data) et en Cybersécurité. Par contre au sein de la communauté Cybersécurité, 2018 aura été, après l'année GDPR en 2017, une année de workshops, publications et conférences très largement consacrés à l'IA (conférence CE&SAR et l'European Cyber Week de novembre entre autres).

Au niveau des cursus des étudiants en cybersécurité aujourd'hui à Telecom SudParis, pour le moment l'enseignement de sciences des données et de la cybersécurité sont disjoints, mais nous tendons à graduellement les intégrer au cursus (tout du moins intégrer quelques notions de data science dans la cyber)

pour permettre aux étudiants de mieux appréhender les outils de détection et de supervision qui reposent sur ces concepts.

Grégory signale qu'il faut cependant toujours faire attention aux résultats de recherche qui sortent et qui sortiront encore. Le travail se fait sur des jeux de données qui sont toujours trop petits et non équilibrés, tempérant ainsi ce sentiment de « magie » de l'apprentissage supervisé.

Enfin, Grégory conclue sur de nouveaux travaux dans le domaine de l'empoisonnement de données et de l'évasion de modèles appris (adversarial machine learning), activités qui commencent pour chercher à anticiper ce que seront les contre-attaques de jeux de données pollués à dessein par les attaquants.

Davide Canali, absent pour raison de santé, et représenté par Laura Peytavin

Davide représente le parcours d'un ancien élève qui a fait ses études dans une des écoles de Mines Télécom (en l'occurrence EURECOM à Sophia Antipolis) et y a fait sa thèse dans le domaine de la cybersécurité.

En tant qu'analyste il est dans son quotidien professionnel l'utilisateur de ce que lui fournit une véritable chaîne d'analyse en continu des menaces (malware, phishing, fraudes, leurres) qui comportent des briques et outils d'IA (principalement du Machine Learning et du « behavior Detection »). Chaine qui face à cette volumétrie de plusieurs centaines de milliers d'échantillons d'attaques par jour sur plusieurs milliards de supports numériques de ces messages (courriels, posts de réseaux sociaux, activités des applications dans le cloud) se déploient sur presque un millier de machines, analysant, détectant, jouant en bac à sable (sandboxing) les menaces une par une.

A chaque élément de la chaîne, il y a des opérateurs humains, des experts et des analystes qui pour certains ont pour tâche de corriger les taux de faux positifs et faux négatifs, et d'autres comme Davide de traiter et enrichir la description d'attaque particulièrement intéressante, car ciblée, et ou appliquant une innovation que les clients doivent avoir connaissance au plus vite.

Jordi Saniger-Paré,

Ancien élève de Centrale-Supelec, Jordi a travaillé dans le groupe EADS et Airbus et a contribué au rapport France IA.

Jordi insiste sur le fait que l'IA est un mot valise qui regroupe non seulement les grandes familles de l'apprentissage automatique qui ont un succès remarqué et remarquable (Machine Learning, réseau de neurones profonds) mais aussi celles qui travaillent sur les représentations de connaissances sous forme ontologique et symbolique.

Même si le sujet de l'empoisonnement des « datasets » par les attaquants devient un grand sujet de préoccupation en cybersécurité, les autres domaines sur la représentation de la connaissance font l'objet de travaux de recherche qui sauront eux aussi être utilisés à de mauvaises intentions.

Un très rapide état des lieux des pays qui investissent beaucoup en cybersécurité, et notamment, mise à part les Etats-Unis :

- La Chine qui n'expose pour le moment en termes de publications de recherche dans le domaine que peu de choses très avancées, mais qui a toujours su surprendre ses partenaires par le passé, en surgissant avec des réalisations remarquables, et donc peut être aussi en cybersécurité.
- Israël, qui est très en lien avec les Etats-Unis en matière de sécurité numérique et qui investit 400 millions pour son écosystème de sociétés du domaine.

- L'Allemagne qui investit 3 milliards jusqu'en 2025 en IA (domaine santé, transports, et automatisation des systèmes), en comparaison des 1,5 milliards pour la France.

Table ronde

Voici le résumé des principaux échanges :

A la question « Pourquoi parle-t-on tant d'IA en 2018 dans les métiers de la Cybersécurité ? », les panélistes ont apporté les réponses suivantes :

- Beaucoup d'attaques systémiques récentes et qui ont fait du bruit et ont précipité le besoin de comprendre ce que l'IA va apporter comme nouvelles capacités offensives et comme moyens de défense dans le proche avenir
- Les données numériques à protéger ne cessent d'augmenter en volume et en valeur alors que dans le même temps l'innovation apportée par l'apprentissage profond semble apporter beaucoup de promesses

Cependant, le problème de l'explicabilité et de la traçabilité des approches connexionnistes (réseaux de neurones profonds) est partagé. Il pose un problème juridique lorsqu'il s'agira de dresser les responsabilités lors d'incidents ou accidents numériques.

Les intervenants conviennent que les approches qui seront suivies pour assurer notre sécurité numérique n'abandonneront pas facilement l'hybridation dans les solutions et les processus, mêlant approches classiques explicables (analytiques ou à base de règles) et pures approches par apprentissage supervisé.

Pour le moment le « mindset » et le capital de savoir-faire des professionnels en cybersécurité tournent autour de la sécurité des systèmes, des réseaux, du code, qu'ils soient du côté des hackers ou des analystes en cyber-veille. Quand et comment sauront-ils embrasser aussi les savoirs et les compétences des data-scientistes et des spécialistes de l'apprentissage supervisé ? Pour Grégory Blanc, il est vraisemblable que l'imagination et l'innovation est aux pouvoirs chez les hackers eux-mêmes dont certains sont d'excellents mathématiciens et pour qui les modèles connexionnistes et d'apprentissage supervisé ou non supervisé ne font pas peur. Ils mettront en œuvre des attaques illustrant ces synergies, nourris d'une motivation supplémentaire consistant à aller chercher ce qu'il y a sous le « capot de l'IA ».
En terme académique, les cas d'usage de cybersécurité qui se présentent désormais vont donner l'occasion de voir converger les 2 domaines Big Data et Cybersécurité - pour in fine une IA au service de la cybersécurité, et vice et versa une cybersécurité au service de l'IA.

Peut-on décrire plus précisément des cas d'utilisation de l'IA en préparation par les hackers ?

- Après des attaques virales récentes, de nature systémique, de type Wanacry et Not Petya, qui ont joué finalement par opportunisme en exploitant des vulnérabilités négligemment trop répandues encore, on peut penser que l'IA va permettre aux attaquants de passer de l'opportunisme à la préparation avec scans massifs des « devices » sur Internet, de malwares boite à outils effectuant de la préanalyse pour construire ainsi des attaques massives, systémiques et polymorphes à la fois.
- On constate déjà dans la cinétique des attaques latérales les formes d'une meilleure intelligence pour aller chercher les comptes les plus vulnérables et les comptes à haut privilèges.
- On pressent que l'analyse des réseaux sociaux par des outils d'IA va permettre des spear phishing extrêmement ciblés et bien fait –

- La protection des accès par captcha risque de subir des attaques par usage systématique de reconnaissance de caractères ou d'images très performantes.
- Le Cyber Grand Challenge et d'autres expérimentations par IBM laissent présager que des outils d'IA utilisés par des hackers pourraient devenir très dangereux car ils quand on voit par exemple ce que donne la convergence entre 2 réseaux de neurones qui apprennent l'un de l'autre. C'est ainsi que des « password cracker » extrêmement performants ont déjà vu le jour.
- La mise à disposition dans le domaine public opensource d'outils d'analyse d'image pour recomposer une partie d'image manquante ou de recomposition des mouvements des lèvres est préoccupante car c'est l'outil idéal pour réaliser des attaques par messages frauduleux de type « attaque au président ».

Quels risques supplémentaires font peser les objets connectés ?

Ils sont très nombreux (plusieurs milliards) et rajoutent à chaque fois de nouveaux risques. Ces objets n'auront toujours que des ressources limitées pour s'auto-protéger, ce qui fait que le problème de leur sécurité ne sera jamais maitrisé par design. Il est probable que la cybersécurité des constellations d'objets connectés passera plutôt par l'usage de de modèles d'apprentissage non supervisé voire même markovien adapté à un périmètre d'analyse peu maîtrisé.

Question sur le déficit en termes de profils et experts en cybersécurité. Que voit-on des besoins et profils à l'avenir ?

La cybersécurité passe par la protection des cibles, qui, en premier rideau, sont très souvent les êtres humains eux-mêmes, avec leur faille utilisée par l'attaquant pour leur faire faire la ou les premiers étages de l'attaque ou de la compromission. Et pour les tromper, l'IA est déjà à l'œuvre pour faire de l'ingénierie sociale à grande échelle. A ce niveau, les compétences sont relativement éloignées de la connaissance de codes malveillants mais plutôt à la croisée de l'analyse comportementale, de la maitrise du langage (chatbot) et même de la psychologie humaine. Tout un pan de savoir qui ouvre à des profils complètement différents de ceux qui intégraient le secteur auparavant.

L'apprentissage supervisé dans les techniques d'IA est marqué par des biais cognitifs de leur concepteur et des administrateurs. Ces biais en cybersécurité comme dans tout autre domaine sont dommageables de telle sorte que le secteur

qui n’a de cesse de chercher des talents qui manquent à l’appel doit en profiter pour ouvrir les portes à plus de femmes et de profils différents.

Une question sur les perspectives économiques en cybersécurité :

Le marché de l’IA connait une croissance de 34% par an, et de son côté le secteur de la cybersécurité croit de 15% par an.

Question sur l’éthique et la morale

Les hackers ne sont pas les commanditaires directs de la plupart des attaques. Ce sont les donneurs d’ordre qui sont divers, depuis les mafias, des intérêts privés divers jusqu’au états. Les spécialistes du secteur sont la plupart des entreprises qui innovent pour continuer à protéger contre des menaces cyber toujours plus sophistiqués et nombreuses, mais aussi des individus très sensibles aux valeurs d’une société numérique éthique et juste (ex le refus des employés de Google pour la mise à contribution de leur IA sur un contrat avec la NSA).

Par ailleurs François Charbonnier de l’ANSSI rappelle que la France a été à l’initiative d’un cyberespace dans lequel le « hack-back » des états serait combattu pour éviter des escalades ravageuses.