



Impact de l'IA sur les compétences

en matière de CYBERSÉCURITÉ

NOTE

L'association Talents du numérique, qui associe établissements d'enseignement supérieur et entreprises du numérique, a réalisé un travail important sur le développement des compétences des professionnels du secteur du numérique.

La commission compétences de Talents du numérique a pour objectif de préparer l'avenir des entreprises et des établissements de formation afin que le secteur soit en mesure de réagir à l'évolution des compétences recherchées, alors que de nouvelles technologies arrivent et se déploient, tandis que de nouveaux usages et enjeux apparaissent.

Éléments de contexte

La révolution numérique que nous vivons dépasse largement le cadre purement technologique. Elle bouscule les équilibres économiques et transforme les usages à une vitesse jamais atteinte jusque-là. Elle touche tout autant les clients des entreprises numériques dans leurs activités, leurs chaînes de valeur et leurs organisations, que les individus dans leur vie quotidienne et la société en général, dans ses règles et ses équilibres. Il s'en suit pour les utilisateurs - individuels ou collectifs, publics ou privés - de potentiels risques engendrés par l'exploitation extensive des données, l'avènement de l'intelligence artificielle et par la virtualisation des échanges et des processus qui renforcent le besoin de cybersécurité.

En tant qu'opérateurs de transformations numériques, les professionnels du numérique sont confrontés à de nouvelles responsabilités et exigences face aux risques (cyberattaques, dévoiement de l'usage des données, risques opérationnels internes, etc.) :

- Ils sont tenus de garantir la conformité au cadre législatif et réglementaire des systèmes et outils qu'ils conçoivent et utilisent ;
- Ils doivent s'assurer que ces mêmes dispositifs se déploient dans des environnements de confiance, avec des partenaires et des systèmes respectueux d'un cadre éthique et de sécurité ;
- Ils doivent tenir les objectifs de la cybersécurité qui sont la confidentialité, l'intégrité, la disponibilité (CID) auxquels on peut ajouter la traçabilité, la non-répudiation et la conformité.

De nombreux exemples d'attaques et de fuites de données ces dernières années ont montré les limites de la sécurité informatique. La nécessité de poursuivre la recherche en ce domaine, la diffusion des différentes technologies disponibles, la sensibilisation aux risques, l'acculturation et la formation de l'ensemble des collaborateurs des entreprises, des usagers et des citoyens sont primordiales. C'est un enjeu clé pour l'ensemble des entreprises, aucun secteur d'activité n'étant épargné. Les attaques informatiques peuvent par exemple paralyser des usines, des administrations ou des entreprises, parfois dans des secteurs critiques comme l'énergie ou la santé¹.

Concernant les enjeux liant cybersécurité et intelligence artificielle (IA), nous identifions trois dimensions :

- La **cybersécurité de l'IA** (le « produit ») : les systèmes d'IA présentent des vulnérabilités comme tout système d'information et peuvent faire l'objet d'attaques, appelant à leur sécurisation ;
- La **cybersécurité par l'IA** (au bénéfice de la défense cyber) ;
- La **cybersécurité face à l'IA** (au bénéfice des attaquants).

Nous nous consacrerons dans cette note essentiellement aux deux derniers sujets.



Les besoins de notre économie en professionnels de la cybersécurité sont immenses. La cybersécurité fait partie intégrante de l'ensemble des domaines informatiques et des projets numériques. Le recrutement est perçu comme une difficulté majeure par les entreprises de ce secteur, qui devrait générer en France en 2030, selon les prévisions, un chiffre d'affaires de 10 Mds €. Dans une étude réalisée par l'OPIIEC en 2025, la cybersécurité représentait 45000 emplois de la branche des métiers de l'ingénierie, du numérique, des études, du conseil et des métiers de l'événement, 78000 emplois sont attendus d'ici 2028².

Cependant, cette croissance se heurte à une pénurie de profils qualifiés. Les entreprises peinent à recruter, notamment dans les domaines de la cryptographie, du cloud, de l'IA appliquée à la cybersécurité ou encore de la sécurité des objets connectés (IoT).

¹ Nous vous invitons à lire le Panorama de la cybermenace 2025 (<https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/>), réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Au cours de l'année 2025, l'ANSSI a traité, avec différents niveaux de mobilisation, 3 586 événements de sécurité, soit une diminution de 18 % par rapport à l'année précédente. Une diminution pouvant s'expliquer par les pics de signalements observés lors de la tenue des Jeux Olympiques et Paralympiques de Paris, entre les mois de mai et d'août 2024. Ainsi, 2 209 signalements et 1 366 incidents ont été portés à la connaissance de l'Agence en 2025 avec quatre secteurs d'activité qui ont été particulièrement visés : l'Éducation et la recherche (34 %), les ministères et les collectivités territoriales (24 %), la santé (10 %) et les télécommunications (9 %).

² Besoins en compétences, emplois et formations en matière de cybersécurité en France | <https://www.opiiec.fr/etudes/141341>.

Au-delà de ces besoins propres du secteur, la commission compétences insiste sur l'enjeu fondamental de la transversalité de la cybersécurité, incluant une profondeur d'expertise de l'ensemble des métiers IT. Réciproquement, les experts de la cybersécurité doivent avoir cette connaissance et cette vision transversales. Les emplois de la cybersécurité dépassent le strict cadre du secteur de la cybersécurité et cette dernière ne doit pas rester l'apanage de quelques experts. Développer une culture de la sécurité numérique est essentiel afin de se protéger de catastrophes économiques et industrielles. L'effort pédagogique à réaliser doit être impulsé par les directions générales afin d'être concluant et opérant.



Photo : R - stock.adobe.com

Impact de l'intelligence artificielle sur la cybersécurité³

L'intelligence artificielle joue aujourd'hui un rôle croissant dans le domaine de la cybersécurité. Elle est présente dans l'ensemble des briques cybersécurité à tous niveaux (Gouvernance Risque et Conformité⁴ - GRC, Security Information and Event Management - SIEM⁵, Security Orchestration, Automation and Response - SOAR⁶...). C'est un outil transversal qui impacte profondément la manière dont on opère en cybersécurité. Le premier constat relevé par la commission compétences consiste en la permanence de la validité des fondamentaux techniques et scientifiques. Cependant, l'IA transforme les pratiques, les risques, les process et les profils recherchés. Face à l'augmentation du volume et de la sophistication des cyberattaques, les organisations doivent développer des moyens de défense plus rapides, plus intelligents et capables de traiter d'importantes quantités de données. Dans ce contexte, l'IA constitue un outil stratégique permettant d'améliorer la détection, la prévention et la gestion des incidents de sécurité. Toutefois, elle peut également être exploitée par les cybercriminels, ce qui crée de nouveaux défis pour les systèmes de protection.

³ Nous n'évoquerons pas dans ce document le sujet, également majeur de la sécurisation de l'IA, qui impose également de nouvelles compétences à développer et à adresser.

⁴ Le GRC : (Gouvernance, risque et conformité) est un moyen structuré d'aligner l'informatique sur les objectifs de l'entreprise tout en gérant les risques et en respectant les réglementations sectorielles et gouvernementales.

⁵ Les systèmes SIEM collectent et analysent les journaux de l'ensemble de l'organisation, y compris les serveurs, les dispositifs réseau, les pare-feu, d'autres solutions de sécurité et les applications cloud. L'objectif de cette collecte de données est de découvrir les anomalies qui indiquent une menace potentielle.

⁶ Le SOAR (« Security Orchestration, Automation and Response ») est un type de solution logicielle qui permet aux équipes de sécurité d'intégrer et de coordonner des outils de sécurité distincts, d'automatiser les tâches répétitives et de rationaliser les workflows de réponse aux incidents et aux menaces.

- **Amélioration de la détection des menaces**

L'un des principaux apports de l'intelligence artificielle en cybersécurité concerne la détection des menaces. Traditionnellement, les systèmes de sécurité reposaient sur des bases de signatures ou des règles prédéfinies permettant d'identifier des logiciels malveillants connus. Cette approche présente cependant des limites face aux attaques inédites ou évolutives.

Grâce aux techniques d'apprentissage automatique, les systèmes de cybersécurité peuvent analyser de grandes quantités de données issues des réseaux, des systèmes informatiques ou des comportements des utilisateurs. Ces analyses permettent d'identifier des anomalies ou des comportements suspects, même lorsqu'ils ne correspondent pas à des attaques déjà répertoriées. Ainsi, l'IA améliore la capacité des organisations à détecter précocement des intrusions ou des activités malveillantes.

- **Automatisation de la réponse aux incidents**

L'intelligence artificielle contribue également à accélérer l'automatisation de certaines actions de réponse face aux incidents de sécurité. Lorsqu'une menace est détectée, les systèmes intégrant de l'IA peuvent déclencher automatiquement différentes mesures de protection, comme l'isolement d'un poste infecté, le blocage d'une adresse IP suspecte ou la désactivation d'un compte compromis.

Cette automatisation permet de réduire considérablement le temps de réaction face aux attaques, ce qui est essentiel dans un contexte où les cyberattaques peuvent se propager en quelques minutes. Elle permet aussi de diminuer la charge de travail des équipes de sécurité, qui peuvent se concentrer sur les incidents les plus complexes.

- **Capacité d'anticipation et analyse prédictive**

Un autre avantage important de l'intelligence artificielle réside dans sa capacité à analyser de vastes volumes d'informations afin d'identifier des tendances ou des schémas d'attaque. En exploitant les données issues des journaux de sécurité, des bases de vulnérabilités ou des sources de renseignement sur les menaces, l'IA peut contribuer à anticiper certaines attaques.

Cette approche prédictive permet notamment de prioriser les correctifs de sécurité, d'identifier les systèmes les plus vulnérables et d'adapter les stratégies de défense en fonction des menaces émergentes. La cybersécurité évolue ainsi d'un modèle principalement réactif vers une approche plus proactive.

- **Utilisation de l'intelligence artificielle par les cybercriminels**

Malgré ses nombreux avantages, l'intelligence artificielle peut également être utilisée à des fins malveillantes. Les cybercriminels exploitent de plus en plus ces technologies pour automatiser leurs attaques et les rendre plus efficaces.

Par exemple, l'IA peut être utilisée pour générer des campagnes d'hameçonnage (ou phishing) très convaincantes, créer des contenus frauduleux personnalisés ou produire des programmes malveillants capables de s'adapter aux systèmes qu'ils attaquent. De plus, certaines technologies comme les deepfakes⁷ peuvent être employées pour usurper l'identité de personnes et faciliter des fraudes ou des manipulations. Cette évolution renforce la complexité du paysage des menaces et oblige les organisations à investir davantage dans des solutions de cybersécurité avancées.

- **Une cybersécurité augmentée par l'intelligence artificielle**

Il est important de souligner que l'intelligence artificielle ne remplace pas les experts en cybersécurité. Elle constitue plutôt un outil d'assistance qui permet d'améliorer leurs capacités d'analyse et de réaction, mais également de structurer et valider la conformité. En automatisant certaines tâches répétitives et en facilitant l'analyse de grandes quantités de données, l'IA permet aux spécialistes de la sécurité de se concentrer sur les menaces les plus critiques.

⁷ Un deepfake est un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle.

- **De nouvelles vulnérabilités du fait de l'emploi « caché » de l'IA par les collaborateurs**

Autre phénomène à prendre en compte : le Shadow AI⁸ (ou IA fantôme). L'utilisation de l'intelligence artificielle s'est considérablement répandue. L'accès aux applications d'IA est simple et souvent gratuit ou peu coûteux. Or, de nombreuses organisations n'ont pas encore mis en place de politiques liées à l'IA ou ignorent les risques associés à l'utilisation privée de l'IA par leurs employés à des fins professionnelles. Ce phénomène est comparable dans une certaine mesure à la problématique du BYOD (Bring Your Own Device, ou « apportez vos appareils personnels ») en cybersécurité, qui avait déclenché un débat important sur la gouvernance il y a quelques années. La part de l'IA cachée est déjà considérable d'après certaines études compromettant la sécurité des organisations.



Photo : NingPhatthaphorn - stock.adobe.com

Ainsi, une des avancées essentielles de l'IA est de permettre de traiter des volumes de données beaucoup plus importants qu'avant, grâce à des algorithmes de machine learning capables d'analyser en temps réel les flux. Elle automatise la détection des menaces en identifiant des comportements anormaux plus rapidement que les humains. Elle permet également de trouver des pistes de remédiation ou de traitement des vulnérabilités. Les systèmes basés sur l'IA priorisent les alertes, réduisant le bruit en aidant les équipes à se concentrer sur les incidents critiques. Elle améliore aussi la réponse aux attaques en déclenchant des actions automatiques (blocage, etc.). Enfin, elle apprend en continu, ce qui permet d'adapter la défense face à des menaces toujours plus nombreuses, sophistiquées et évolutives. L'avenir de la cybersécurité repose cependant en grande partie sur une collaboration entre l'expertise humaine et les technologies d'intelligence artificielle, afin de faire face à des menaces numériques de plus en plus complexes. L'intégration de l'IA dans les systèmes de sécurité doit s'accompagner d'une vigilance constante et d'une adaptation continue des stratégies de défense.

⁸ Exemple : dans les collectivités, le taux de shadow IA est estimé à 60 % selon la Banque des Territoires. <https://teriagen.com/shadow-ia-dans-les-collectivites-60-de-vos-agents-utilisent-deja-lia-sans-le-dire/>.



Les limites de l'IA en matière de cybersécurité

Malgré les nombreux avantages qu'elle apporte, l'intelligence artificielle présente également certaines limites dans le domaine de la cybersécurité. En effet, son efficacité dépend de plusieurs facteurs techniques, humains et organisationnels. Ces limites doivent être prises en compte afin d'éviter une dépendance excessive à ces technologies et de maintenir un niveau de sécurité adapté aux menaces actuelles.

- **Dépendance à la qualité et à la quantité des données**

Les systèmes d'intelligence artificielle reposent principalement sur l'analyse de grandes quantités de données. Par conséquent, la performance de ces systèmes dépend fortement de la qualité, de la diversité et de la fiabilité des données utilisées pour leur entraînement.

Si les données sont incomplètes, biaisées ou insuffisantes, les modèles d'IA risquent de produire des résultats incorrects. Cela peut entraîner une mauvaise identification des menaces, une incapacité à détecter certaines attaques ou, au contraire, générer un nombre élevé de fausses alertes. Ainsi, la gestion et la mise à jour des données constituent un défi important pour les organisations qui utilisent l'IA en cybersécurité.

- **Risque de faux positifs et de faux négatifs**

Les systèmes d'intelligence artificielle peuvent parfois générer des erreurs d'analyse. Les faux positifs correspondent à des situations où une activité légitime est considérée comme une menace, tandis que les faux négatifs désignent des attaques réelles qui ne sont pas détectées.

Un nombre élevé de faux positifs peut entraîner une surcharge de travail pour les équipes de sécurité, qui doivent analyser des alertes non pertinentes. À l'inverse, les faux négatifs peuvent permettre à des cyberattaques de passer inaperçues, ce qui représente un risque important pour les systèmes d'information.

- **Vulnérabilité des systèmes d'IA eux-mêmes**

Les systèmes basés sur l'intelligence artificielle peuvent également devenir des cibles pour les cyberattaques. Des techniques spécifiques peuvent être utilisées pour manipuler ou tromper les modèles d'apprentissage automatique.

Par exemple, certaines attaques visent à modifier les données utilisées pour entraîner les algorithmes, ce qui peut fausser leur fonctionnement. D'autres techniques consistent à créer des entrées spécialement conçues pour tromper les systèmes de détection. Ces vulnérabilités montrent que les solutions basées sur l'IA ne sont pas infaillibles et doivent elles-mêmes être protégées.

- **Manque de transparence et difficulté d'interprétation**

Certains modèles d'intelligence artificielle, en particulier les modèles complexes comme les réseaux neuronaux profonds, fonctionnent comme des « boîtes noires ». Il peut être difficile pour les experts de comprendre précisément comment ces systèmes prennent leurs décisions.

Ce manque de transparence peut poser des problèmes dans le domaine de la cybersécurité, où il est souvent nécessaire d'expliquer les raisons d'une alerte ou d'une décision de blocage. L'interprétation des résultats devient alors plus complexe et peut limiter la confiance accordée à ces technologies.



Photo : Maxime - stock.adobe.com

- **Coût et complexité de mise en œuvre**

La mise en place de solutions de cybersécurité basées sur l'intelligence artificielle nécessite des ressources importantes. Elle implique notamment l'acquisition de technologies avancées, la gestion de grandes infrastructures de données et le recrutement de spécialistes capables de concevoir et d'exploiter ces systèmes.

Pour certaines organisations, en particulier les petites et moyennes entreprises, ces coûts et cette complexité peuvent représenter un obstacle à l'adoption de solutions basées sur l'IA.

- **La question de la souveraineté des données, de leurs hébergements et du modèle de déploiement**

La question de la souveraineté des données en cybersécurité et en IA est centrale, car elle concerne le contrôle, la localisation et l'usage des informations sensibles. Elle s'inscrit notamment dans le cadre réglementaire européen comme le RGPD, qui impose des règles strictes sur le traitement et le transfert des données. Elle implique que les organisations gardent la maîtrise de leurs données (où elles sont stockées, qui y accède, sous quelle juridiction). Le recours à des solutions d'IA, souvent proposées par de grands acteurs internationaux, peut poser des enjeux de dépendance et d'extraterritorialité (ex. lois étrangères). Le choix de l'hébergement des données (cloud public, privé ou local) détermine le niveau de contrôle et de sécurité. Des initiatives comme Gaia-X visent à garantir un hébergement conforme aux exigences européennes, en limitant les transferts hors UE et en assurant la transparence. Les modèles de déploiement de l'IA peuvent aussi avoir une incidence en matière de sécurité⁹. Trois approches principales existent :

- **On-premise** : IA déployée localement, offrant un contrôle maximal mais nécessitant des ressources importantes.
- **Cloud** : plus flexible et scalable, mais avec des enjeux de souveraineté et de dépendance.
- **Hybride** : compromis permettant de garder les données sensibles localement tout en exploitant la puissance du cloud.

Au final, l'enjeu est de trouver un équilibre entre performance technologique, conformité réglementaire et autonomie stratégique.

- **Transformations des processus et des organisations**

L'impact de l'IA sur l'organisation interne en matière de cybersécurité est profond, car elle transforme à la fois les rôles et la prise de décision, ce qui peut amener à des failles et à des menaces. De même, de nombreuses entreprises, souvent les plus petites, externalisent leur sécurité. Cela crée une dépendance et aussi une externalisation de potentielles failles dues aux prestataires utilisés.

Par conséquent, l'IA doit être considérée comme un outil complémentaire aux méthodes traditionnelles de sécurité et à l'expertise humaine. Une approche équilibrée, combinant technologies avancées et compétences humaines, demeure essentielle pour faire face aux cybermenaces actuelles.

⁹ Des initiatives européennes au niveau de secteurs incarnent précisément cet équilibre stratégique : CATENA-X (automobile) : un cloud hybride avec les standards de Gaia-X pour l'interopérabilité de la supply chain :

- Data4NuclearX (EDF/CEA) : un data mesh décentralisé, des données souveraines, et des échanges peer-to-peer ;
- EONA-X : une orchestration fédérée, des données qui restent chez le producteur, avec une conformité RGPD/NIS2 ;
- PONTUS-X : des smart contracts dans le cadre de Gaia-X pour une monétisation et une conformité avec les normes de l'UE ;
- DECADE-X (aéronautique/défense) : il s'inscrit dans cette logique, priorisant souveraineté et interopérabilité pour des chaînes de valeur critiques.

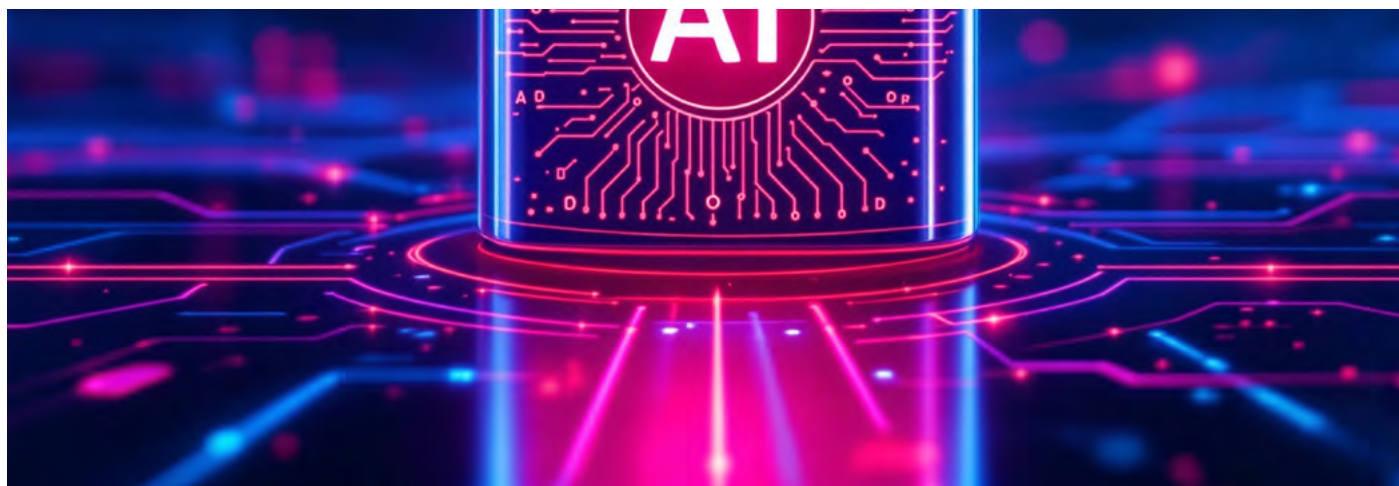


Photo : Agus - stock.adobe.



L'impact de l'intelligence artificielle sur les métiers de la cybersécurité (hors compétences)

L'intelligence artificielle transforme progressivement les métiers de la cybersécurité. Face à l'augmentation du nombre de cyberattaques et à la complexité croissante des systèmes d'information, les organisations doivent adapter leurs méthodes de protection. Dans ce contexte, l'IA modifie les pratiques professionnelles, les compétences requises et l'organisation du travail des spécialistes de la cybersécurité. Elle ne remplace pas les experts humains, mais elle transforme leurs missions et renforce leur capacité d'action.

Au-delà de l'automatisation de certaines tâches de sécurité et l'amélioration de la capacité d'analyse des experts déjà évoquées, l'IA permet également le développement de la communication technico-fonctionnelle, axée gestion de crise et prise de décision sous incertitude.

Elle a également un impact sur :

- **La transformation de l'organisation du travail**

L'utilisation de l'intelligence artificielle dans la cybersécurité modifie également l'organisation du travail au sein des équipes de sécurité informatique. Les centres d'opérations de sécurité (SOC) s'appuient de plus en plus sur des plateformes automatisées capables de centraliser et d'analyser les informations provenant de multiples sources.

Cette évolution conduit à une répartition différente des rôles entre les outils automatisés et les analystes humains. Les systèmes d'IA assurent la surveillance continue et la détection préliminaire des menaces, tandis que les experts humains interviennent pour l'analyse approfondie, la prise de décision et la gestion des situations complexes.

Il est bon de noter que cela a un impact sur les métiers de l'ensemble de l'entreprise et pas seulement sur les professionnels du numérique. L'intégration de l'IA doit être maîtrisée, cela nécessite une gestion et un accompagnement spécifique.

- **La création de nouveaux métiers spécialisés**

Enfin, le développement de l'intelligence artificielle dans la cybersécurité favorise l'apparition de nouveaux métiers spécialisés. Parmi ces nouveaux rôles figurent notamment les spécialistes de la sécurité des systèmes d'IA, les ingénieurs en apprentissage automatique appliqué à la cybersécurité ou encore les analystes chargés de superviser et d'améliorer les modèles d'intelligence artificielle utilisés dans les systèmes de protection.

Ces nouveaux métiers illustrent la convergence croissante entre les domaines de la cybersécurité, de la science des données et de l'intelligence artificielle.

Ainsi, loin de remplacer les professionnels, l'IA agit comme un outil complémentaire qui renforce leur efficacité. L'évolution des métiers de la cybersécurité repose ainsi sur une collaboration étroite entre l'expertise humaine et les technologies avancées d'intelligence artificielle.



Évolution des compétences requises

L'intégration de l'intelligence artificielle dans les outils de cybersécurité entraîne également une évolution des compétences nécessaires pour les professionnels du secteur.

Il convient tout d'abord de signifier que tout ne change pas. Des compétences de base restent opérantes. Nous pensons notamment à la maîtrise de la dimension hardware (matériel, électronique) – trop souvent sous-estimée - à la compréhension des protocoles, les architectures, les réseaux, le système d'exploitation (ou OS, Operating System), la sécurité applicative, la capacité à faire une analyse de risque structurée, la maîtrise des bonnes pratiques (confidentialité, intégrité, disponibilité), l'intégration des grandes notions du numérique responsable (éthique, empreinte environnementale ...) dans la conception et la conduite des projets.

Ce qui change : l'IA augmente le volume de données à traiter, crée de nouveaux vecteurs d'attaque et requiert une interaction homme-machine dans les boucles de décision. Les entreprises attendent des professionnels capables de synthétiser des signaux complexes, de piloter des outils intelligents et de prendre des décisions contextuelles et responsables. Ainsi, en plus des compétences techniques traditionnelles liées aux réseaux, aux systèmes informatiques et à la sécurité des applications, les experts doivent désormais posséder des connaissances dans des domaines tels que l'analyse de données, l'apprentissage automatique et l'exploitation des systèmes automatisés.

Cette évolution favorise l'émergence de profils hybrides capables de combiner des compétences en cybersécurité et en intelligence artificielle, avec d'autres domaines de compétences non techniques (exemple : maîtrise de la réglementation - IA Act¹⁰, RGPD...). Les professionnels doivent également être capables de comprendre le fonctionnement des algorithmes utilisés par les outils de sécurité afin d'interpréter correctement les résultats qu'ils produisent.

Cette évolution conduit à une redéfinition des profils professionnels et à l'émergence de compétences interdisciplinaires.

• Élargissement des compétences techniques

Traditionnellement, les professionnels de la cybersécurité possédaient principalement des compétences en administration des systèmes, en gestion des réseaux, en cryptographie et en sécurité des applications. Cependant, avec l'intégration de l'intelligence artificielle dans les outils de sécurité, ces compétences doivent être complétées par des connaissances dans des domaines tels que l'apprentissage automatique, l'analyse de données et le traitement de grandes quantités d'informations.

Les experts en cybersécurité doivent être capables de comprendre le fonctionnement général des algorithmes d'intelligence artificielle afin de pouvoir exploiter efficacement les outils de détection automatisée des menaces. Cette compréhension permet notamment d'interpréter les résultats produits par ces systèmes et d'identifier leurs éventuelles limites.

• Développement des compétences en analyse de données

L'utilisation de l'intelligence artificielle repose en grande partie sur l'analyse de grandes quantités de données issues des systèmes d'information, des réseaux et des journaux d'activité. Par conséquent, les professionnels de la cybersécurité doivent développer des compétences en analyse de données afin de pouvoir exploiter ces informations de manière pertinente.

Ces compétences incluent notamment la capacité à collecter, structurer et analyser des données provenant de différentes sources. Les experts doivent également être capables d'identifier des tendances ou des anomalies dans ces ensembles de données afin de détecter des comportements suspects ou des attaques potentielles.

¹⁰ Le Règlement européen sur l'intelligence artificielle : publics concernés, dates clés, conséquences pour les entreprises | Direction générale des Entreprises.

- **Compréhension des systèmes d'intelligence artificielle**

L'essor de l'IA dans la cybersécurité nécessite également une meilleure compréhension des systèmes d'intelligence artificielle eux-mêmes. Les professionnels doivent être en mesure de comprendre les principes de fonctionnement des modèles d'apprentissage automatique, ainsi que les facteurs qui peuvent influencer leur performance.

Cette compréhension est essentielle pour évaluer la fiabilité des systèmes automatisés et pour éviter une dépendance excessive à des outils dont le fonctionnement pourrait être mal interprété. Les experts doivent également être capables d'identifier les biais potentiels dans les données utilisées pour entraîner les modèles et de comprendre les limites des systèmes basés sur l'IA.

- **Renforcement des compétences d'analyse et de prise de décision**

Bien que l'intelligence artificielle puisse automatiser certaines tâches, elle ne remplace pas le jugement humain. Les professionnels de la cybersécurité doivent continuer à analyser les situations complexes et à prendre des décisions stratégiques face aux incidents de sécurité.

Dans ce contexte, les compétences analytiques, la capacité à interpréter des informations complexes et le raisonnement critique deviennent encore plus importants. Les professionnels doivent être capables de combiner les résultats fournis par les outils d'IA avec leur propre expertise afin d'évaluer correctement les risques et de définir les actions à entreprendre.

- **Importance croissante de la formation continue**

L'évolution rapide des technologies liées à l'intelligence artificielle implique également que les professionnels de la cybersécurité doivent s'engager dans un processus de formation continue. Les outils et les méthodes évoluent rapidement, ce qui nécessite une mise à jour régulière et constante des compétences.

Les organisations doivent donc encourager le développement professionnel de leurs équipes à travers des formations spécialisées, des certifications et des programmes d'apprentissage adaptés aux nouvelles technologies. Cette formation continue est essentielle pour permettre aux professionnels de s'adapter aux transformations du domaine de la cybersécurité

L'exemple de l'impact sur le métier de développeur en cybersécurité est éloquent. Pour ces derniers, l'IA devient un véritable levier, en intervenant tout au long du cycle de développement logiciel :

- **Détection précoce des vulnérabilités** : des outils basés sur la machine learning analysent automatiquement le code pour repérer des failles (injections SQL, erreurs d'authentification, mauvaises configurations). Cela permet de corriger les problèmes dès les premières phases de développement.
- **Revue de code automatisée** : l'IA assiste les développeurs en effectuant des audits continus du code, en suggérant des correctifs et en signalant les pratiques non sécurisées. Elle agit comme un "coéquipier" qui renforce la qualité et la sécurité du code.
- **Génération de code sécurisé** : certains assistants de programmation peuvent proposer du code en intégrant directement des bonnes pratiques de sécurité (gestion des entrées, chiffrement, authentification). Cela réduit les erreurs humaines et accélère le développement.
- **Tests de sécurité intelligents** : l'IA améliore les tests en simulant des attaques et en identifiant automatiquement des scénarios à risque. Elle permet d'aller au-delà des tests classiques en explorant des combinaisons complexes difficilement détectables manuellement.
- **Réduction de la charge cognitive** : en automatisant les tâches répétitives et techniques, l'IA permet aux développeurs de se concentrer sur la logique métier et les décisions critiques, tout en maintenant un haut niveau de sécurité.



Au préalable, notons que l'émergence de l'IA en matière de cybersécurité a un impact sur l'ensemble des professionnels du numérique – ce qui pose la question de l'existence de certifications plus orientées vers la pratique de l'IA appliquées à la cybersécurité - et sur l'ensemble des professionnels utilisant des outils numériques, pas simplement sur les experts cybersécurité. Pour ces derniers, la maîtrise de l'ensemble des dimensions susmentionnées en 3 ou 5 ans est utopique, ce qui impliquera une formation tout au long de la vie.

Cependant, l'émergence de l'intelligence artificielle transforme le contenu des formations en cybersécurité. Cela nécessite un renforcement global des modules IA dans les parcours cybersécurité. Les programmes pédagogiques doivent désormais intégrer à la fois de nouvelles compétences techniques et des approches méthodologiques adaptées aux menaces automatisées. Les programmes doivent préparer les professionnels non seulement à utiliser des systèmes intelligents de défense, mais également à comprendre leurs limites et à adopter une approche stratégique face aux menaces émergentes. Et c'est aussi pour cela, que le développement de softskills devient stratégique : la pensée critique permet d'anticiper les attaques adverses sophistiquées, tandis que la collaboration interdisciplinaire favorise la co-construction de réponses résilientes face à des menaces polymorphes.

• Introduction de compétences liées à l'IA

Les formations doivent inclure la compréhension des algorithmes d'IA appliqués à la cybersécurité, la capacité à analyser de grandes masses de données pour détecter des comportements suspects, et la maîtrise des systèmes automatisés de défense et de réponse aux incidents. Ces compétences viennent compléter les savoir-faire traditionnels en matière de sécurité informatique, de cryptographie et de gestion des vulnérabilités.

• Adaptation aux menaces automatisées

Avec l'utilisation croissante de l'IA par les cyberattaquants, les contenus pédagogiques intègrent désormais :

- Des modules sur la détection et la neutralisation des attaques pilotées par IA ;
- Des simulations réalistes et dynamiques d'incidents de sécurité ;
permettant aux apprenants de se confronter à des scénarios complexes ;
- Une sensibilisation aux risques liés aux systèmes autonomes et aux bots malveillants.



Photo : R - stock.adobe.com

¹¹ <https://talentsdunumerique.com/sites/default/files/pages-editoriales/tdn202501notecompetencesdroit.pdf>
Exemple: Le Digital Services Act, ou règlement sur les services numériques, <https://www.economie.gouv.fr/actualites/numerique-dsa-entre-en-vigueur>

- **Simulations réalistes et apprentissage pratique**

L'IA facilite le développement de simulations avancées de cyberattaques, permettant aux apprenants de se confronter à des scénarios proches de la réalité sans risque pour les infrastructures réelles. Les environnements virtuels pilotés par IA peuvent générer automatiquement des attaques sophistiquées, variées et imprévisibles, renforçant ainsi la capacité de réaction et la prise de décision des professionnels de la cybersécurité. Cet apprentissage se fera par projet intégrant des outils IA.

- **Gouvernance, conformité et éthique de l'IA**

Outre les compétences techniques, les formations doivent développer la capacité à interpréter les recommandations des systèmes IA et à évaluer leurs limites. La réflexion éthique et stratégique devient essentielle, notamment pour comprendre les biais possibles des algorithmes et anticiper les comportements imprévus des systèmes automatisés.

La compréhension des cadres réglementaires (ex : RGPD, AI Act) est également nécessaire, ainsi que de nouvelles compétences : gestion de la conformité (analyse d'impact, registre de traitements, documentation), maîtrise des obligations de transparence et de traçabilité, intégration de la protection des données dès la conception (privacy by design) et capacité à dialoguer avec les juristes et le délégué à la protection des données (DPO). Ces compétences transverses incluent des softskills critiques : pensée critique pour anticiper les attaques adverses, collaboration interdisciplinaire pour co-construire des réponses résilientes, leadership empathique pour fédérer autour des priorités, et communication adaptative pour vulgariser la complexité technique auprès de tous les publics. Ces aptitudes humaines permettront aux futurs professionnels de déployer des solutions d'IA en cybersécurité à la fois performantes, sûres et conformes.

Enfin nous n'oublions pas le nécessaire rapport de ces formations avec le droit et les normes, pour cela nous vous invitons à lire la note que la commission a publié en janvier 2025¹².

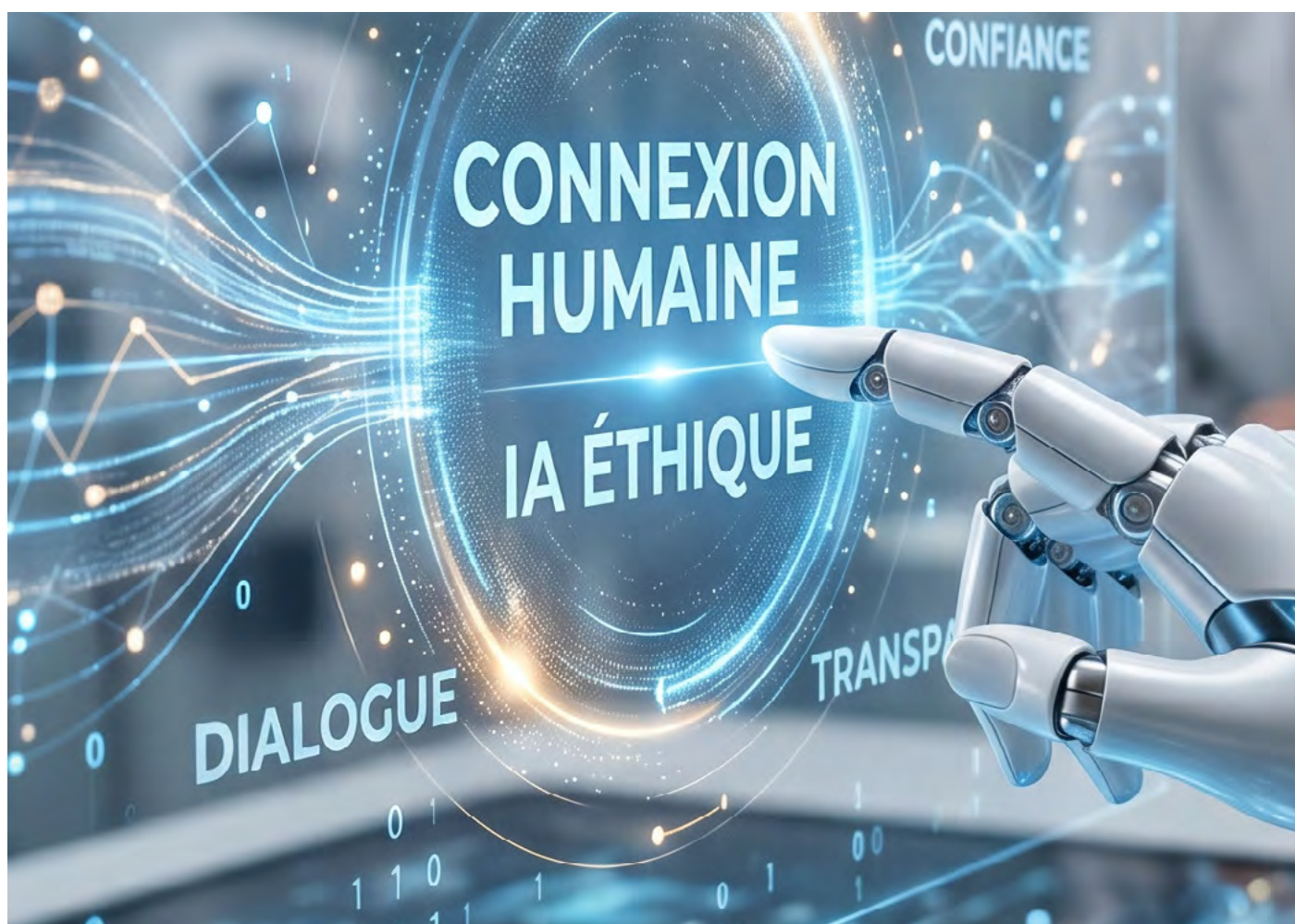


Photo : Maxime - stock.adobe.com

La commission compétences estime qu'il convient d'agir auprès des trois populations susceptibles d'être impactées par l'émergence de l'IA dans la cybersécurité et de construire des parcours de formation spécifiques :

- Pour l'ensemble des professionnels ;
- Pour l'ensemble des professionnels du numérique ;
- Pour les experts de la cybersécurité, stricto sensu.

Pour les deux premières catégories, les besoins en sensibilisation et formation aux concepts et à la pratique sont réels et importants. Cependant, force est de constater que cette dimension est encore trop peu présente ou structurée dans les cursus étudiants, et que de grandes disparités existent d'une formation à une autre, d'une spécialité à une autre, au sein d'un même établissement. L'objectif est de former des profils multi-compétents, disposant d'une vision large, systémique du numérique et de ses enjeux. Cet enseignement ne doit pas être seulement théorique, il doit inclure des ateliers/travaux pratiques afin de confronter les futurs professionnels aux situations concrètes auxquelles ils seront confrontés. Cet enseignement doit également comporter des moments d'échanges, de discussion et des débats sur les notions et les situations rencontrées. Il s'agit de permettre aux étudiants d'acquérir les bons réflexes qui leur seront nécessaires pendant l'ensemble de leur carrière.

Pour répondre à cet effort de massification, il convient de :

- Développer, faire connaître et rendre accessibles les cursus hybrides (cyber & droit, cyber & management...) ¹² ;
- Valoriser les certifications (CEH, ISO 27001, etc.) ;
- Renforcer les formations continues courtes et accessibles, notamment via le e-learning ¹³.

Pour les experts, les établissements de formation doivent :

- Intégrer des modules obligatoires sur l'intelligence artificielle, le machine learning et les modèles génératifs dans les cursus de cybersécurité ;
- Former les étudiants aux risques spécifiques de l'IA : prompt injection, empoisonnement des données, attaques adverses et fuite d'informations ;
- Développer des laboratoires pratiques permettant de tester et sécuriser des systèmes d'IA réels ;
- Enseigner l'utilisation de l'IA comme outil de cyberdéfense pour la détection des menaces et la réponse aux incidents ;
- Renforcer les compétences en gouvernance, éthique et conformité liée aux réglementations sur l'IA ;
- Mettre à jour régulièrement les programmes afin de suivre l'évolution rapide des technologies et des menaces ;
- Développer des partenariats avec les entreprises et organismes spécialisés en cybersécurité et en IA ;
- Encourager une approche pluridisciplinaire combinant sécurité informatique, science des données, droit et gestion des risques.

¹² Citons notamment : le Master Droit du numérique – parcours Informatique et droit (UPEC) ; le Master Droit du numérique – parcours Tiers de confiance et sécurité numérique (La Rochelle Université) ; le Master Droit du numérique – parcours Droit de la cybersécurité (Université de Caen).

¹³ Nous pensons notamment aux dispositifs existants comme les formations courtes labellisées SecNumedu-FC et les stages du CFSSI/ANSSI (panorama SSI, méthode EBIOS, fondamentaux techniques...) pour les professionnels en activité ; les MOOC en cybersécurité de l'ANSSI (SecNumAcadémie et MOOC EBIOS Risk Manager), gratuits et certifiants, qui permettent une montée en compétences à distance ; les parcours en ligne ou hybrides proposés par des écoles spécialisées (ex. formations professionnelles Guardia, SecureSphere by EPITA).



Photo : Agis - stock.adobe.com



**TALENTS DU
NUMÉRIQUE** DES MÉTIERS
D'AVENIR
POUR UN MONDE
À INVENTER

INFOS

CONTACT

À bientôt !

Suivez toute l'actualité de Talents du Numérique
sur le site www.talentsdunumerique.com

et sur nos réseaux sociaux :
www.talentsdunumerique.com/communaute

Rémi Ferrand (délégué général)
remi.ferrand@talentsdunumerique.com