GOUVERNEMENT
Liberté
Égalité
Fraternité

CCI HAUTS-DE-SEINE PARIS ILE-DE-FRANCE

CROCIS L'économie en Île-de-France Chiffres, analyses, tendances

Un centre d'observation de CCI PARIS ILE-DE-FRANCE PROSPECTIVE

IA School

Université Paris Nanterre

pôle emploi

FRANCE 2030

« Diagnostic CS&IA-92 »

Premier levier des transitions numériques et écologiques, la formation des jeunes et des salariés permet de renforcer le capital humain indispensable au fonctionnement de nos entreprises et au-delà de toute la société. C'est aussi le meilleur moyen pour proposer des emplois durables et de tous niveaux de qualification sur l'ensemble du territoire.

C'est également une des conditions majeures pour la réussite du plan France 2030 : soutenir l'émergence de talents et accélérer l'adaptation des formations aux besoins de compétences des nouvelles filières et des métiers d'avenir. 2,5 milliards d'euros de France 2030 seront mobilisés sur le capital humain pour atteindre cette ambition.

L'appel à manifestation d'intérêt « Compétences et métiers d'avenir » s'inscrit dans ce cadre et vise à répondre aux besoins des entreprises en matière de formations et de compétences nouvelles pour les métiers d'avenir.

Dans le cadre de ce dispositif, **la réalisation de diagnostics des besoins en compétences et en formations sont financés et diffusés.**

DIAGNOSTIC DE FORMATION
20 février 2023

Sommaire

Préambule

Le diagnostic sur la cybersécurité et l'intelligence artificielle a été réalisé par le Consortium composé de :

- La Chambre de Commerce et d'Industrie des Hauts-de-Seine
- Le CROCIS
- L'IA School
- L'Université Paris Nanterre
- Pôle Emploi

En réponse à l'appel à manifestation d'intérêts « Compétences et métiers d'avenir » qui, dans le cadre du programme France 2030, vise à répondre aux besoins des entreprises en matière **de formations et de compétences nouvelles pour les métiers d'avenir.**

Les auteurs tiennent à remercier l'ensemble des membres du Comité de Pilotage, les interlocuteurs de la Caisse des dépôts et consignations ainsi que tous les représentants d'entreprises interrogées, répertoriées en Annexe 4 lorsqu'elles n'ont pas souhaitées rester anonymes, qui ont accepté de partager des informations précieuses pour l'étude.

Contexte et enjeux du diagnostic

La digitalisation croissante de l'économie s'accompagne à la fois de l'augmentation de risques de cybercriminalité mais aussi de l'opportunité de création de valeur au travers du développement de l'intelligence artificielle (IA).

Ainsi, entre 2020 et 2021, le nombre d'intrusions avérées dans les systèmes d'information, signalées à l'ANSSI, a augmenté de 37%. Toutes les entreprises sont concernées : en premier lieu les TPE, PME-ETI qui représentaient 34% des victimes en 2021, les collectivités 19% et les entreprises stratégiques 10%.

Définition de l'Agence Nationale de la Sécurité des Systèmes d'Information :

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Dans le même temps, l'IA se diffuse dans les entreprises au travers d'applications plus ou moins complexes. Toutefois, le bénéfice de l'IA qui en résulte n'est pas optimisé. Selon une étude d'Accenture (juin 2022) auprès de 1 200 entreprises, « seules 12% ont suffisamment fait progresser la maturité de l'IA pour booster leur croissance et leur transformation ».

Définition du Parlement européen :

Intelligence Artificielle

L'intelligence artificielle représente tout outil utilisé par une machine afin de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité.

Le besoin des entreprises d'une cybersécurité renouvelée et renforcée pour s'adapter aux attaques d'une part, le développement et l'usage de l'IA d'autre part, génèrent des besoins en compétences.

Selon une enquête sur les profils de la cybersécurité de l'ANSSI[1], 45% des professionnels de la cybersécurité ont moins de 5 ans d'ancienneté et 73% exercent dans le secteur privé. 7 206 offres d'emploi étaient à pourvoir en Ile-de-France en cybersécurité en 2021. L'Île-de-France, concentre plus de la moitié des professionnels de la cybersécurité. La cybersécurité se caractérise par des professionnels principalement issus d'environnements techniques très qualifiés en cybersécurité et informatique de niveau bac +5 et plus, possédant un diplôme et/ou une certification dans le domaine de la cybersécurité.

[1] Les profils de la cybersécurité Enquête 2021.

L'association France Digitale alerte sur la nécessité de s'intéresser également à des emplois de l'IA, de niveau Bac+2, Bac pro, ne nécessitant pas de connaissances en mathématiques et en informatique poussées pour épauler les ingénieurs (préparateur de données, qualiticien de données, assistant data), emplois qui peuvent contribuer à pallier la pénurie de talents[2]. Les start-ups de l'IA ont permis la création de 13 459 postes (pour 70 000 emplois indirects générés) et prévoient de recruter 9 000 personnes en 2022, selon une étude réalisée par France Digitale. L'ensemble de ces postes n'est pas dévolu aux seuls ingénieurs ou chercheurs (testeurs, analystes, contrôleurs qualité).

Le besoin de compétences dans les domaines de la cybersécurité et d'IA des entreprises s'accélèrent. Les dirigeants de PME prennent la mesure de leur vulnérabilité et des conséquences des cyberattaques et entrevoient l'apport de l'IA en termes de création de valeur. Par ailleurs, le financement de projets à travers France Relance favorise la création d'emplois. A titre d'exemple, le projet de recherche Beyond 5G lancé par Thales en collaboration avec Ericsson, les écoles de l'Institut Mines-Telecom et Eurecom à Sophia-Antipolis, bénéficiera d'un cofinancement de 4,56M€. Ce projet visant à élaborer des architectures et solutions 5G souveraines prévoit la définition et l'expérimentation de composantes de cybersécurité adaptées à de nouvelles architectures, en s'appuyant notamment sur des éléments d'IA et de big data. Plusieurs dizaines de techniciens, ingénieurs seront nécessaires au développement de ce projet.

Les besoins en compétences dans les territoires sont indissociablement liés au tissu entrepreneurial. Les entreprises de services du numérique (ESN) portent 50% des offres d'emploi. Le secteur Banque-Assurance 20%.

Le tissu entrepreneurial des Hauts-de-Seine compte[3] 199 813 établissements, dont :

- 78,96% n'ont aucun salarié, 16,1% de 1 à 9 salariés, 4,2% de 10 à 99 salariés, 0,62% de 100 à 499 salariés, 0,12% plus de 500 salariés.
- Le secteur des services représente ¾ du tissu entrepreneurial.
- 11 119 entreprises de services du numérique[4] sont comptabilisées dont 161 ont 100 salariés et plus, et 8 246 n'ont aucun salarié.

C'est un tissu particulièrement divers et contrasté. Ainsi, aux côtés de grandes entreprises de très haute technologie, telles que Thalès, EDF, TotalEnergies, des entreprises de services numériques avec IBM, Microsoft, Oracle, Worldline, Keyrus et les grands cabinets de conseil qui ont développé des secteurs Numérique comme E.Y, Mazars, il existe un réseau de petites et moyennes entreprises dont les dirigeants ont une sensibilité variable à la nécessité d'opérer des transformations importantes de leur chaine de production industrielle et ou de service par de l'introduction d'IA et de protéger leurs systèmes d'information des attaques.

Le quartier d'affaires Paris La Défense, premier quartier d'affaires d'Europe, accueille de grandes entreprises internationales fortement exposées aux risques de cyberattaques et qui par ailleurs ont recours à l'IA dans l'ensemble de leur process. C'est sur ce même territoire qu'est implanté Campus Cyber qui rassemble les principaux acteurs nationaux et internationaux de la cybersécurité.

Fort de ce tissu d'entreprises, les Hauts-de-Seine enregistrent d'importantes tensions sur le marché de l'emploi des métiers rattachés à l'informatique. Au 3ème trimestre 2022, Pôle emploi comptabilise 20 290 offres dans la catégorie « études et développement informatique » pour 2 560 demandes.

Le diagnostic a pour objectif de :

- Définir et structurer les besoins de compétences des entreprises des Hauts-de-Seine, sans distinction de taille et de secteur, en matière de cybersécurité et d'IA en vue de la mise en place d'une offre de formation adaptée, notamment de formations et de parcours (apprentissage) de proximité ainsi qu'à l'accueil de candidats aux profils divers (jeunes formés ou peu formés, personnes en reconversion professionnelle, sous réserve de prérequis).

[2] IA et data. 25 propositions pour une stratégie européenne. France Digitale 2020

[3] Sirene 2021

[4] Codes : 5829A, 5829C, 6201Z, 6202A, 6202B

Au-delà de ce diagnostic, le Consortium souhaite initier une dynamique territoriale, dans le temps, autour de 2 axes :

1. Mieux accompagner les TPE-PME dans leur développement par le recours à l'IA et à la cybersécurité, dans leur process de production au travers de recrutements adaptés. Si les grands groupes sont structurés afin de répondre à ces enjeux, la plupart des entreprises (TPE-PME) n'ont pas mis en place ou ne sont pas en mesure d'assurer leur transition numérique dans toutes ses dimensions.
2. Former les jeunes et les demandeurs d'emploi aux compétences demandées.

Cette étude est décomposée en 3 parties :

1. Les besoins en compétences et en formation des entreprises
2. L'offre de formations
3. Accompagner les évolutions professionnelles et l'accès aux métiers de la cybersécurité et de l'IA d'un large public

Partie 1 : Les besoins en compétences et en formation des entreprises des Hauts-de-Seine

Les objectifs de l'analyse des besoins en compétences et en formations des entreprises des Hauts-de-Seine sont de répertorier et de quantifier :

- Les pratiques en matière de cyber sécurité (CS) et d'Intelligence Artificielle (IA) concernant la protection et l'utilisation des données massives ;
- Les besoins de compétences et de formations pour les salariés.

1. Méthodologie

Le périmètre d'étude

L'étude concerne les entreprises implantées sur les Hauts-de-Seine de plus de 5 salariés, et de tout secteur (à l'exception des commerces de détail).

La taille et le secteur d'activité des entreprises peuvent être à l'origine d'une grande diversité de pratiques et de besoins de compétences en matière d'IA et de cybersécurité, notamment :

- Certaines entreprises intègrent la cybersécurité et/ou l'IA au cœur de leurs stratégies avec des équipes dédiées : offre de services, intégration dans les fonctions essentielles de l'entreprise, etc.
- D'autres ont recours à un prestataire pour faire face à leurs besoins ;
- Enfin, des entreprises ne sont concernées ni par la cybersécurité ni par l'intelligence artificielle.

Cette hétérogénéité potentielle justifie des études par catégorie en fonction de la taille.

Techniques de recueil des données

L'étude fait appel à plusieurs techniques de recueil de données complémentaires :

- Enquêtes par questionnaire et entretiens semi-directifs auprès des entreprises
- Recherches documentaires
- Relevés d'offres d'emplois
- Entretien avec l'OPCO Atlas, l'opérateur de compétences de la branche professionnelle du secteur des services financiers et du conseil dont numérique

La population d'entreprises cible de l'étude a été divisée en trois catégories suivant leur taille. Le mode d'administration des questionnaires et leurs types ont été différents pour chacune de ces trois catégories :

- Enquête quantitative auprès des :

- Entreprises de plus de 20 salariés par téléphone ;
- Entreprises de 5 à 19 salariés, questionnaire en ligne.

- Enquête qualitative par entretiens semi-directifs en face à face avec :

- De grandes entreprises (notamment du CAC 40) et les collectivités
- Quelques TPE/PME

1.1. Enquête quantitative sur les besoins des entreprises

Au regard de la diversité des entreprises étudiées, il y avait un besoin de préalablement mesurer la sensibilité des entreprises à l'égard des enjeux de la cybersécurité, de leurs sentiments et de leurs vulnérabilités, et de rendre compte des mesures utilisées par les dirigeants d'entreprises.

Le fichier de base de l'enquête

Le Consortium a réalisé cette enquête à partir d'une extraction du fichier des entreprises inscrites auprès de la CCI de région Paris Ile-de-France et implantées sur les Hauts-de-Seine et ce, en conformité avec le RGPD.

Le questionnaire d'enquête

Un questionnaire de 47 questions a été construit pour collecter des informations, sur :

- La nature des données disponibles au sein de l'entreprise et leur traitement ;
- L'exposition au risque cyber et l'investissement réalisé pour y faire face ;
- Le développement de l'IA ;
- Les besoins en compétences, en recrutement et en formation pour les deux secteurs ;
- Les évolutions des métiers cyber et IA au sein de l'entreprise ;
- Mais aussi en raison de la diversité des entreprises interrogées, mesurer leur perception d'une part du risque d'exposition à la cyberattaque ; d'autre part l'usage de l'IA dans leur entreprise et de son apport possible.

Le questionnaire a été adapté pour les entreprises de services numériques et des sièges sociaux (auxquelles le plus souvent sont rattachées les directions : informatique, du développement, de la sécurité, …)[5].

Administration du questionnaire

Pour les entreprises de plus de 20 salariés, le questionnaire a été administré par **téléphone. L'enquête,** confiée à un prestataire (l'entreprise Qualitest), a été réalisée entre le 7 juin 2022 et le 4 juillet 2022.

3 616 entreprises ont été contactées dont 1 501 entreprises de services numériques et des sièges sociaux (5 relances sur chaque numéro). Les réponses ont été anonymisées.

120 réponses ont été recueillies, dont 49 entreprises de l'économie du numérique, principalement des PME & TPE

Le nombre de réponses collectées à la suite de l'enquête téléphonique est faible mais permet de mettre en évidence **de grandes tendances** *en matière de cybersécurité et d'intelligence artificielle. Toutefois, le nombre de réponses limité ne permet pas une analyse des réponses par secteur d'activité autre que celles du secteur de l'économie du numérique dont les informations ont été recueillies de façon distincte.*

Pour les entreprises entre 5 et 19 salariés, l'enquête a été réalisée par **mail** entre le 17 juin et le 25 juillet 2022. 875 contacts ont été interrogés dont 351 du secteur du numérique et 524 des autres secteurs. Le questionnaire avait été adapté pour les entreprises du numérique.

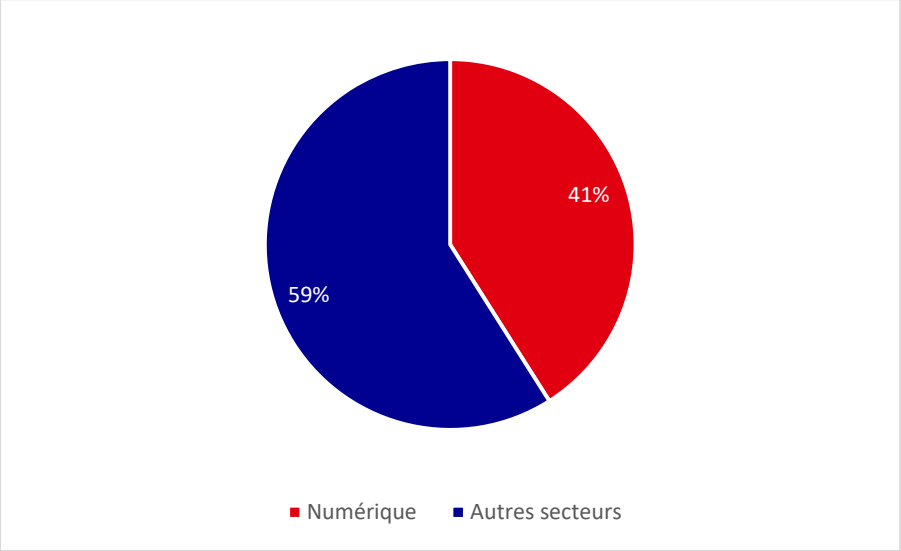
En dépit de 3 relances, seules 24 réponses ont été enregistrées (8 entreprises du secteur du numérique et 16 entreprises autres secteurs). Au regard du **nombre de retours trop faible**, les réponses[6] n'ont pas été retenues pour l'analyse.

[5] Codes NAF de l'INSEE : 5829A éditions logiciels système et réseaux - 5829C éditeurs de logiciels - 6201Z Programmation informatique - 6202A Conseil en systèmes et logiciels informatiques - 6202B Tierce maintenance de systèmes et d'applications informatiques - 7010Z Activités sièges sociaux - 8542Z Enseignement privé - 8559A Formation continue adultes

[6] Réponses anonymes

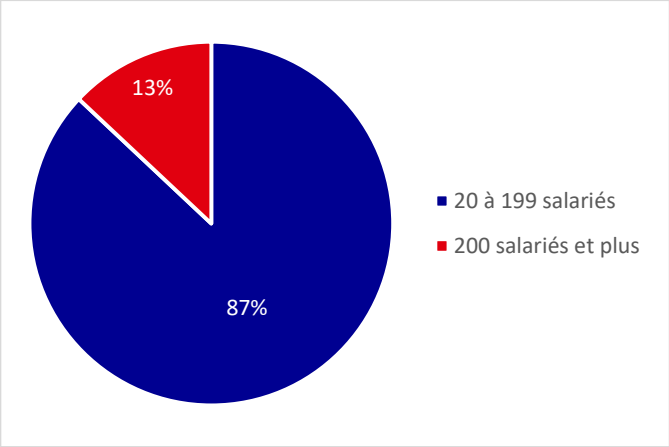
Le taux de non-réponses est particulièrement élevé pour les deux enquêtes (téléphone et mail). Le prestataire, qui a conduit pour d'autres donneurs d'ordre des enquêtes sur la sécurité numérique, s'était heurté aux mêmes difficultés. De même, ce niveau de taux de non-réponse est rare pour des enquêtes réalisées par la CCI Paris Île-de-France par mail, à partir de ce même fichier d'entreprises.

REPARTITION PAR SECTEUR DES ENTREPRISES AYANT REPONDU AU QUESTIONNAIRE



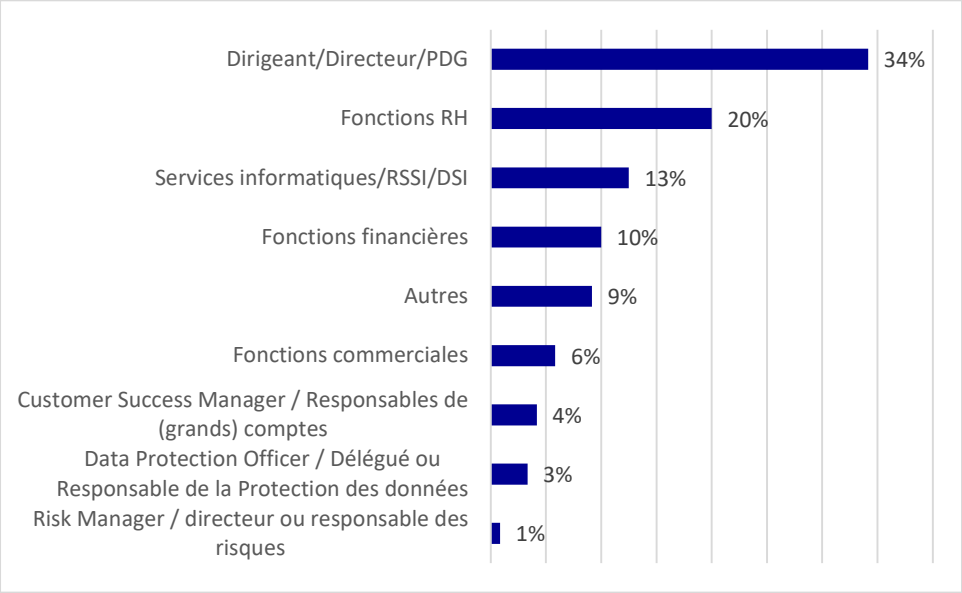
La répartition des entreprises ayant répondu entre secteur numérique (41%) et autres secteurs (59%) reprend celle du fichier de base.

TAILLE DES ENTREPRISES AYANT REPONDU AU QUESTIONNAIRE



Les entreprises qui constituent l'échantillon sont à 87% des petites et moyennes entreprises, elles ont un effectif compris entre 20 et 199 salariés (104). Seules 13% des entreprises qui ont répondu ont plus de 200 salariés (16).

FONCTIONS DES PERSONNES REPRESENTANT LES ENTREPRISES AYANT REPONDU AU QUESTIONNAIRE



Le tableau des fonctions au sein de l'entreprise des répondants correspond à l'organisation et au fonctionnement des petites et moyennes entreprises dans lesquelles le dirigeant assume la responsabilité de très nombreuses fonctions et, les questions relatives aux compétences et à l'emploi sont orientées vers la personne ou le service en charge des ressources humaines. Les petites entreprises – à l'exception de celles du numérique - n'ont pas la taille critique pour intégrer ou attirer des professionnels aux seules compétences informatiques.

1.2. Les entretiens semi-directifs en face à face

- **16 entretiens** ont été conduits auprès de :

- **9 grandes entreprises** ou institutions[7]

Eurogroup Consulting, EDF, Keyrus, La Poste, Mazars, Paris La Défense, Solocal, Thalès Group, Hôpital Foch.

Ces entretiens ont permis d'apporter des éléments essentiels au diagnostic puisque ces groupes sont à un stade de maturité très avancé et expriment des besoins autres que ceux des PME/TPE. Ces entretiens ont été sources d'éléments prospectifs.

- **7 PME/TPE**, tous secteurs confondus.

Oceane consulting group, Roux ingenierie, France Cobalt, Entreprise Sauvaget, Cap Enfants, Mavica, Irea

Ils ont permis, en complément de l'enquête quantitative, de mieux comprendre comment elles appréhendent et formalisent les problématiques de cybersécurité et d'IA (investissements, stratégies etc.).

- **2 Focus group**

Des focus group dédiés respectivement à l'IA et à la cybersécurité

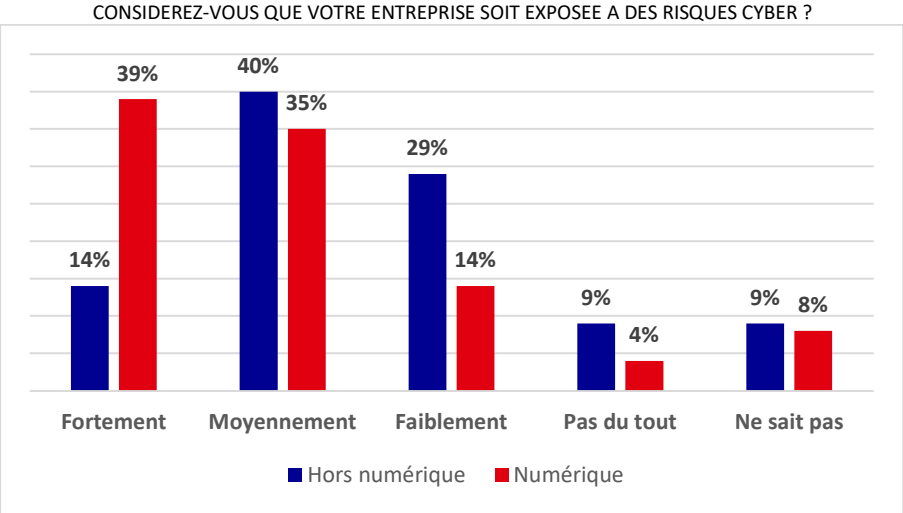
[7] Trois entretiens ont été conduits au sein du cabinet Mazars auprès de trois dirigeants aux secteurs d'intervention différents : conseil en Cybersécurité, conseil en IA, Réseaux informatiques.

2. Analyse des besoins en compétences des entreprises des Hauts de Seine exprimés lors des enquêtes

Un lien a été recherché entre d'une part la perception à l'exposition aux risques de cyberattaques et à l'introduction et au développement de l'IA dans les process de production et décision au sein de l'entreprises et d'autre part l'expression de besoins en compétences.

L'enquête quantitative et les entretiens semi-directifs confirment les écarts d'appréhension, et de prise en compte de la cybersécurité et de l'IA au sein de l'entreprise entre de très nombreuses petites et moyennes entreprises et les grandes entreprises.

La cybersécurité



Près de 75% des entreprises du secteur du numérique estiment être exposées fortement ou moyennement à des risques cyber (rançonnage, espionnage, sabotage, phishing, atteinte à l'image ou encore cybercriminalité) contre 54% pour les entreprises des autres secteurs alors même que certaines stockent des données sensibles (clients, industrielle, RH…).

Pour faire face à cette vulnérabilité, 77% des entreprises de l'économie du numérique ont mis en place un référent ou une équipe dédiée à la cybersécurité, le taux est de 45% pour les entreprises des autres secteurs d'activité.

De même, 71% d'entre elles ont investi dans du matériel. La mise en place d'anti-virus, VPN, de serveurs sécurisés ou encore de pare-feu sont suffisantes aux yeux des dirigeants[8].

Les TPE et PME interrogées, intégrées à un réseau ou à un groupe d'entreprises (filiales), bénéficient des investissements des systèmes d'information de la tête de réseau.

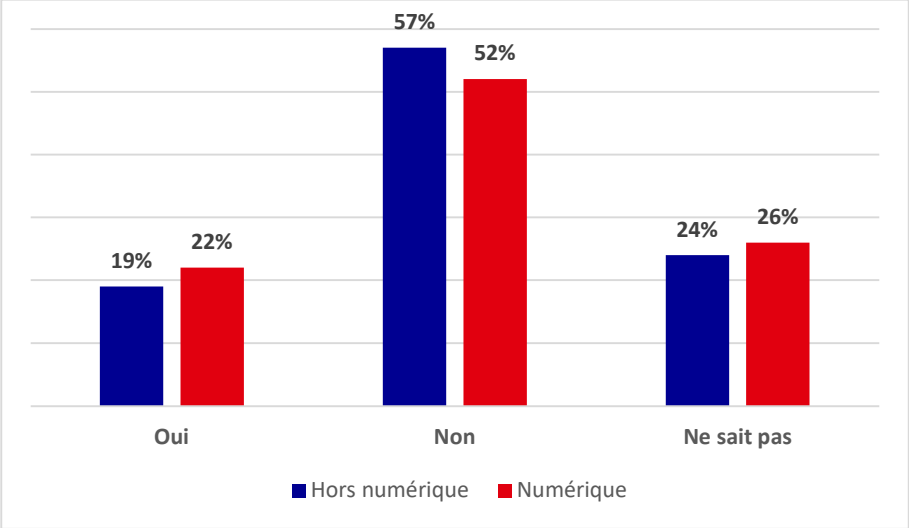
90% des répondants envisagent un renforcement prochain de la cybersécurité de leur entreprise pour répondre aux exigences de leurs clients, fournisseurs et autres partenaires.

[8] Une étude réalisée par CCI France, La Tribune et LCI, en octobre 20228 met en évidence une moindre vigilance des dirigeants envers les risques de cyberattaques, à des degrés divers, sur une année (octobre 2021 / octobre 2022). Et ce, que l'entreprise ait été victime ou non d'une attaque. La part des dirigeants qui n'ont mis en place aucune mesure de défense sur cette période est en augmentation (de 2 points) par rapport à la période précédente. La grande consultation des entrepreneurs – Sondage d'opinionWay pour CCI France / La Tribune / LCI : Les dirigeants d'entreprise et la cybersécurité. Octobre 2022

Les grandes entreprises disent leur très grande vigilance à prévenir des attaques autour d'équipes dédiées, par le développement de modèles intégrant de l'IA et des campagnes importantes de sensibilisation et de responsabilisation de tout le personnel.

L'Intelligence Artificielle

VOTRE ENTREPRISE A- T-ELLE RECOURS A DES APPLICATIONS QUI FONT APPEL A L'IA ?



L'enquête quantitative fait apparaître peu de différences entre les PME numériques et celles des autres secteurs d'activité quant à leur recours à des applications faisant appel à l'IA.

Un quart des répondants n'ont pas de vision de l'usage l'IA. Plus de la la moitié des PME déclarent ne pas recourir à des application en IA. L'un des objectifs de la stratégie nationale pour l'intelligence artificielle est de corriger cette situation, en accélerant la diffusion de systèmes IA responsables au sein des TPE et PME.

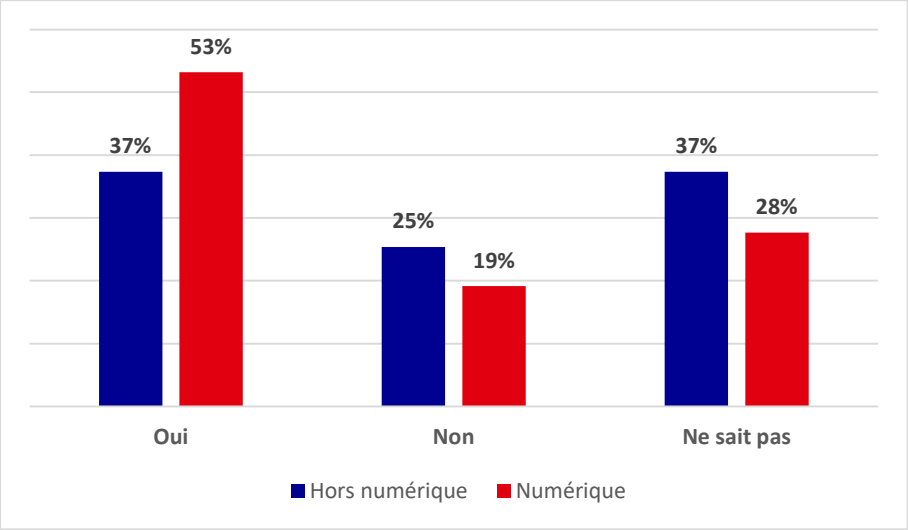
Les entreprises qui ont recours à l'IA le font principalement sur les fonctions marketing/vente (47%) et processe de services (26%).

Les grandes entreprises sont engagées, depuis plusieurs années, dans le développement continu de modèles d'IA, porté par des moyens importants de mise en œuvre (équipes, financement).

2.1. L'appréciation des compétences internes à l'entreprise

L'objectif est de mesurer la satisfaction des entreprises interrogées sur le niveau de compétences de leurs collaborateurs et d'identifier les compétences qui doivent faire l'objet d'une actualisation et ainsi connaître les formations à mettre en place (contenu et volume).

ETES-VOUS SATISFAITS DU NIVEAU DE COMPETENCES IA OU CYBER DE L'ENSEMBLE DES COLLABORATEURS ?

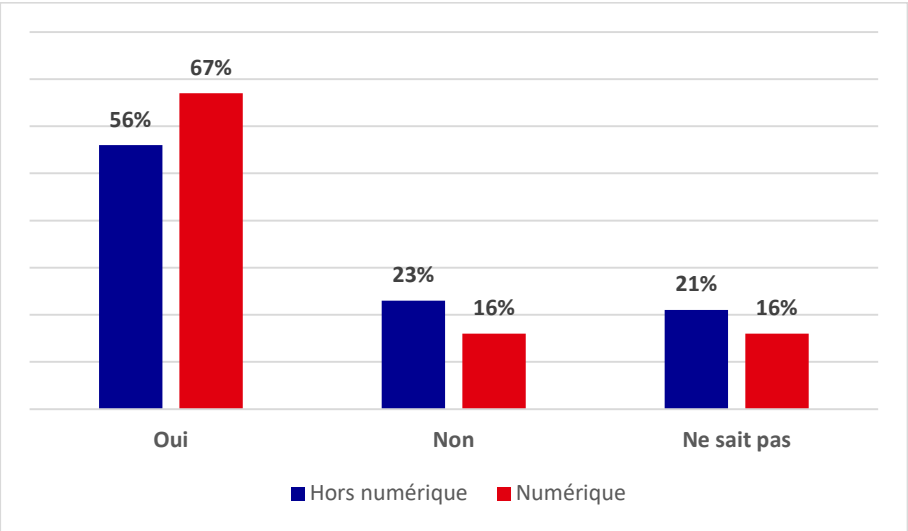


37% des entreprises des secteurs hors numérique sont satisfaites du niveau de l'ensemble des collaborateurs, cette satisfaction est de 53% pour les entreprises du numérique.

Le niveau de satisfaction est plus important concernant les compétences en cybersécurité qu'en IA. Ce qui s'explique par les actions de sensibilisation aux enjeux de la cybersécurité et de formation de plus en plus adressées à l'ensemble des collaborateurs notamment au travers de jeux pédagogiques, e-learning, passeport cyber, exercices etc.

25% des entreprises hors numérique et 19% des entreprises de l'économie du numérique expriment une insatisfaction sur le niveau de compétences ou de sensibilisation des collaborateurs aux dangers des attaques (phishing, rançonnage, espionnage etc.).

LES COMPETENCES DES COLLABORATEURS SONT-ELLES MISES A JOUR ?



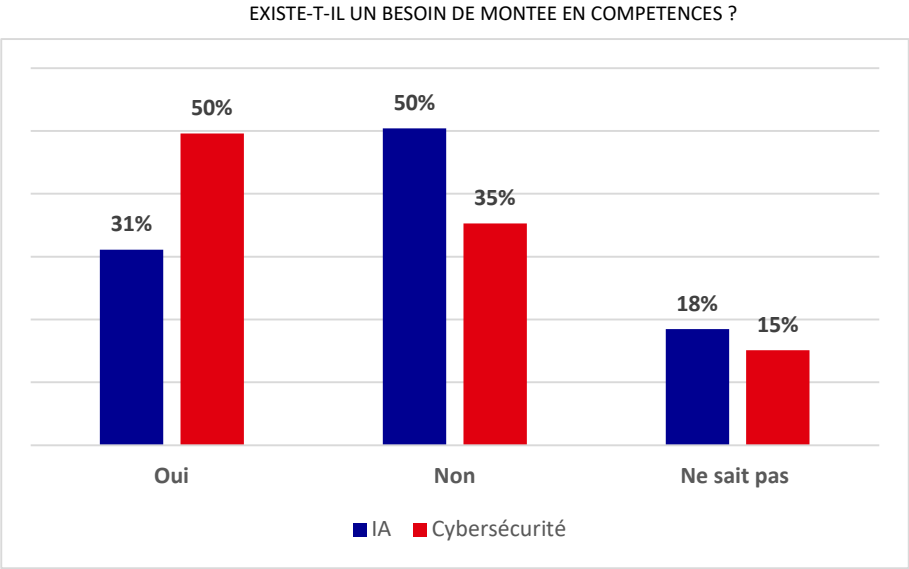
Les entreprises, qu'elles soient du hors numérique (56%) ou de l'économie du numérique (67%), mettent en place des actions d'actualisation des compétences de leurs collaborateurs sur les problématiques de cybersécurité et/ou d'IA.

Les entreprises de l'économie du numérique mettent à jour les compétences de leurs collaborateurs régulièrement (68%). Le taux est un peu plus faible pour les entreprises hors numérique même si plus de la moitié (53%) le font aussi régulièrement.

Concernant les **équipes dédiées** à la cybersécurité et à l'IA, la montée en compétences se fait principalement au travers de l'expérience et de la pratique quotidienne de cas.

Les grandes entreprises ont mis en place des outils de mises en situations réelles comme des exercices de phishing, ou encore des formations afin de sensibiliser les collaborateurs aux risques liés à la cybersécurité. Les moyens mis en œuvre sont difficilement applicables pour des entreprises de plus petite taille.

2.2. Les besoins en montée de compétences ou compétences nouvelles des entreprises



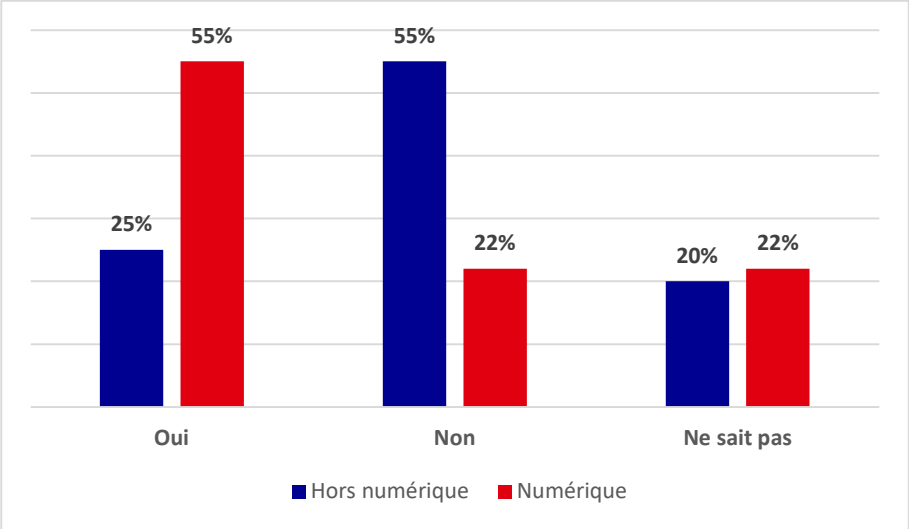
Une entreprise sur deux exprime un besoin de montée en compétence des collaborateurs en cybersécurité, il s'agit principalement (59%) des entreprises du secteur numérique.

De même, une entreprise sur deux déclare ne pas avoir besoin de montée en compétence en IA, dont 38% sont des entreprises du numérique.

Les grandes entreprises gèrent les évolutions de compétences des collaborateurs dédiés principalement par des mises en situation professionnelle, mais aussi des formations complémentaires de courte durée.

Les besoins de compétences générées par la mise en place d'infrastructures et/ou de programmes nouveaux sont assurés par des formations constructeurs.

L'ENTREPRISE A-T-ELLE BESOIN DE NOUVELLES COMPETENCES ?

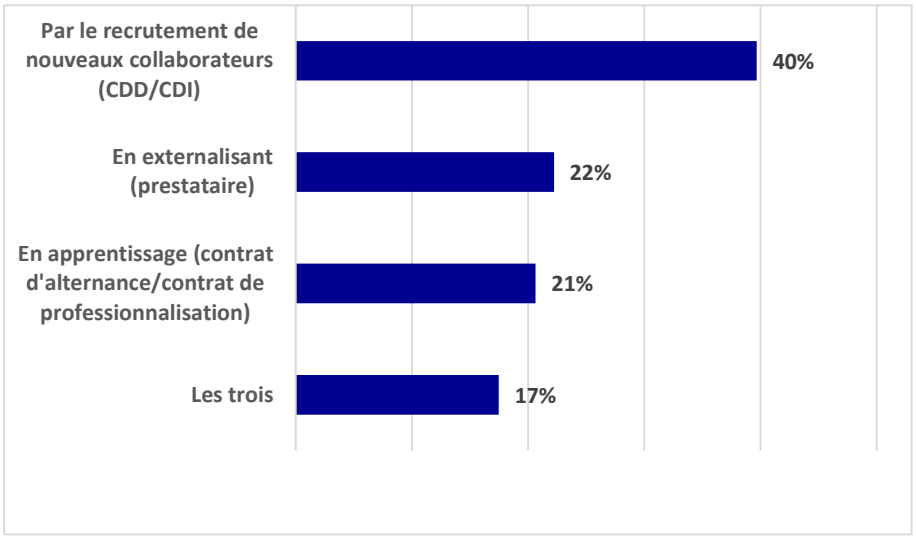


Les besoins en compétences nouvelles émanent principalement d'une part des entreprises du Numérique (55%), d'autre part des entreprises numériques ou non qui utilisent l'IA.

Les grandes entreprises du numérique expriment des besoins de nouvelles compétences complémentaires à celles déjà présentes dans l'entreprise, notamment en matière éthique et juridique.

Plus de la moitié des entreprises n'ont pas de besoin de compétences nouvelles.

COMMENT ENVISAGEZ-VOUS D'ACQUERIR CES NOUVELLES COMPETENCES ?



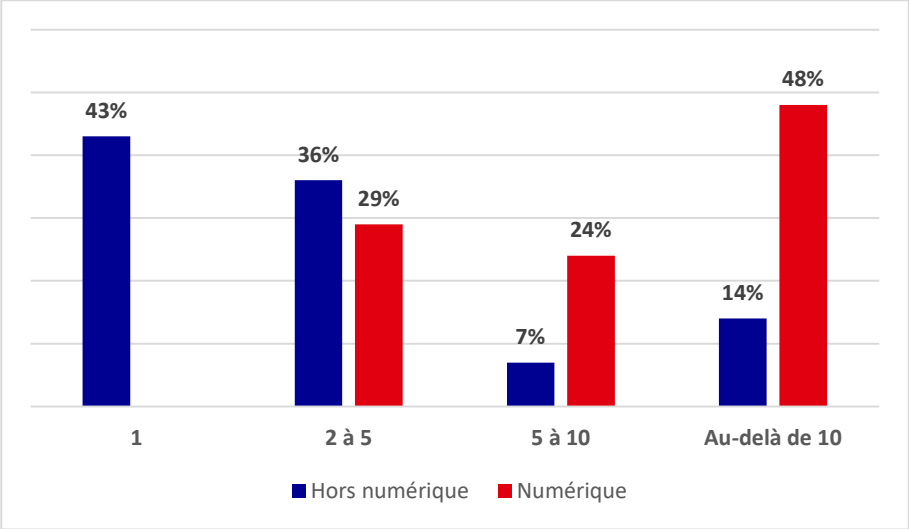
Pour faire face à ce besoin de nouvelles compétences, les entreprises projettent de recruter de nouveaux collaborateurs en CDD ou CDI (40% des réponses), d'externaliser par le recours à un prestataire l'activité concernée par le besoin (22% des réponses), de recruter un alternant (21% des réponses) ou les trois (17% des réponses).

Le recours à l'apprentissage ou à l'alternance est différemment perçu, des responsables informatiques ont mis en avant, lors des entretiens, la difficile compatibilité du rythme de l'alternance avec les besoins des métiers en cybersécurité. C'est pourquoi, ils préfèrent recruter des stagiaires.

Face aux difficultés de recrutement de collaborateurs, de fidélisation de ceux-ci, de la surenchère de la part de certaines entreprises pour attirer des compétences, les entreprises choisissent d'externaliser, faisant ainsi glisser les besoins en recrutement et compétence sur les entreprises de services numériques.

2.3. Les besoins en recrutements

COMBIEN DE COLLABORATEURS CELA REPRESENTE ?

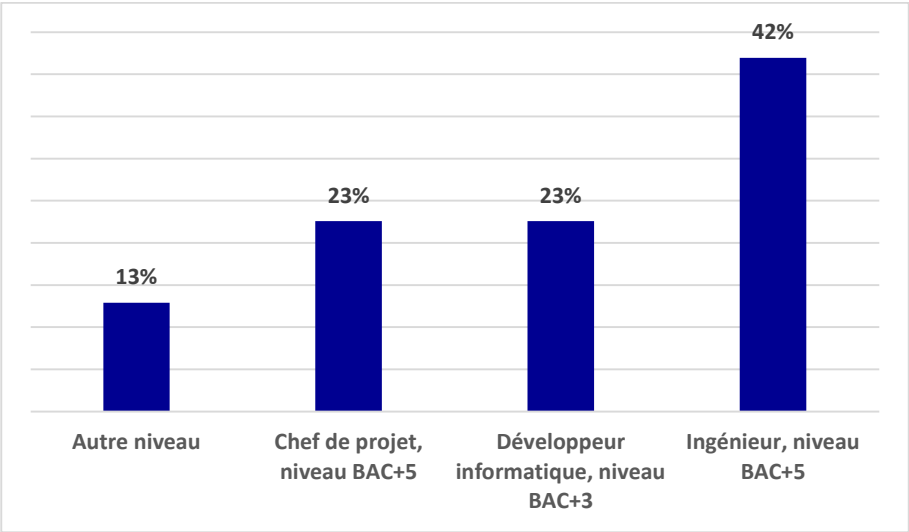


Seulement 30% des entreprises interrogées sont en mesure d'évaluer leur besoin en recrutement, principalement des entreprises numériques qui sont le plus en demande de volume important de nouveaux collaborateurs : 10 et plus.

A l'inverse, les besoins des entreprises hors secteur numérique se limitent à 1 personne.

Les grandes entreprises interrogées qui ont des implantations sur l'ensemble du territoire national évaluent au niveau du groupe, elles ne territorialisent pas.

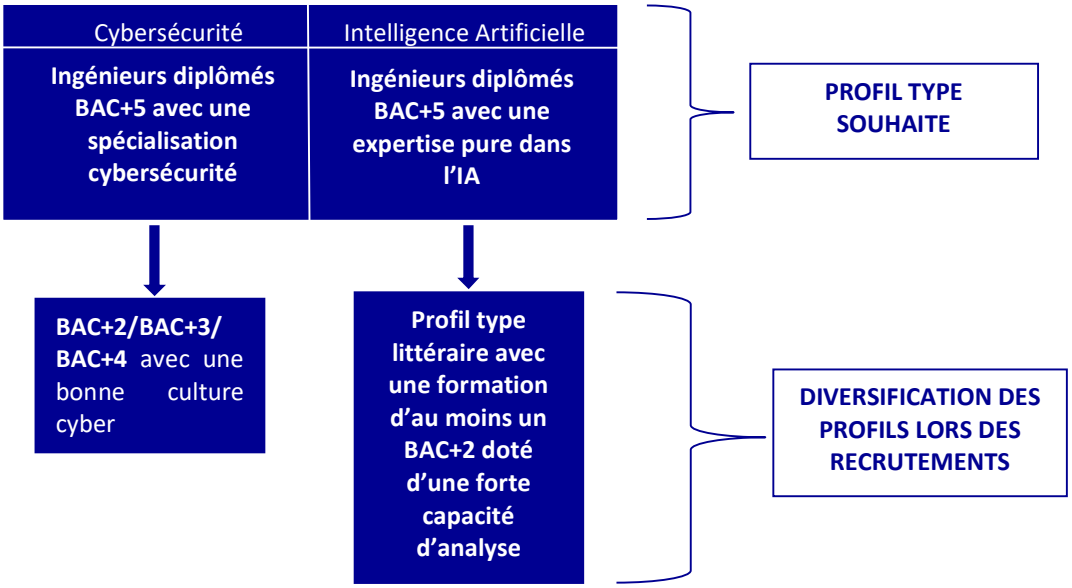
SUR QUELS PROFILS ENVISAGEZ-VOUS LE RECRUTEMENT DE COLLABORATEURS ?



Qu'elles soient petites, moyennes ou grandes, les entreprises affichent la volonté de recruter principalement des profils de niveau BAC+5 (65% des réponses) et dans une moindre quantité des profils de niveau BAC+3 (23%).

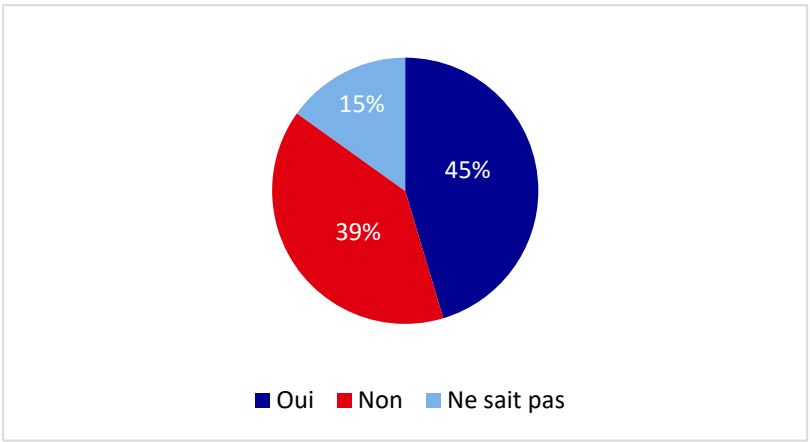
Les grandes entreprises recherchent principalement des ingénieurs de niveau Bac+5, mais aussi des Bac+2/Bac+3, Bac+4 avec une bonne culture cyber pouvant monter en compétences au sein de l'entreprise.

Les évolutions des métiers liés à la data, et le décloisonnement du métier de Data Analyst opérés ces dernières années ont entrainé une hausse des besoins en spécialiste de la donnée dans les grandes entreprises. Les profils recherchés dans ce domaine sont des profils d'ingénieurs (Bac+5) avec une spécialisation dans l'IA ou des profils plus littéraires de niveau au moins Bac+2 dotés d'une forte capacité d'analyse, et une importante curiosité. Un bon niveau en mathématiques et/ou dans des matières scientifiques est important afin de comprendre et de mettre en place des modèles d'IA. Le manque de compétences recherchées sur le marché pousse les grandes entreprises à recruter hors de France. D'autres accompagnent le développement de compétences des collaborateurs de profil ingénieur plus généraliste déjà dans l'entreprise au travers de mobilités internes.



2.4. Les besoins en formation des entreprises

ENVISAGEZ-VOUS DE FORMER DES COLLABORATEURS EN PLACE DANS L'ENTREPRISE ?

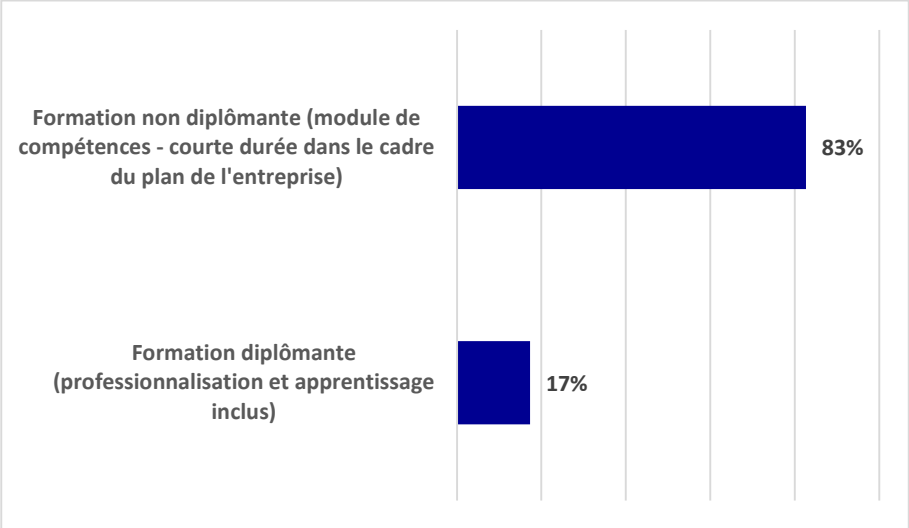


Alors que toutes les grandes les entreprises interrogées soulignent l'importance de la formation dans l'accompagnement des collaborateurs à l'évolution de leur métier et de l'environnement de celui-ci et mettent en place des plans de formation, les PME ont des perceptions différenciées de ce besoin : moins de la moitié envisage de former leurs collaborateurs.

Parmi les entreprises qui envisagent de former, 36% formeront plus de 10 collaborateurs.

« Ne sait pas » sont le fait de répondants de petites entreprises où les décisions ne sont pas prises tardivement en fonction de priorités.

PAR QUEL BIAIS ENVISAGEZ-VOUS DE LES FORMER ?

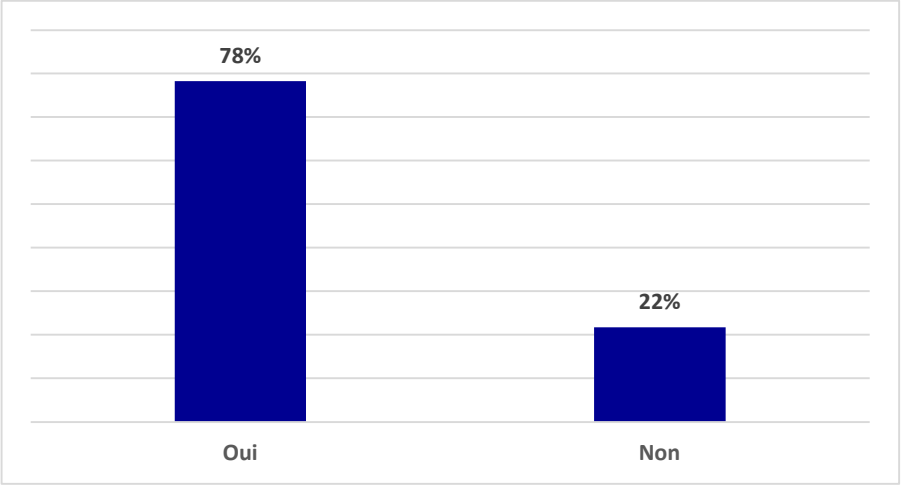


Les formations envisagées sont majoritairement (83%) des formations non diplômantes et de courte durée.

Les formations sous format de e-learning, webinaires sont de plus en plus privilégiées.

2.5. Questions aux seules entreprises numériques

ANTICIPEZ-VOUS UNE EVOLUTION DE VOTRE METIER EN MATIERE DE CYBERSECURITE OU D'IA ?



Les entreprises du numérique questionnées perçoivent une future évolution de leur métier en matière d'IA et/ou cybersécurité (78%).

Alors même que la définition et le contenu de métiers de Data Scientist, Data Analyst, Data Engineer, Data Architect Data Steward sont très récentes, celles-ci sont déjà en voie de redéfinition. Des entreprises anticipent un repositionnement de la fonction du Data Analyst par le transfert de tâches d'analyse vers les métiers opérationnels ainsi la fonction de Data Analyst reposerait sur une expertise technique plus importante.

L'interdépendance de l'IA et de la cybersécurité entraînera des évolutions dans ces métiers. Des experts interrogés dans le cadre de diagnostic font état de l'impact croissant de l'IA sur la cybersécurité et inversement. Les modèles d'IA viennent en appui aux analystes de la sécurité afin de les aider dans la détection de dangers (identification des menaces, accélération des temps de réponse), ce qui implique une évolution du contenu du métier.

Pour faire accompagner les évolutions des métiers de la cybersécurité et l'IA, les entreprises prévoit un plan formation (47%) des réponses affichent la nécessité d'une formation régulière pour y faire face.

3. Cartographie des métiers et des compétences

3.1. La cartographie des métiers

INTELLIGENCE ARTIFICIELLE (IA)

Focus sur 6 métiers dans le cadre de l'analyse des secteurs de l'IA :

Métiers	Descriptifs
Chief Data Officer	Le Chief data Officer est spécialiste de la data et s'occupe de la récolte de toutes ces nouvelles données. Il est responsable du pilotage, du traitement des données, de leur qualité ainsi que de leur administration. La mission première du CDO est de recueillir et d'analyser l'ensemble des données à sa disposition, en créant un environnement permettant à tous les responsables de l'entreprise d'accéder aux informations voulues, rapidement et en toute sécurité. Il doit aussi, selon plusieurs méthodes statistiques bien précises, extraire les données les plus pertinentes nécessaires à la stratégie opérationnelle et organisationnelle de son entreprise. Avant cela, il s'assure de leur fiabilité et de leur cohérence.
Ingénieur Big data	L'ingénieur Big data occupe un rôle essentiel dans la chaîne de traitements de données pour l'entreprise. Il est le premier acteur de l'ensemble du processus de traitement de la donnée, et est donc responsable de toutes les opérations concernant les bases de données. Ses missions consistent à fournir les supports nécessaires aux traitements d'un grand volume de données dans de bonnes conditions. Il est à l'origine de la conception de l'architecture, de la mise en place et de la configuration des clusters ainsi que de l'ajout des algorithmes, des tests techniques et de la qualité des résultats.
Data Analyst	Le data analyst a pour rôle d'exploiter les informations recueillies via les différents canaux pour faciliter la prise de décision des parties prenantes de son entreprise. Au vue du nombre de données aujourd'hui récoltées par les entreprises, le data analyst est devenu un des métiers clés de l'intelligence artificielle et du big data. A partir des données choisies, il détermine le profil d'un client type, ses attentes et ses besoins. Il en résulte des indicateurs pertinents pour influencer la stratégie opérationnelle de l'entreprise. Il est donc au cœur de la base de la stratégie marketing à construire pour la suite, en élaborant des critères de segmentations

Data Scientist	Le data scientist gère, analyse et exploite la masse de données au sein d'une entreprise. Il a une vue globale de l'ensemble des données et les croise de plusieurs sources. Il a pour rôle de comprendre et de modéliser les différentes problématiques métiers ainsi que d'élaborer des modèles prédictifs afin d'anticiper les évolutions de la data et des tendances du secteur d'activité de son entreprise.
Data Miner	Le data Miner fouille l'ensemble des données à sa disposition, les explore pour pouvoir sélectionner les données nécessaires à l'entreprise. On appelle ça le Data mining. Analyste et traducteur des données cachées du marketing, il permet de les rendre intelligibles.
Développeur Big Data	Le développeur Big data maîtrise les langages et codages informatiques, le développeur Big Data intègre les algorithmes aux systèmes de stockage de données Le développeur Big Data est spécialisé dans les langages de script de types Java, Scala ou Python. Il doit développer des applications spécialisées en big data

CYBERSÉCURITÉ

Focus sur 5 métiers ayant la responsabilité de la cybersécurité dans l'entreprise :

Métiers	Descriptifs
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Le Responsable de la Sécurité des Systèmes d'Information (RSSI) assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation. Il définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction de son périmètre.
Data Protection Officer (DPO)	Le Data Protection Officer (DPO) est le référent interne de la politique de protection des données Son rôle est d'instaurer un cadre juridique unifié pour l'ensemble de l'UE, de renforcer les droits des personnes et de responsabiliser tous les acteurs traitant des données
Responsable du SOC (Security Operation Center)	Le Responsable du SOC (Security Operation Center) planifie et organise les opérations quotidiennes du SOC afin d'évaluer le niveau de vulnérabilité et de détecter des activités suspectes ou malveillantes. Il met en place le service de détection des incidents de sécurité. Il valide la bonne exécution des processus de supervision et de gestion des évènements de sécurité et assure un reporting complet et précis des indicateurs clés.
Responsable de projet de sécurité	Le Responsable de projet de sécurité définit, met en œuvre et conduit des projets de déploiement de solutions et d'outils de sécurité, en lien avec les objectifs de sécurité fixés par l'organisation.
Architecte sécurité	L'Architecte sécurité assure que les choix techniques et technologiques des projets IT et métiers respectent les exigences de sécurité de l'organisation. Il constitue l'autorité technique sur les architectures de sécurité, définit les modèles de sécurité et accompagne le développement des architectures de sécurité au sein du SI, en cohérence avec la stratégie IT et les politiques de sécurité de l'organisation.

3.2. La cartographie des compétences

Dans le cadre de l'étude menée pour France2030, et à la suite des audits effectués auprès des entreprises de différents secteur d'activités, la cartographie des compétences présentée des métiers de l'IA et de la cybersécurité s'articule autour de :

- Trois profils suivants :

PROFIL A : EN FORMATION
Le ou la candidat·e en formation qui cherche à développer des compétences dans le domaine et n'ayant pas ou peu de pré-requis.
Il ou Elle va suivre un parcours de formation « complet » lui permettant d'accéder à un socle de compétences « junior »
PROFIL B : EN DEVELOPPEMENT
Le ou la candidat·e a acquis de l'expérience professionnelle dans un secteur ou une organisation et éprouve le désir / la nécessité de développer de nouvelles compétences. Il a besoin de renforcer ses compétences principalement techniques.
PROFIL C : EN RENFORCEMENT
Le ou la candidat·e occupe un poste en lien direct avec le domaine concerné et cherche à développer une ou des compétences spécifiques dans le but de renforcer son activité et répondre à des évolutions du marché.

- 3 blocs de compétences nécessaires et indispensables aux domaines de l'IA et de la cybersécurité.

Bloc 1 : Softskills / Compétences transverses
Ce bloc regroupe l'ensemble des compétences humaines, relationnelles que chaque professionnel doit développer afin de répondre aux exigences internes des organisations.
Tant sur le plan interne que dans le cadre des relations clients et fournisseurs.
Ce champ de compétence apporte une meilleure insertion des profils au sein des organisations, permet de garantir une ouverture d'esprit et une capacité à faire preuve d'autonomie, ce qui est fortement apprécié par les organisations.

Bloc 2 : Compétences techniques
Il convient de distinguer les compétences techniques de l'IA et de celles de la cybersécurité.
Ce bloc donne évidemment le socle essentiel de la pratique métier. Les compétences techniques sont au cœur du quotidien et occupent une place fondamentale dans les formations proposées.

Bloc 3 : Compétences managériales
Par compétences managériales, il faut entendre la capacité à piloter des projets et à être le liant des ressources humaines.
Le management au sens large prend une place importante dans les organisations et ce même si le profil n'occupe pas de position hiérarchique auprès des équipes.

La liste des compétences attendue présentée ne peut être exhaustive à date, car les techniques et les technologies continuent d'évoluer, de ce fait le bloc de compétences techniques demande une veille régulière apportant ainsi un regard sur l'existant, les évolutions possibles et donc les besoins émergents.

INTELLIGENCE ARTIFICIELLE (IA)

L'utilisation de l'IA est diverse et variée et s'implémente de plus en plus dans de nombreuses organisations. Bien que le domaine de l'IA apporte une forme d'approche futuriste dans l'esprit du commun, son utilisation est bien actuelle et s'invite dans notre quotidien sous des formes connues (chatbot, traitement de texte, contrôle d'accès…)

Cartographie des compétences pour les métiers de l'Intelligence Artificielle			
	Profil A : En formation	Profil B : En développement	Profil C : En renforcement
Bloc 1 : Softskills	Anglais Culture Générale La communication interpersonnelle Design thinking Savoir pitcher	Anglais Design thinking Aisance à l'oral Renfoncement des écrits	Anglais Design thinking Prise de parole en public
Bloc 2 : Techniques	Matrices Fonctions à plusieurs variables Loi de probabilités Statistiques Modélisation Langage : Python Langage : R Base de données Sql, NoSql Règlement Général de la Protection des Données (RGPD)	Langage : Python Langage : R Machine Learning Deep Learning Gestion des bases de données (Github) RGPD	Algorithmie Computer Vision – Détection & reconnaissance Traitement automatique des langues (NLP) Apprentissage par renforcement RGPD
Bloc 3 : Management	Méthode AGILE Méthode SCRUM Outils de pilotage (GANTT, PERT) Gestion des conflits Approche financière d'un projet Prendre en compte les situations de handicap	Méthode AGILE Méthode SCRUM Rentabilité d'un projet Prendre en compte les situations de handicap	Savoir donner du feedback Mettre en place des outils de reporting Prendre en compte les situations de handicap

CYBERSÉCURITÉ

La cybersécurité apporte une réponse à la vulnérabilité des systèmes d'informations aussi bien sur les matériels en place que sur les opérateurs. Il est donc important d'arriver à allier une maitrise des environnement informatiques et digitaux des organisations et une sensibilisation des opérateur·trice·s quant aux failles qu'ils·elles représentent.

Liste non exhaustive des métiers correspondants : Cybersecurity Engineer, SOC Analyst, Ingénieur SIEM, Cybersecurity Architect, Chef de projet, Architecte sécurité des SI, DPO

Cartographie des compétences pour les métiers de la cybersécurité			
	PROFIL A : EN FORMATION	***PROFIL B : EN DEVELOPPEMENT***	***PROFIL C : EN RENFORCEMENT***
Bloc 1 : Softskills	Anglais Culture Générale La communication interpersonnelle Design thinking Savoir pitcher	Anglais Design thinking Aisance à l'oral Renfoncement des écrits	Anglais Design thinking Prise de parole en public
Bloc 2 : Techniques	Bases de données Langage : C/C++ Systèmes d'exploitation Architectures & Administration des Systèmes d'informations (SI) Architectures & Administration des réseaux Cryptographie Sécurité des réseaux et terminaux ISO 27001	Gestion des antivirus Penetration testing Sécurité applicative Sécurité deceptive ISO 27001	Antivirus & EDR/XDR Framework AWS, CGP, Azure ISO 27001
Bloc 3 : Management	Méthode AGILE Méthode SCRUM Outils de pilotage (GANTT, PERT) Gestion des conflits Approche financière d'un projet Prendre en compte les situations de handicap	Méthode AGILE Méthode SCRUM Rentabilité d'un projet Prendre en compte les situations de handicap	Management des risques Savoir donner du feedback Mettre en place des outils de reporting Prendre en compte les situations de handicap

3.3. Les parcours universitaires

Les diplômes d'ingénieur, et de Master 2 sont des parcours de formation recherchés en priorité par les entreprises. La pénuries de candidats ayant ce parcours conduit les entreprises à embaucher des profils bac+3 (voire bac+2), sous certaines conditions. Les profils Bac+3, Bac+2 (DUT) doivent avoir de solides bases en cyber sécurité qui doivent être complétées par des formations permettant de monter en compétences.

Partie 2 : L'offre de formation

1. Cartographie des formations et des dispositifs existants et financés dans les Hauts de Seine

1.1. Cartographie des formations

La liste des formations recensées dans ce diagnostic n'est pas exhaustive. Les formations présentées dans cette cartographie sont des formations situées dans les Hauts-de-Seine, ainsi que des formations accessibles pour les personnes résidants ou travaillant dans les Hauts-de-Seine.

La cartographie réalisée identifie 145 formations en Cyber sécurité et 60 formations en IA, tous publics et tous niveau confondus.

L'offre provient essentiellement d'écoles d'ingénieurs et d'universités, mais aussi d'autres organismes de formation généralistes et plus spécialisés.

La répartition géographique des formations en Ile de France est inégale, avec une concentration importante de formations dans le 75 (30% pour la Cyber et 40% pour l'IA). Viennent ensuite les départements du 91 et 92. Le département des Hauts de Seine accueille 25% des formations en cybersécurité et 14% des formations en IA. Il est important de noter que pour le département du 92 il s'agit, pour la majorité, de formations courtes non diplômantes.

Les forces historiques de la recherche scientifique et de la formation en ingénierie implantées dans le département des Hauts de Seine sont l'Université Paris Nanterre (seule université dont le site principal se situe dans le département) et plusieurs écoles d'ingénieurs accrédités par la CTI (IFP School, ESILV, CESI et ISEP).

Ces établissements mènent, au sein de leurs laboratoires, des travaux de recherche mono et pluridisciplinaires en Data Science, Informatique, Information et la communication et, plus récemment en IA et Cyber risques, proposent des formations, essentiellement de niveau bac+5 sur ces mêmes thématiques et aussi intègrent une initiation à l'IA et/ ou à la Cybersécurité, dans leurs formations plus classiques. Ainsi, l'ESILV propose un diplôme d'ingénieur en informatique, spécialisé en sécurité des systèmes et des objets connectés ; l'Université Paris Nanterre propose un CMI en Data Science for Social Sciences et un master MIAGE, parcours Systèmes d'information fiables et intelligence des données, le CESI, un bachelor en Sciences et en Ingénierie spécialisé en Intelligence artificielle et l'IFP School forme les élèves ingénieurs des programmes *Petroleum Geosciences* (PGS) et *Reservoir Geoscience and Engineering* (RGE) aux méthodes de l'IA.

Aux côtés de ces établissements pluridisciplinaires présents de longue date sur le territoire du 92, se sont installés plus récemment des organismes de formation de taille plus réduite, avec une offre de formation plus spécialisée, diplômante ou non, de durée variable, destinée principalement à des étudiants en alternance ou à des salariés comme par exemple de l'IA School, l'ESGI ou bien de H2S ou Guardia Cybersecurity School.

En conclusion, les fonctions occupées à ce jour dans les métiers de l'IA et de la cybersécurité sont occupés par des personnes ayant reçu une formation spécifique et dont les missions ont évolué au cours du temps pour répondre aux besoins spécifiques.

Nous avons montré que dans les profils d'apprenant, le cas du collaborateur qui veut développer ou renforcer ses compétences fait partie des profils types en entreprise.

Voir le tableau des formations en annexe.

1.2. Les dispositifs existants et financés dans les Hauts de Seine

Des financements collectifs tels que :

- Le Marché FOAD (Formation ouverte et/ou à distance) de Pôle emploi :

- Data analyst
- Ingénieur Intelligence Artificielle (IA)
- Data scientist
- Manager en infrastructures et cybersécurité des systèmes d'information
- Responsable de projet cybersécurité et SI

- Le programme Régional IDF E-Learning :

- Technicien cybersécurité - Certification Cisco CCNA Security

- Les POEC (Préparations Opérationnelles à l'Emploi Collective) mises en œuvre à l'initiative de la branche professionnelle.

- AGCC - Analyse et Gouvernance Contre les Cyber-menaces
- Développeur cybersécurité

A noter que les programmations 2023 de ces dispositifs, et d'autres comme celle du Programme Régional Formation pour l'Emploi (PRFE 2022-2026) ne seront disponibles que prochainement.

Des dispositifs de financement en lien avec l'entreprise

- La POEI (Préparation Opérationnelle à l'Emploi Individuelle)
- L'AFPR (Action de Formation Préalable au Recrutement

Des financements individuels

- L'AIRE (Aide individuelle régionale vers l'emploi)
- L'AIF (Aide individuelle à la formation) qui peut également intervenir en cofinancement du CPF si la formation est éligible et si le bénéficiaire a des droits.

2. Les enjeux environnementaux des formations et les axes d'amélioration de leur conception et de leur mise en œuvre

2.1. Les enjeux liés à l'IA

L'IA est porteuse de nombreux espoirs mais également de risques. A ce titre, son encadrement normatif est devenu un enjeu international visant à limiter les dérives et les conséquences potentiellement négatives de son développement et de son utilisation.

Parmi les risques identifiés, l'impact environnemental du développement de l'IA est aujourd'hui au cœur des préoccupations des instances internationales (Nations Unies, Union Européenne, Organisation de coopération et de développement économiques, Conseil de l'Europe…).

A ce titre de nombreuses recommandations ont été émises notamment dans le domaine de la formation aux enjeux de l'IA.

L'intelligence artificielle : un concept englobant

L'IA est loin d'être un concept homogène. Pour preuve le nombre important de définitions dont elle est l'objet.

Initialement définie par Alan Turing ou John MacCarthy comme renvoyant à des « machines pensantes », puis par Marvin Minsky comme étant « la science consistant à faire faire à des machines des choses qui requerraient de l'intelligence si elles étaient faites par des hommes » et nécessitant « des processus mentaux de haut niveau tels que l'apprentissage perceptuel, la mémoire et la pensée critique », la définition de l'IA fait aujourd'hui l'objet de nombreux débats.

L'Union européenne, qui évoque même « les intelligences artificielles », a retenu quant à elle la définition suivante :

« L'IA désigne la possibilité pour une machine de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité. »

Cette définition est aujourd'hui battue en brèche en raison d'une confusion entre l'IA en tant que telle et les systèmes d'intelligences artificielles. La définition de ces derniers, proposée notamment dans le projet d'AI Act et dans les recommandations du Groupe d'Experts de haut niveau est d'ailleurs, est souvent utilisée en lieu et place de celle de l'IA (Commission Européenne, 2018 ; Commission Européenne, 2020a :1; GEHN IA, 2019 :8 ; Commission Européenne, 2020b).

Finalement l'IA est un concept très large englobant les processus et les systèmes et couvrant un large spectre d'outils.

Ce caractère englobant impacte bien évidemment l'évaluation des conséquences que l'IA peut avoir sur l'environnement. Plus la définition est large, plus les risques identifiables sont nombreux.

L'IA et les objectifs de développement durable

Contrairement à la tendance actuelle, il est plus que jamais nécessaire d'adopter une approche holistique couvrant l'ensemble des phases clés du développement des systèmes d'IA, allant du traitement des données aux inférences en passant par l'expérimentation et l'entrainement du système. Cette approche inclue également le cycle de vie des systèmes et ses quatre phases que sont la production, le transport, l'utilisation et le recyclage (Wu et al., 2022 ; Gupta et al., 2021 ; Ligozat et al., 2022). Cette perspective est d'ailleurs reprise par l'Union européenne qui souligne qu'il « faut dûment tenir compte de l'incidence environnementale des systèmes d'IA tout au long de leur cycle de vie et sur l'ensemble de la chaîne d'approvisionnement » (Commission Européenne, 2020b).

La notion de progrès étant souvent associée à l'amélioration de la qualité, la quête de modèles de plus en plus performants a masqué la réalité de l'augmentation des besoins énergétiques et de l'empreinte environnemental liée à la croissance de l'IA. Ainsi, le développement des outils s'est fait au détriment de l'environnement (Wu et al., 2022).

Pour être plus efficace dans la gestion de l'impact environnemental des systèmes d'IA, il est essentiel de les envisager comme des écosystèmes dont chaque dimension doit faire l'objet d'une évaluation. Au-delà de l'empreinte carbone liée à la consommation énergétique opérationnelle de l'IA, celle intégrée aux systèmes devient un élément essentiel à prendre en compte (Wu et al., 2022 ; Ligozat et al. 2022).

Pour gagner en efficacité et rendre la démarche pérenne il faut œuvrer au développement d'un état d'esprit spécifique, un « sustainability mindset » (Wu et al., 2022) au sein des équipes des acteurs de l'IA. Cette attente est conforme aux Objectifs de développement durables (ODD) des Nations Unies, en particulier de l'objectif n° 9 sur l'industrie, l'innovation et les infrastructures (ONU, 2020).

L'Union Européenne est elle-même particulièrement attentive à la dimension environnementale de l'IA et appelle dans l'ensemble de ses travaux au développement de systèmes contribuant au « bien-être sociétal et environnemental » (GEHN IA, 2019).

De plus en plus, l'exigence de respect de l'environnement conditionne le développement des nouveaux outils technologiques. L'IA ne fait pas exception et la demande de systèmes d'IA respectueux de l'environnement et participant de sa durabilité est en voie de devenir la règle. Ainsi, comme le souligne Wu et al. (2022), il est essentiel que les concepteurs et architectes repensent les principes de conceptions des systèmes pour en minimiser l'empreinte environnementale. Il est par ailleurs nécessaire de s'orienter vers de meilleures pratiques en matière de responsabilités liées à l'empreinte carbone des systèmes d'IA (Gupta et al., 2021).

Le paysage normatif

La position française

Dans le respect des normes européennes la France affirme sa volonté d'œuvrer au respect de l'environnement de manière générale et en particulier dans le domaine du développement technologique.

Cette volonté est clairement affirmée dans le rapport Villani (2018) qui souligne que « pour renforcer l'écosystème français et européen de l'IA» il est nécessaire de « concentrer l'effort sur quatre secteurs prioritaires : santé, environnement, transports-mobilités et défense-sécurité ».

Pour la France, au-delà de la réduction de l'impact environnemental de l'IA, il s'agit également de favoriser « les innovations en IA pourront servir à optimiser les consommations d'énergie et le recyclage et à mieux comprendre les effets de l'activité humaine sur l'environnement » (Villani, 2018). Il faut donc penser la soutenabilité écologique de l'IA pour en tirer les bénéfices en limitant son impact sur l'environnement.

Cette politique s'inscrit dans le cadre des ODD ainsi que de l'Accord climat (plus connu sous le nom d'Accord de Paris) de 2015 et du Pacte mondial pour l'environnement adopté en 2018.

La position européenne

L'engagement de l'Union européenne en faveur de l'environnement dépasse largement les frontières des technologies.

Comme l'indique la décision 2022/591 du Parlement européen et du Conseil, l'Union est face à « une occasion unique » de jouer « un rôle moteur en matière de durabilité au niveau mondial » durant les dix prochaines années.

Dès 2019, le Parlement avait déclaré, au travers de la résolution 2019/2930(RSP), « l'état d'urgence climatique et environnementale » et appelé la Commission et les Etats membres à prendre des mesures concrètes.

En décembre 2019, l'Union Européenne avait d'ailleurs présenté son Pacte vert pour l'Europe mis en œuvre en 2021, avec pour objectif d'agir contre la « menace existentielle pour l'Europe et le reste du monde » que représentent le changement climatique et la dégradation de l'environnement.

C'est dans ce cadre général que s'inscrit la politique européenne en matière de développement d'une IA soutenable sur le plan écologique.

Ainsi, le rapport du Groupe d'experts de haut niveau (GEHN IA, 2019), souligne l'importance de la prise en compte des potentielles atteintes à l'environnement naturel dans le développement des systèmes d'IA et fait figurer parmi ses six exigences la durabilité et le respect de l'environnement. Exigence déjà contenue dans le Livre Blanc sur l'IA(Commission Européenne, 2020b), qui par ailleurs concrétise l'articulation entre protection de l'environnement et nouvelles technologies :

« Toutefois, l'empreinte environnementale actuelle du secteur des TIC est estimée à plus de 2 % de l'ensemble des émissions mondiales. La stratégie numérique européenne qui accompagne le présent Livre blanc propose des mesures en faveur de la transformation verte du secteur du numérique. »

Là encore, l'Union européenne envisage la question environnementale sous deux aspects : d'une part la prise en considération de l'impact du développement des systèmes d'IA sur l'environnement, et, d'autre part, le rôle que peut jouer l'IA dans la protection de l'environnement.

Il est donc clair que l'Union Européenne est particulièrement sensible aux problèmes environnementaux découlant de l'IA. En 2021, la Commission présentait d'ailleurs sa « boussole numérique » dans le cadre de La décennie numérique de l'Europe, dans laquelle figurait, parmi ses objectifs, sa volonté d'aller vers « des infrastructures numériques sûres et durables ». Enfin, dans son rapport Façonner l'avenir numérique de l'Europe (Shaping Europe's Digital Future), la Commission appelait à un « changement immédiat de direction vers des solutions plus soutenables, qui seraient économes en ressources et neutres sur le plan climatique » (Commission Européenne, 2020a).

2.2. Les enjeux liés à la cybersécurité

La question de l'énergie est consubstantielle de celle de la sécurité. L'actualité tend à le démontrer, la sécurité de l'approvisionnement énergétique est un facteur essentiel de l'autonomie et de la souveraineté des Etats.

La cybersécurité s'inscrit naturellement dans cette logique consistant à sécuriser les approvisionnements énergétiques pour maintenir en fonction l'ensemble des outils technologiques alimentés par l'électricité. En cela, elle est étroitement liée aux questionnements environnementaux posés par les technologies (Cassota et al., 2019).

Les besoins de sécurité vont bien entendu de pair avec le développement de solutions technologiques et d'infrastructures ayant elles-mêmes un impact sur l'environnement. La consommation des ressources naturelles nécessaires à la fabrication d'infrastructures numériques de plus en plus complexes et sécurisées, n'est évidemment pas sans conséquences sur l'environnement.

Enfin, il est essentiel d'envisager la cybersécurité comme un élément essentiel de la protection de systèmes traitant directement d'activités liées à l'environnement.

La cybersécurité

La relation entre cybersécurité et environnement couvre au moins deux aspects. D'une part, la mise en place de systèmes de sécurité pour faire face au nombre croissant de cyberattaques (WEF, 2022) implique nécessairement un impact environnemental comme vu précédemment.

D'autre part, la cybersécurité peut-être également envisagée comme un outil permettant de limiter ou d'éviter les dommages environnementaux en protégeant les infrastructures critiques (ICs) (Galaz et al., 2021).

Ces structures hautement digitalisées et dépendantes du cyberespace sont particulièrement vulnérables et nécessitent donc une protection accrue. Selon Cassota et al. (2019), l'absence de cadre réglementaire sur la protection des infrastructures critiques pose aujourd'hui problème. Les menace cyber et les risques associés, dont environnementaux, doivent, selon les auteurs, être intégrés dans un cadre réglementaire qui permettrait aux acteurs d'être proactifs sur la question.

Ces risques sont bien entendu d'autant plus importants qu'ils concernent des infrastructures directement liées à l'environnement : installations de production d'énergie, management d'écosystème, urbanisation, gestion de ressources naturelles, systèmes d'accompagnement aux activités agricoles (Galaz et al. 2021). A ce titre la cybersécurité verte (Green Cybersecurity) est aujourd'hui un sujet de préoccupation dans la limite où elle traite de la sécurisation de « processus directement ou indirectement liés à la gestion et à la protection de 'l'environnement » (Sulich et al., 2021).

Pour le Forum Economique Mondial (Sanek & Dolan, 2022), il est évident que la cybersécurité s'inscrit dans les critères environnementaux, sociaux et de gouvernance (ESG) eux-mêmes intégrés dans les exigences de responsabilité sociale des entreprises (RSE), à savoir la contribution des entreprises « à améliorer la société et rendre plus propre l'environnement » (Commission des Communautés Européennes, 2001) ou encore « l'intégration volontaire par les entreprises de préoccupations sociales et environnementales à leurs activités commerciales et leurs relations avec les parties prenantes » (Commission Européenne, 2011).

La pandémie de Covid a contribué à l'accélération de la modernisation et à la digitalisation des ICs gourmandes en données et exigeantes en ressources énergétiques et favorisé l'augmentation des cyberattaques (WEF, 2022). Le besoin de sécurité pour ces infrastructures s'est accru en conséquence (Raimundo et al., 2021). Des systèmes mieux sécurisés présentent l'avantage de faciliter la réduction des impacts environnementaux de la technologie. Les bénéfices associés au développement des ICs, en particulier des infrastructures ICT (Information, Communication and Technology), s'accompagne de risques cyber qu'il est nécessaire d'évaluer et de contrer par des mesures efficaces (Vasiu & Vasiu, 2018). Selon Vasiu & Vasiu, la cybersécurité doit donc être envisagée comme un facteur différenciant par les entreprises de plus en plus dépendantes des technologies. Les potentiels défauts de cybersécurité, considérés comme une menace majeure à court terme (WEF, 2022) et le manque d'investissement en matière de durabilité écologique sont donc deux risques que les entreprises doivent prendre en compte.

Pour Sulich et al. (2021), « la cybersécurité, la régulation des données et la soutenabilité seront des éléments clés du processus de transformation digital des prochaines années ». La protection des ICs dans le domaine des énergies renouvelable est à ce titre illustrative de l'articulation entre cybersécurité et durabilité environnementale (Deloitte, s.d.).

Le stockage des données

L'établissement d'infrastructures efficiente sur le plan énergétique est une préoccupation majeure de l'Union européenne. A ce titre, outre la mesure des risques, le benchmarking doit désormais permettre de mesurer l'efficacité énergétique des centres informatiques.

Comme le souligne la feuille de route adressée par 27 PDG de compagnies européennes à la Commission européenne « les services et infrastructures numériques gênèrent environ 4% des émissions actuelles de gaz carbonique, et cette proportion risque d'augmenter en raison de la tendance exponentielle de la consommation de données » (Collective work, 2021).

Les centres de calcul équipés de techniques économes en énergies représentent, à ce titre, une opportunité dans la ligne de la demande sociétale en matière de pratiques soutenables traduite dans la ODD.

Selon l'Union européenne, les industries numériques représentent 9% de la consommation mondiale d'électricité, avec une croissance de 9% par an (Ferreboeuf, 2019). Dans ce cadre, toute initiative en termes de technologies ou d'infrastructures permettant de réduire cette part est considérée avec intérêt.

Ainsi, l'accroissement du flot de données et de la demande en solutions permettant d'économiser de l'énergie, ont accentuer l'attrait pour les centres de calculs (IEA, 2021) considérés comme des infrastructures clés en ce qu'elles rapprochent les données des utilisateurs et limite donc la consommation énergétique en plus d'assurer la souveraineté des Etats.

Pour autant les performances de ces centres de calcul (computing centers) doivent être contrôlées, notamment en matière de consommation d'énergie et d'émissions de gaz carbonique. Toujours selon la feuille de route (Collective work, 2021), « l'industrie tirerait bénéfice de plateformes de données décarbonées » et « du développement d'indicateurs de performance d'eco-efficience ». Le benchmarking des performances en matière de soutenabilité environnemental devient ici critique.

Désormais les opérateurs de centres de calcul se sont engagés à respecter les exigences émises par le Pacte vert pour l'Europe en termes de réduction des gaz à effet de serre et d'atteinte de la neutralité climatique à l'horizon 2050. Ainsi, il a été convenu que les centres de calcul seraient neutres en 2030 (Kundaliya 2021).

Dans ce cadre, le Partnership for Advanced Computing in Europe (PRACE) s'est engagé à « améliorer l'efficience énergétique des systèmes de calculs (computing systems) et à réduire leur impact environnemental » .

De manière plus générale, la croissance du nombre de données a conduit à une augmentation du besoin en matière d'infrastructures de stockage et de traitement de ces dernières. Cette augmentation s'est évidemment accompagnée d'un accroissement de la demande énergétique et donc de l'impact environnemental des infrastructures dédiées. La sensibilité de l'Union européenne aux questions environnementales explique l'intérêt de l'Union pour les super centres de calcul, moins énergivores et présentant l'avantage d'être implantés au plus près des utilisateurs, ce qui permet également d'assurer la souveraineté de l'Europe et de faciliter la sécurisation des infrastructures et donc des données.

L'ensemble de ces considérations s'inscrit dans un cadre plus large de promotion de pratiques éthiques notamment soulignée par le Groupe d'experts de haut niveau (GEHN IA, 2019) et aux nombres desquelles exigences se trouvent le bien-être sociétal et environnemental, mais également le respect de la vie privée et la gouvernance des données, ou encore la robustesse technique et la sécurité.

En d'autres termes, les questions liées à la sécurité des infrastructures et des données sont étroitement liées aux préoccupations environnementales, le tout étant inclus dans des considérations d'ordre éthique.

2.3. Les enjeux environnementaux des formations et axes d'amélioration

Les enjeux des formations

Les enjeux en matière de formation sont nombreux. Ils concernent à la fois les contenus et les modalités des formations.

C'est notamment ce que souligne le rapport Villani (2018) qui indique que « [l]e développement de l'IA nécessite une transformation des manières de former ainsi que des contenus de formation ». Toujours selon le rapport, la modification des formations doit d'abord concerner celles délivrées aux enseignants eux-mêmes.

Les efforts doivent concerner tous les aspects de la formation qu'elle soit initiale, professionnelle, technique, de haut niveau, auprès des acteurs publics ou privés.

L'enjeu essentiel est ici de former les acteurs présents et futurs de l'IA aux questions environnementales soulevées par ces technologies. La sensibilisation précoce aux enjeux environnementaux est fondamentale à la compréhension des problématiques liées aux technologies telles que l'IA. Avant même de s'aventurer dans les méandres de l'articulation entre IA et environnement, il est essentiel que les futurs acteurs de l'IA disposent de connaissances suffisantes à l'appréhension de ces problématiques. La compréhension générale de enjeux environnementaux est donc un prérequis pour aborder ces sujets en contexte spécifique tel que celui de l'IA.

La formation doit être accrue quantitativement (multiplié par trois selon le rapport Villani), mais surtout qualitativement en favorisant le développement de l'esprit critique et d'une véritable culture du questionnement constructif.

Ces contenus doivent par ailleurs couvrir un vaste champ de connaissances non limités aux aspects techniques de l'IA. Ainsi, de plus en plus d'institut de formation propose des contenus couvrant les aspects géopolitiques et éthiques du développement de l'IA. Il est par ailleurs évident que, comme l'indique le rapport Villani, les besoins de formation en IA doivent également inclure un renforcement des enseignements en mathématique et en informatique. Seule la capacité à articuler sciences dures et sciences humaines est à même d'offrir les outils nécessaires à une appréhension correcte de la complexité des questions liées à l'IA.

La conception, le développement, et l'utilisation de systèmes d'IA respectueux de l'environnement nécessite une prise de conscience globale que seule une formation large et complète peut alimenter.

Les axes d'amélioration

Plusieurs axes sont proposés par le rapport Villani (2018).

Outre l'accroissement du nombre de personnes formées à l'IA, il est aujourd'hui nécessaire de créer de nouveaux cursus transverses traitant des aspects techniques et non-techniques de l'IA. Dans ce cadre les questions environnementales méritent une place particulière.

Comme le souligne le rapport Villani, « [l]a formation de spécialistes hybrides, qui maîtrisent des compétences autres en plus des compétences en IA, est ainsi nécessaire ».

Il est par ailleurs, recommandé de créer des formations plus généralistes au profit de personnes en formation ou en activité professionnelle. Ces formations doivent s'adresser tant aux acteurs publics que privés.

Elles doivent par ailleurs accentuer la dimension éthique afin d'accompagner les acteurs de l'IA dans leurs réflexions sur les enjeux de cette technologie, mais aussi sur leur rôle et responsabilité. La formation à l'éthique est par ailleurs essentielle à une appréhension correcte des questions environnementales et doit être intégrée dans les cursus de formation des ingénieurs. Comme le souligne le rapport Villani « pour parvenir à former des professionnels plus responsables, l'enseignement de l'éthique et plus largement des sciences sociales doit irriguer l'ensemble de la formation des ingénieurs et informaticiens. »

De manière générale, il est nécessaire de créer de véritable formations hybrides dans lesquelles les sciences humaines ne seraient plus considérées comme des apports marginaux ou des modules d'ouverture. Les sciences humaines doivent trouver une place plus importante dans les formations des ingénieurs de manière à développer une capacité d'analyse des enjeux, dont ceux liés à l'environnement, plus précise et plus globale.

3. Hypothèses des évolutions des besoins en formation à partir des travaux de recherche

3.1. L'évolution des domaines disciplinaires et des questions de recherche en lien avec l'IA et la cybersécurité

Intelligence Artificielle

Les premières recherches en IA ont été menées dans les champs disciplinaires des neurosciences, de la psychologie, puis de l'informatique, de la statistique et de l'ingénierie. Leur objectif était le développement d'algorithmes et de systèmes conduisant à des raisonnements et à des actions automatisées et optimisées, visant à remplacer et améliorer des activités généralement attribuées à l'intelligence humaine. Les questions liées à l'optimisation de la collecte, du stockage et du traitement des très grands volumes de données de différents formats (numériques, textuelles, images, …) indispensables pour la mise en œuvre des algorithmes de l'IA, ainsi que les questions portant sur l'amélioration des algorithmes d'apprentissage statistique ont été et restent aujourd'hui au cœur des programmes de la recherche fondamentale en IA.

L'élargissement des applications des techniques de l'IA à de très nombreux secteurs d'activité a suscité des questions nouvelles et stimulé des recherches mono et pluridisciplinaires au-delà du domaine des sciences et techniques, en sciences juridiques, économiques et de gestion, en sciences humaines, sociales environnementales et en santé. En 2018, le rapport de la mission parlementaire présidée par C. Villani identifie 4 domaines pour de futures de futures applications de l'IA : la santé, les transports, l'environnement et la défense.

Pour les chercheurs et les praticiens du droit, l'IA a aussi ouvert de nouvelles perspectives et posé de nouvelles questions. L'utilisation indispensable pour l'apprentissage de très grandes quantités de données, souvent personnelles, a notamment alimenté des recherches en droit du numérique liées à la protection des données personnelles, au régime juridique de la donnée et à l'éthique des algorithmes.

L'IA peut aussi être mise au profit de la justice à des niveaux différents. Des bases de données permettent d'alléger le temps de recherche de lois ou de jurisprudences auquel étaient confrontés tout autant les professionnels du droit que les justiciables. Pour aller plus loin, les algorithmes de justice prédictive pourraient servir à uniformiser les prises de décisions des juges, notamment en matière de montants d'indemnisation. L'analyse a posteriori des décisions de justice permettrait de garder une cohérence entre les décisions prises au fil du temps en fonction des différentes caractéristiques soumises aux algorithmes. Les travaux scientifiques les plus récents sur le sujet sont publiés notamment dans la revue scientifique de l'éditeur Springer, intitulée *Artificial Intelligence and Law* (https://www.springer.com/journal/10506) et un article de Villata et al. (2022) dans cette même revue retrace l'historique des applications des techniques de l'IA et de la gestion des données massives dans le domaine juridiques en ces 30 dernières années.

Plus généralement, dans de nombreux domaines, dans lesquels de grandes quantités de données sont collectées et stockées les techniques de l'IA sont de plus en plus mobilisées pour répondre à des questions de recherche anciennes ou nouvelles et aussi pour optimiser la prise de décision. Les travaux de ce type regroupent des spécialistes des disciplines fondamentales de l'IA (informatique et statistique) avec des spécialistes de la discipline dans laquelle la question de recherche est posée. De plus en plus de chercheurs en sciences humaines et sociales sont ainsi impliquées dans des recherches mobilisant les technologies de l'IA. Dans le domaine de l'analyse de l'innovation par exemple, des travaux récents proposent d'appliquer des méthodes de l'IA en utilisant les données numériques et textuelles contenues dans les registres officiels des offices des brevets pour : (i) identifier l'émergence d'innovations au sein d'un domaine technologique, (ii) positionner une entreprise et évaluer sa contribution et son importance au sein du sentier technologique caractérisant une technologie précise ;(iii) Evaluer la valeur du portefeuille de brevets d'une entreprise et sa contribution à l'écart entre la valeur économique de l'entreprise et sa valeur comptable ; (iv) identifier l'émergence d'innovations de rupture ou de nouveaux acteurs au sein d'un domaine technologique précis. Ce type de travaux nécessite la participation, aux côtés des spécialistes en IA (informaticiens et statisticiens), de chercheurs en économie d'entreprise et de l'innovation.

De même, les projets de conception de Smart cities, d'optimisation de la gestion des ressources naturelles et du trafic font l'objet de travaux regroupant des chercheurs en algorithmique et Data sciences avec des chercheurs en géographie et aménagement.

Concernant la recherche plus fondamentale en IA, les tendances les plus récentes s'orientent vers une mobilisation des avancées en neurosciences pour améliorer la performance des algorithmes d'apprentissage.

Cybersécurité

Le site gouvernemental sur la prévention des risques majeurs (https://www.gouvernement.fr/risques/) définit une cyber-attaque comme une atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les « smartphones » ou les tablettes. Plus récemment, s'y sont ajoutés les objets connectés, les véhicules autonomes et les systèmes de conduite industriels.

Il existe quatre types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

Une stratégie nationale pour la cybersécurité a été annoncée par le Président de la République en janvier 2021 visant à soutenir et stimuler la filière des industries de sécurité et à créer un « écosystème de la cybersécurité ». Le pilotage du programme de recherche associé à cette stratégie qui vise à développer des solutions souveraines et de faire émerger des technologies de ruptures bénéficiant à l'ensemble des acteurs socio-économiques face aux cybermenaces a été confié CNRS, au CEA et à l'Inria. Les recherches fondamentales et appliquées des différents instituts et laboratoires de ces organismes couvrent un large spectre de domaines de recherches en lien avec la cybersécurité allant de la cryptologie à la protection des données en passant par la détection d'intrusions et la protection contre les logiciels malveillants.

Les avancées de la recherche en IA nourrissent les travaux sur les réponses optimales face aux menaces de cyber attaques. En effet, la cyberdéfense et la cybersécurité évoluent dans un contexte de surabondance informationnelle et de complexification constante des menaces. Les modes opératoires des attaquants étant de plus en plus difficilement détectables par la seule capacité d'analyse des opérateurs humains du fait des temps longs et de la subtilité des signaux d'attaque produits, les techniques d'apprentissages mises en œuvre par l'IA permettent d'imaginer des outils plus performants de détection, de protection et de réponses à des attaques nouvelles.

Les cyber attaques font par ailleurs partie des risques émergents auxquels sont confrontés les économies et à ce titre, elles font l'objet de recherches portant sur leur perception et sur les solutions possibles pour leur gestion, notamment par des mécanismes assurantiels. Ces recherches sont menées en sciences actuarielles et en économie comportementale. Enfin, risque cyber ayant comme origine des comportements criminels, les sciences juridiques sont mobilisées dans les recherches sur les évolutions législatives.

La multiplicité des domaines disciplinaires impliqués dans les recherches sur la cyber sécurité et des compétences nécessaires pour protéger les entités contre les cyberattaques appellent une réflexion au sein des entreprises sur les arbitrages entre ressources à mobiliser en interne et externalisation pour les différentes dimensions de la protection à mettre en place.

Sur le territoire des Hauts de Seine, concernant l'IA, en plus des travaux de recherche menées dans les laboratoires des écoles d'ingénieurs, des recherches davantage pluridisciplinaires sont menées à l'Université Paris Nanterre, université à dominante SHS. Ces recherches sont menées principalement dans deux UMR du CNRS : EconomiX (laboratoire de recherche en sciences économiques) et MODALIX (laboratoire de mathématiques axé sur la modélisation aléatoire et couvrant un large spectre dans le champ des probabilités et des statistiques, et de leurs interactions notamment avec l'analyse.) et dans un laboratoire de recherches en droit, le CRDP, partenaire du Centre Internet et Société, groupement de recherche du CNRS.

Concernant les recherches sur les Cyber risques et la cybersécurité dans les Hauts de Seine, aux côtés des travaux menés par dans les laboratoires des écoles d'ingénieur et de l'université, il est important de souligner le rôle important joué par le Campus Cyber, dans sa mission d'organisation de manifestations scientifiques et de rencontres entre les acteurs de la recherche et les entreprises et acteurs du territoire.

3.2. Les hypothèses d'évolution des besoins de formations

On constate un élargissement du spectre des disciplines :

- qui sont impliquées dans la recherche fondamentale en IA et cybersécurité. Aux côtés des mathématiques, de la statistique et de l'informatique, les disciplines juridiques (notamment pour les aspects éthiques et réglementaires de l'IA et de la cybersécurité) et les sciences du comportement (notamment pour les aspects perception et tolérance au risque) sont de plus en plus présentes.

- qui mobilisent les méthodes de l'IA pour répondre à des questions de recherche nouvelles, et aussi pour proposer des réponses plus efficaces à des questions de recherches plus anciennes. Comme évoqué ci-dessus, en plus des disciplines du domaine Sciences, Technologie, Santé, à l'origine du développement de l'IA, et qui très tôt ont commencé à utiliser ses avancées dans leurs travaux, les disciplines du domaine Droit, Economie Gestion, ainsi que certaines disciplines du domaine Sciences Humaines et Sociales et même Arts, Lettres et Langues mobilisent de plus en plus les outils IA dans leurs travaux de recherche.

Ce constat peut avoir deux types d'implications pour les besoins de formation.

- D'abord concernant la formation des chercheurs, il plaide en faveur d'une part de l'intégration d'une initiation à l'IA dans les modules de formation doctorale au-delà des écoles doctorales des disciplines Scientifiques et techniques (des cours gratuits sont disponibles en ligne, à titre d'exemple https://openclassrooms.com/fr/courses/6417031-objectif-ia-initiez-vous-a-lintelligence-artificielle ou https://www.elementsofai.com/) et d'autre part, de l'organisation de séminaires de recherche pluridisciplinaires visant à stimuler les collaborations scientifiques entre spécialistes de l'IA et chercheurs d'autres disciplines.

- ensuite concernant la formation des publics plus larges. Comme le souligne C. Villani dans son rapport : « La recherche française est au premier plan mondial pour ce qui concerne ses chercheurs en mathématiques et en intelligence artificielle, **mais elle a du mal à transformer ses avancées scientifiques en applications industrielles et économiques »**.

L'intégration des avancées de la recherche en IA et cybersécurité dans l'entreprise, surtout lorsqu'il s'agit de domaines d'activité ne nécessitant pas de compétences scientifiques et techniques, requiert une augmentation du nombre de salariés formés, ou du moins sensibilisés, aux techniques de l'IA et aux problématiques de la cybersécurité.

Cette formation peut se faire par deux voies : la formation initiale et la formation continue.

Pour le moment, la formation continue semble privilégiée car elle permet de répondre au besoin de former rapidement un grand nombre de collaborateurs. Cependant, à moyen et à plus long terme, les avancées rapides des recherches dans les domaines de l'IA et les menaces accrues en termes de cyberattaques plaident en faveur d'une intégration de ces sujets dans la formation initiale aussi bien sous forme d'initiation dès la licence (par exemple dans le cadre des enseignements transversaux de type préparation à la certification PIX) pour les formations de tous les domaines disciplinaires que sous la forme de doubles cursus de Licence ou de Master (comme les doubles licences Economie-Mathématiques, Informatique- Sciences de gestion ou IA-Sciences des organisations) qui permettraient l'arrivée en entreprises de cadres susceptibles de participer très rapidement à l'intégration des techniques IA et des process de cybersécurité.

Concernant le domaine de l'IA, ces évolutions et les besoins de formation qui en découlent ont bien été identifiés lors de l'élaboration de **La stratégie nationale pour l'IA** (https://www.intelligence-artificielle.gouv.fr/fr/strategie-nationale/la-strategie-nationale-pour-l-ia) dont l'un des objectifs **(« Attirer les talents et la meilleure expertise en intelligence artificielle ») se décline en trois volets , combinant le développement de la recherche académique, l'amélioration des liens entre industrie et recherche publique et l'augmentation (doublement) du nombre d'étudiants formés à l'IA.**

Concernant plus précisément la formation, le Président de la République a fixé, en octobre 2019, les objectifs principaux suivants pour l'Enseignement supérieur :

- Doublement des promotions annuelles en masters en IA pour accroitre le potentiel haut niveau en IA et en double expertise ;

- Développement d'un niveau de formation intermédiaire en IA (licence professionnelle par exemple) ;

- Création d'un label permettant de repérer les formations en IA dans l'enseignement supérieur.

Le besoin d'experts en IA avec une double compétence pour le développement d'applications IA adaptées aux différents secteurs de l'économie a aussi été bien identifié, les champs identifiés étant : IA et santé, IA et environnement, A et éducation...) .

Les évolutions récentes aussi bien des travaux de recherche identifiés que du développement de l'IA dans les différents secteurs de l'économie plaident aussi de plus en plus en faveur du développement d'une double compétence IA – Droit, IA-Sciences du comportement et aussi IA- philosophie pour la prise en charge des dimensions éthiques, juridiques et comportementales.

En parallèle, l'augmentation du nombre de thèses financées prévues dans le cadre du volet recherche de la Stratégie nationale a pour objectif la promotion de la recherche fondamentale et appliquée sur les thématiques de l'IA, avec la perspective, pour un certain nombre de docteurs, de s'orienter vers une carrière non académique, dans le secteur privé, et répondre ainsi au besoin de grandes entreprises de très haut niveau de qualification pour le développement de recherches en interne sur les thématiques de l'IA.

Concernant la Cybersécurité**, la Stratégie nationale d'accélération pour la cybersécurité lancée en 2021** (https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite#), met aussi fortement l'accent sur la nécessité d'augmenter de façon significative le nombre de personnes formées à tous les niveaux de bac+2 à bac+8 en proposant une offre de formation en cohérence avec les avancées technologiques du secteur. Comme dans le domaine de l'IA, la recherche sur les thématiques liées aux cyber risques et à la cybersécurité sera soutenue par le financement de 100 thèses.

Les évolutions des travaux de recherches semblent, comme pour l'IA, plaider aussi, dans ce domaine, en faveur de la nécessité de proposer des formations permettant l'acquisition d'une double compétence : Cyber – Droit, Cyber-Sciences du comportement, Cyber-Actuariat pour répondre aux futurs besoins de compétences des entreprises.

4. Les meilleures pratiques européennes et internationales

Il existe plusieurs classements des meilleures pratiques internationales en matière de cybersécurité, ils ont été établis par des entreprises ou instituts tels que le Global Cybersecurity Index (GCI)[9] et le classement UiPathEn ce qui concerne l'IA, le rapport Roland Berger[10] fait aussi état d'un classement des pays pionniers du secteur.

Depuis deux décennies, de nombreuses initiatives ont été développées en France pour d'une part sensibiliser le plus grand nombre aux enjeux de la cybersécurité et de l'IA d'autre part conforter, au plan international, l'excellence d'établissements de formation et de recherche de ces deux disciplines. Elles ont été renforcées dans le cadre des stratégies nationales pour l'intelligence artificielle et la cybersécurité.

Les formations reconnues comme les meilleures au monde dans le domaine de la cybersécurité et de l'IA se trouvent principalement aux Etats-Unis, en Israël et en Europe dont la France. Le crédit dont bénéficient ces formations leur permet d'attirer toujours plus de candidats et d'accroître leur renommée à l'échelle internationale. Ces formations présentent des éléments communs :

- Les diplômes sont le plus souvent rattachés à un département d'études ou une chaire : Informatique.
- Les cursus sont pluri ou interdisciplinaires. Ils sont composés de majeures telles que réseaux et télécom, génie électrique, génie informatique, génie industriel, génie climatique, Big data et machine learning et de mineures (modules complémentaires) technologiques axés sur des secteurs d'activités (santé, industrie, robotique) mais aussi les sciences humaines.
- Une approche R&D dans la formation

Les formations sont assez semblables, les seuls éléments du cursus ne permettent pas de leur donner une valeur discriminante. C'est l'environnement offert, en complément, de la formation qui leur permet de se démarquer. Parmi les formations les plus plébiscitées et reconnues, nombre sont celles qui mobilisent un corps d'enseignants-chercheurs dans un cadre international et qui valorisent les cas pratiques et les simulations.

Sensibilisation du plus grand nombre

Pour responsabiliser l'ensemble de la société américaine aux enjeux liés à la cybersécurité, le Département de la Sécurité intérieure des États-Unis, en partenariat avec l'Alliance américaine pour la cybersécurité a décrété à partir de 2003 le mois d'octobre comme celui de la sensibilisation aux problématiques cyber.[11]

Depuis 2012, le mois d'octobre est également le Mois européen de la Cybersécurité. La France a décliné sous cette campagne de sensibilisation sous le nom de *Cybermoi/s*. Parmi les évènements de ce mois : Le *Challenge européen de Cybersécurité*, compétition de hackers éthiques âgés de 14 à 25 ans et le *France Cybersecurity Challenge* pour sélectionner les joueurs français.

La pluridisciplinarité des formations

La frontière entre l'IA et la cybersécurité est fine. Aussi, ces formations coexistent tout en offrant un tronc commun permettant aux étudiants avoir une compréhension globale des problématiques qui en découlent. Cette pluridisciplinarité permet d'aller au-delà du simple enseignement technologique. Cette approche est privilégiée par les établissements israéliens : Le National Cyber Bureau (NCB) israélien dont l'objectif est d'améliorer l'éducation dans les sciences numériques. De nombreux experts des sciences humaines interviennent dans les formations d'enseignement technologique.12. La pluridisciplinarité permet également de mieux s'adapter aux évolutions de la société et à ses futures attentes. Ces doubles parcours sont recherchés par les entreprises.

[9]https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/
[10]https://fr.statista.com/infographie/14370/les-pays-pionniers-de-lintelligence-artificielle/
[11]https://staysafeonline.org/events-programs/
[12]https://www.ifri.org/sites/default/files/atoms/files/noel_cyberpuissance_israel_nov2020.pdf

Cette pluridisciplinarité est fortement en œuvre en France. HEC Paris et l'Ecole polytechnique lancent, en septembre 2023, le double diplôme Data et Finance. Les écoles de management ont intégré l'IA dans leur cursus, elles sont nombreuses à proposer des masters ou des masters of science intégrant l'IA comme majeure, deux exemples : MSc « Intelligence artificielle au service de la transformation des entreprises » proposé par Skema Business School en partenariat avec l'école d'ingénieurs en informatiques et en numérique l'ESIEA, MSc « Science des données et stratégie » à l'EM Lyon business school.

L'Ecole des hautes études en sciences sociales (EHESS) a un programme de recherche interdisciplinaire (2019-2023) « Intelligence artificielle et sciences sociales ».

Les facultés de médecine et de santé [13]ont mis en place des diplômes universitaires (DU) traitant de l'IA dans les champs de la médecine et de la santé.

Les universités et les écoles proposent des formations diplômantes de cybersécurité appliquée à des activités ou secteurs économiques tels que supply chain, santé, sûreté (niveau bac+5).

Développer une approche R&D dans la formation

La recherche joue un rôle central dans les formations. Elle fait le pont entre les enseignements, l'innovation et le développement de solutions innovantes sur le terrain. Les laboratoires de recherches sont des lieux qui rassemblent le plus souvent des acteurs du privé et publics autour des mêmes problématiques.

Il existe de très nombreux exemples, à travers le monde, de collaborations universités/ entreprises / agences publiques ou gouvernementales : Cyber NYC de New-York[14], le Digital Hub Cybersecurity de Darmstadt[15], le « Bavarian IT security and safety cluster »[16], le Cyber Spark de Beer Sheva.[17] Le National Cybersecurity Center of Excellence (NCCoE), aux Etats-Unis, constitue une plateforme de collaboration où les industriels, les agences gouvernementales et les institutions académiques travaillent ensemble sur les enjeux de cybersécurité les plus importants pour les entreprises. Ce partenariat public-privé favorise l'élaboration de solutions pratiques en cybersécurité[18].

Dans le domaine de l'intelligence artificielle, la recherche opérationnelle largement pratiquée dans les universités canadiennes permet de tenir compte des développements les plus récents de l'IA et de l'apprentissage profond.

En France, à La Défense, Campus cyber rassemble en un même lieu dédié à la cybersécurité, les grands groupes, les PME, les organismes d'Etat, des établissements de formation avec parmi ces axes développer des synergies entre acteurs publics/privés, rapprocher la recherche et l'industrie.

Parmi les meilleures initiatives internationales : l'institut DATAIA Paris-Saclay qui fédère et structure des expertises, issues de laboratoires et centres de recherche reconnus internationalement, couvrant un large spectre de disciplines (mathématique, informatique, physique, sciences de la vie, sciences humaines, économie et gestion). Il travaille en lien avec des entreprises industrielles partenaires.

[13] Parmi lesquelles les universités de Bourgogne, de Lille et de Paris Cité

[14]https://cyber-nyc.com/

[15]https://digitalhub-cybersecurity.com/ueber-uns/

[16]https://www.cybersecurityintelligence.com/bavarian-it-security-cluster-4349.html

[17]https://portail-ie.fr/analysis/2370/du-cyber-spark-israelien-au-cyber-campus-francais-entre-inspiration-et-collaboration-internationale

[18]https://www.nist.gov/itl/applied-cybersecurity/national-cybersecurity-center-excellence-nccoe

En milieu scolaire et universitaire

La formation des professeurs

Le National Integrated Cyber Education Research Center (NICERC), aux États-Unis, offre aux enseignants un programme de formation gratuit afin qu'ils intègrent des concepts de cybersécurité dans leurs cours. Il peut également s'agir pour eux d'une opportunité de développement professionnel[19].

Sensibilisation des scolaires aux thèmes de la cybersécurité et de l'Intelligence artificielle

L'Institut national espagnol de la cybersécurité (INCIBE) organise des « Espaces sur la cybersécurité » où des cours techniques et pratiques sont proposés à des classes de lycéens afin d'encourager les jeunes à s'intéresser à la cybersécurité.

Le lien avec le milieu professionnel / Apprentissage

Des établissements d'enseignement ont intégré dans leurs formations une dimension de professionnalisation. A Singapour, l'AI Apprenticeship Program offre une formation pratique grâce aux partenariats avec les employeurs qui permettent aux étudiants de travailler sur de véritables projets d'intelligence artificielle[20].

En Allemagne et en Corée du Sud, des programmes similaires existent et sont couplés avec des conférences.

Le DHS et la NSA sont les sponsors de centaines de « colleges » et d'Universités américaines. Ils labellisent certains établissements « Centres d'excellence académique ». Ces derniers collaborent généralement avec un ensemble d'Universités mais aussi avec des entreprises privées et le gouvernement américain.[21]

La gamification

La gamification apporte un caractère ludique aux formations et facilite l'apprentissage. C'est ainsi que certaines formations ou évènements sont adossées à des institutions de référence. National Cybersecurity Centre (NCSC), au Royaume-Uni, organise le CyberFirst Girls Competition pour inciter les jeunes filles à s'engager sur ces sujets.

Le National Cyber Bureau israélien organise des compétitions « hackathon » afin de repérer des jeunes talents.[22] Hessian Israeli Partenership Accelerator for Cybersecurity (HIPA) est un forum israélo-germanique où des étudiants sont constitués en équipes pour résoudre des problèmes en cybersécurité.23

[19]https://cyber.org/about-us

[20]https://www.nus.edu.sg/cfg/events/513

[21]https://www.cybersecurityeducationguides.org/dhs-and-nsa-cae-cd-designated-schools-by-state/

[22]https://ncb.cyberchallenge.in/

[23]https://www.sit.fraunhofer.de/en/news/latest/press-releases/details/news-article/show/start-fuer-ersten-deutsch-israelischen-cybersicherheits-accelerator/

Les formations de courte durée

L'OEA (Organisation des états américains) et l'Institut National Espagnol de Cybersécurité (INCIBE) organisent des « bootcamps » d'été en cybersécurité : programme de deux semaines rassemblant des étudiants du monde entier (techniciens, responsables de l'application des lois cyber etc.).[24]

En France, des actions de sensibilisation et de formation à l'IA et à la cybersécurité en milieu scolaire tant en direction des enseignants et cadres que des élèves ont été développées, notamment dans le cadre des stratégies nationales pour l'intelligence artificielle et la cybersécurité.

Le volet « Eduquer à l'intelligence artificielle » de la Stratégie nationale pour l'intelligence artificielle vise à acculturer et former à un usage raisonné de l'IA les élèves, leurs parents, les enseignants. Parmi les actions clés de ce plan : 1) des modules sur l'IA pour accompagner les enseignants d'informatique et des sensibilisations – 2) la création de parcours IA dans les académies, en lien avec les collectivités, avec l'installation du premier campus d'excellence de l'intelligence artificielle au lycée Paul-Valéry (Paris 12e).

L'ANSSI en partenariat avec le ministère de l'Education nationale, de la Jeunesse et des Sports (MENJS) a lancé une expérimentation de sensibilisation et de formation des élèves et enseignants à la cybersécurité par la création de jeux CyberEnJeux. Les résultats positifs de cette expérimentation permettront une large diffusion prochainement d'une nouvelle version de CyberEnjeux après quelques améliorations. Le MENJS organise, dans le cadre de Campus Cyber, des formations pour les enseignants sur les sujets de cybersécurité liés au contenu des BTS SIO et SN.

Des summer school (programme une semaine, le plus souvent) dédiées à l'IA[25] et à la cybersécurité[26] sont organisées par les écoles et les universités, tous les ans.

Un très grand nombre de cursus en cybersécurité et en IA intègrent des temps de professionnalisation en entreprises.

En milieu professionnel

L'OEA organise aussi avec l'université internationale de Floride deux jours de certification intensive en leadership et cybersécurité.

[24] https://www.incibe.es/summer-bootcamp

[25] CentraleSupélec Summer School dédiée à l'intelligence artificielle

[26] Université de Lorraine Summer School Cyber in Nancy

Partie 3 : Accompagner les évolutions professionnelles et l'accès aux métiers de la cybersécurité et de l'intelligence artificielle d'un large public

1. Synthèse de l'adéquation entre l'offre de formation et les besoins des entreprises en termes d'emploi et de compétences.

1.1. Offre de formation :

Une offre de formation riche d'un point de vue quantitatif en Ile de France : 145 formations identifiées en Cyber sécurité et 60 formations en IA.

Cette offre de formation qui s'est surtout développée ces 5 dernières années, notamment, pour l'IA, sous l'impulsion de la Stratégie nationale pour l'intelligence artificielle, et s'adresse à tous les publics (étudiants, salariés, demandeurs d'emploi), avec des formats et des durées très variées: formations diplômantes, formations certifiantes, ou non certifiantes dont les durées varient de quelques semaines (pour des formations courtes non certifiantes) à 2 ans pour des formations qui délivrent le diplôme de Master.

L'offre provient essentiellement d'écoles d'ingénieurs et d'universités, mais aussi d'autres organismes de formation généralistes et plus spécialisés.

Les tarifs des formations sont très variables et atteignent souvent des niveaux très élevés.

Concernant le niveau visé par les formations, il est principalement de Bac+5 pour les formatons en IA et beaucoup plus diversifié, de Bac +1 à Bac+5 pour la Cybersécurité.

La répartition géographique des formations en Ile de France est inégale, avec une concentration importante de formations dans le 75 (30% pour la Cyber et 40% pour l'IA). Viennent ensuite les départements du 91 et 92. Le département des Hauts de Seine accueille 25% des formations en Cybersécurité et 14% des formations en IA. Il est à noter que ces pourcentages sont basés sur le nombre de formations et non sur le nombre de personnes formées).

Important : L'offre de formation du département des Hauts-de-Seine est majoritairement composée de formations courtes non diplômantes.

1.2. Besoins des entreprises en termes d'emplois et de compétences

Les études menées dans le cadre du diagnostic, mobilisant différentes méthodes de recueil de données (enquête par questionnaire administré par téléphone et en ligne, entretiens semi directifs et focus groups) ont permis de répertorier plusieurs éléments concernant les pratiques, et les besoins de sensibilisation et de compétences en matière de cybersécurité et d'IA des entreprises des Hauts de Seine.

En cohérence avec des analyses précédemment menées, des différences importantes aussi bien en matière d'intégration de l'IA et de la cybersécurité dans l'entreprise qu'en termes de besoins de compétences apparaissent en fonction de la taille de l'entreprise.

Trois catégories d'entreprises ont été distinguées dans l'étude en fonction de la taille : TPE et PME de moins de 20 salariés, entreprises de plus de 20 salariés et Très Grandes Entreprises (TGE) du CAC40.

1. Pour les TPE,
   Le besoin de compétences en cybersécurité et en traitement des données, et en IA ne semble pas encore bien perçu.

2. Pour les entreprises de plus de 20 salariés

Des besoins de compétences plus importants en cybersécurité qu'en IA :

- Cybersécurité : 70% des entreprises interrogées ont investi dans la cybersécurité, 50% d'entre elles expriment des besoins en montée en compétences de leurs équipes et 40%, un besoin de compétences nouvelles

- IA : 20 % des entreprises interrogées ont recours à des applications faisant appel à l'IA et 30% d'entre elles expriment des besoins en montée en compétences de leurs équipes

Concernant l'acquisition de nouvelles compétences, 40% des entreprises envisagent le recrutement de nouveaux collaborateurs (en CDD ou CDI) et 21% envisagent des recrutements en apprentissage.

3. Pour les TGE

Un stade de maturité très avancé dans le développement de la cybersécurité et aussi de l'usage de l'IA et une présence en interne d'équipes dédiées à ces deux thématiques.

Les besoins exprimés portent d'une part sur des profils techniques très pointus pour lesquels le marché est très concurrentiel, avec des salaires très élevés et un fort turnover, et aussi pour des compétences complémentaires en matière éthique et juridique.

1.3. Evolutions anticipées des besoins en formation à partir des travaux de recherche

La principale conclusion des analyses des travaux de recherche porte sur l'élargissement du spectre des disciplines qui sont d'une part, impliquées dans la recherche fondamentale en IA et cybersécurité et d'autre part, qui mobilisent les méthodes de l'IA pour répondre à des questions de recherche nouvelles, et aussi pour proposer des réponses plus efficaces à des questions de recherches plus anciennes. Ce constat peut avoir des implications d'une part pour la formation des chercheurs, et d'autre part pour la formation des publics au-delà des domaines scientifiques et techniques.

2. Macro plan d'actions pour accompagner les évolutions de l'emploi et des compétences

Les résultats de notre étude révèlent que le nombre de formations en IA et Cybersécurité a considérablement augmenté ces dernières années et s'est enrichi aussi bien en matière de contenus que de niveaux proposés. Cependant, les objectifs ambitieux fixés en matière d'offre de formation et de nombre de personnes formées aussi bien par la Stratégie nationale pour l'intelligence artificielle que par la Stratégie nationale pour la cybersécurité nécessitent, pour être atteints aussi bien nationalement que dans le département des Hauts de Seine, des efforts dans plusieurs directions.

Les différents volets du présent diagnostic ont permis d'identifier d'une part des freins à l'augmentation du nombre de personnes formées à l'IA et à la Cybersécurité et d'autre part des pistes pour l'amélioration des contenus de l'offre de formation afin qu'elle puisse répondre au mieux aux besoins actuels et futures des entreprises du territoire, et de la société dans son ensemble.

Freins :

- l'attractivité limitée, pour les lycéens, et pour les étudiants, des formations et des métiers nécessitant des connaissances poussées en mathématiques ;

- depuis la réforme du lycée, la part importante d'élèves de terminale ne suivant pas d'enseignement de mathématiques ; Un niveau général en mathématiques insuffisant pour s'engager dans un cursus avec une part d'informatique.

- les tarifs élevés des formations proposées par certaines écoles et des organismes de formations privés ;

- les délais importants nécessaires pour l'élaboration et l'accréditation de nouvelles formations diplômantes.

Pistes pour l'amélioration du contenu de l'offre de formation

- inclure, dans l'ensemble des formations proposées en IA et Cybersécurité, aux côtés du bloc de Compétences techniques, un bloc de Compétences transversales (Soft skills) et un bloc de Compétences managériales. Les contenus proposés pour ces blocs sont décrits en p.49

- inclure, dans l'ensemble des formations proposées en IA et Cybersécurité une sensibilisation aux enjeux environnementaux (de sobriété énergétique notamment) et éthiques (de protection des données notamment)

- proposer des doubles cursus IA + X (autre discipline de l'un des 4 grands domaines disciplinaires, SHS, DEG, STS ou ALL) afin de rendre les diplômés plus rapidement opérationnels dans le déploiement de l'IA à des domaines spécifiques.

L'analyse de l'adéquation entre les besoins de compétences actuels et anticipés et l'offre de formation actuelle, l'identification des freins et de pistes d'évolutions nécessaires a permis de définir les trois grands objectifs suivants et de proposer 12 actions en réponses à ces objectifs.

Objectifs I - Répondre à la pénurie de compétences en IA et cybersécurité sur le marché du travail à court et moyen terme.

1.1. Formation initiale pour répondre aux besoins de recrutement
1.2. Formation continue pour accompagner la mobilité professionnelle et la montée en compétence des salariés

Objectif II - Sensibiliser les TPE/ PME au potentiel de création de valeur que représente le traitement avancé des données, son automatisation, et la mobilisation des algorithmes de l'IA dans l'entreprise

Objectif III - Anticiper les évolutions des besoins de compétences

Objectif I Répondre à la pénurie de compétences en IA et cybersécurité sur le marché du travail à court, moyen et long terme

I.1. Formation initiale

Action 1. Diversifier les profils de recrutement en formation initiale, au-delà des ingénieurs et diplômés de Master spécialisés IA ou cybersécurité vers des profils plus généralistes.

- Des formations scientifiques du domaine STS, et même EG et SHS accueillant des bacheliers avec un bon niveau en mathématiques, et comportant un volume horaire important en mathématique, statistique, informatique et programmation durant les cursus peuvent avoir les compétences nécessaires pour les métiers de la Cyber et de l'IA. A titre d'exemple, les Licences économie – gestion, parcours Economie comportent un enseignement de mathématiques à chaque semestre, ainsi que des enseignements de statistiques en 3ème année et pourraient augmenter, après une formation complémentaire adaptée pour leurs diplômés, éventuellement interne à l'entreprise, le vivier de recrutement en IA et Cybersécurité.
- Créer, par le biais des alumnis, des partenariats avec des formations bien identifiées.

Action 2. Accroître l'attractivité des filières IA et cybersécurité par des actions auprès des lycéens et auprès des étudiants.

- Travailler avec les lycées, l'ONISEP et les établissements d'enseignement supérieur pour mettre en œuvre un plan d'information et de communication sur les métiers de l'IA et la Cybersécurité, mobilisant des médias adaptés au public jeune. Il s'agira notamment de déployer, au sein du territoire des Hauts de Seine,
- Envoyer des salariés « ambassadeurs » dans les événements (Forums des métiers, Rencontres entreprises) organisés par les établissements d'enseignement secondaire et supérieur.
- Proposer aux enseignants du secondaire, et aux élèves, une sensibilisation et des formations à l'IA et à la Cybersécurité
- Elargir l'implémentation, dans les collèges et lycées du 92, des actions de formation et de sensibilisation proposées dans le cadre de la Stratégie nationale pour l'IA, comme l'utilisation des MOOC de formation sur l'IA pour accompagner les enseignements d'informatique au lycée (https://www.fun-mooc.fr/courses/course-v1:inria+41018+session01/about) ou la démonstration du robot AlphAI.

Action 3. Intensifier au niveau régional la réflexion et le partage de pratiques en matière de formation et de recrutement sur les thématiques IA et Cyber en impliquant la CCI, les organismes professionnels et les organismes de formations.

Un groupe de travail réunissant des représentants de ces différents acteurs pourrait être constitué et se réunir une fois par an pour un bilan qualitatif et quantitatif sur le territoire d'une part de l'évolution des inscrits en formation et des offres d'emploi, et aussi pour un échange sur les perspectives d'évolutions.

I. 2. Accompagner la mobilité professionnelle et la montée en compétence des salariés

Action 1. Créer des parcours de formation bien identifiés pour les professionnels leur permettant d'évoluer vers des postes de responsabilité en cybersécurité ou en Data management.

Exemples :

- Proposer des parcours de formation continue pour des professionnels de l'informatique vers la cybersécurité
- Proposer des parcours de formation continue pour des professionnels du droit vers des postes de délégués à la protection des données
- Proposer des parcours de formation continue pour des professionnels avec une formation scientifique vers la data science et l'IA
- Proposer des parcours de formation continue pour des cadres en informatique leur permettant d'évoluer vers le métier de Data engineer dont la rareté est soulignée par les grandes entreprises.

Action 2. Travailler avec les organismes professionnels et les organismes de formation pour la mise en place et la communication sur ces différents parcours de formations.

Action 3. Travailler avec les RH pour la communication auprès des salariés sur ces possibilités de mobilité professionnelle.

Objectif II Sensibiliser les TPE/ PME au potentiel de création de valeur que représente le traitement avancé des données, son automatisation, et la mobilisation des algorithmes de l'IA dans l'entreprise

Action 1. Organiser des campagnes d'information sur la valorisation et la culture de la donnée en entreprise.

Action 2. Créer un office départemental de sensibilisation, de conseils et d'orientation sur la valorisation des données et outils de l'IA à destination des TPE/PME.

Objectif III Anticiper les évolutions des besoins de compétences

Action 1. Intégrer une initiation en IA et Cybersécurité dans les formations universitaires dès la Licence.

Les formations de Licence proposées par la majorité des universités aujourd'hui comportent des modules destinés à l'acquisition de compétences transversales (par exemple méthodologie du travail universitaire, outils de professionnalisation etc.), dont des compétences numériques (préparant aussi à la certification PIX). Ces enseignements sont proposés à l'ensemble des étudiants, souvent sous le format d'enseignement à distance asynchrone, complété dans certains cas par des TD en présentiel, avec des volumes horaires relativement limités (entre 15h et 20h) quel que soit le domaine disciplinaire de Licence choisi.

Une sensibilisation aux Cyber risques et à la Cyber sécurité est déjà majoritairement proposée dans les modules de préparation à la certification PIX. Il est possible de l'enrichir, notamment par des contenus plus interactifs.

Concernant l'IA, des modules d'initiation peuvent être proposés suivant le même format (modules d'enseignement à distance combinés avec du présentiel ou du distantial synchrone) pour toutes les formations du domaine STS, mais aussi pour les formations des domaines Droit Economie Gestion (DEG) et Sciences Humaines et Sociales (SHS) comportant des enseignements en mathématiques appliquées, statistiques et informatique.

Action 2. Proposer de nouveaux cursus de Master en Intelligence artificielle et Cybersécurité sur le territoire du 92

Même si de nombreuses formations de Master ont vu le jour depuis la mise en place de la Stratégie Nationale pour l'IA et la Cybersécurité (concernant l'IA**, 35 masters ont été recensés en 2019** contre 19 en 2017, et actuellement plus de 40), peu d'entre eux se situent sur le territoire du 92. Par ailleurs, plusieurs formations, notamment à l'Université Paris Nanterre, tout en formant aux compétences de l'IA ne sont pas précisément identifiés comme tel (par exemple le CMI Data Sciences for Social Sciences ou le Master Statistique et économie du risque).

Les nouvelles formations proposées doivent comporter l'ensemble des 3 blocs identifiés par les entreprises comme indispensables pour la formation d'un cadre de la cybersécurité ou de l'intelligence artificielle, à savoir : le bloc technique, le bloc de compétences transversales et le bloc de compétences managériales. Une composante indispensable du bloc de compétences transversales à inclure dans les futures formations en IA est un module sur la protection des données et sur l'éthique des algorithmes.

Concernant les métiers visés, l'étude réalisée incite à mettre l'accent sur ceux de Data engineer, Architecte big data, Ingénieur Big data, Chef de projet Data, Cybersecurity Engineer, SOC Analyst, Ingénieur SIEM, Cybersecurity Architect, Chef de projet Cyber, Architecte sécurité des SI.

Action 3. Créer des doubles cursus de Licence ou de Master.

Les doubles licences et les masters habilités sur deux domaines disciplinaires rencontrent aujourd'hui un succès croissant auprès des étudiants. Ces formations, très sélectives, attirent un public de bacheliers et de diplômés de Licence de très bon niveau, attaché au système universitaire et à la vie étudiante qui est associée. Ces formations, qui garantissent à leurs diplômés une culture pluridisciplinaire, et une grande ouverture, proposent aussi des débouchés professionnels plus riches, notamment vers de nouveaux métiers.

Des doubles formations de Licence qui peuvent mener vers les métiers de l'IA et de la Cybersécurité, ou vers des Masters spécialisés existent, mais elles restent pour le moment mal identifiées et peu visibles, comme par exemple les doubles licences Mathématiques-Informatique, les Doubles licences Economie-Gestion-Mathématiques, doubles licences Informatique-Economie-Gestion, exception faite de la très récente double licence IA-Sciences des organisations.

Des doubles licences Cybersécurité- Sciences du comportement, IA-Sciences des organisations ou IA-Droit pourraient répondre à certains besoins de compétences bien identifiés relatifs à la sensibilisation aux cyber risques, à la protection des données personnelles et aussi à l'usage de l'IA dans les organisations. Néanmoins, les recrutements se faisant principalement à un niveau Bac+5, les doubles licences ne sont pas seulement une voie vers une insertion professionnelle directe, mais plutôt un voie privilégiée vers des masters spécialisés particulièrement sélectifs, comme le sont les Masters préparant aux métiers de la Data et de la cybersécurité.

Concernant les Masters, des masters habilités sur les deux domaines STS et DEG ou STS et SHS peuvent permettent aux diplômés d'acquérir les compétences nécessaires pour l'implémentation des algorithmes de l'IA dans différents domaines.

Ainsi, des formations de Master en IA et géographie, IA et Gestion des risques, IA et santé, IA et environnement ou IA et Droit par exemple, proposées par des universités pluridisciplinaires qui proposant toutes ces disciplines et peuvent adosser ces formations à des laboratoires de recherche, peuvent répondre aux besoins de compétences des entreprises en formant à des métiers de Data analyst ou Data engineer spécialisé dans un domaine particulier, et aussi de DPO.

Action 4. Stimuler les recherches pluridisciplinaires appliquées en IA et cybersécurité.

Les stratégies nationales IA et Cybersécurité prévoient le financement de thèses sur ces thématiques, mais essentiellement pour des projets de recherche fondamentale menés dans les laboratoires de mathématique, informatique et sciences de l'ingénieur. Pour stimuler les recherches pluridisciplinaires, et aussi sur des sujets qui accompagnent les dimensions techniques de l'IA et de la cyber, par exemple sur les dimensions éthiques, environnementales et comportementales, des financements de thèse dans les disciplines du domaine DEG et SHS pourraient être proposés, par exemple au niveau de la région.

Action 5. Créer une cellule régionale de veille scientifique et technologique associant chercheurs et entreprises.

3. Articulation avec les priorités du plan France 2030

France 2030 et les stratégies nationales « IA » et « Cybersécurité »

Présentées respectivement en 2018 et 2021 et rattachées à France 2030, les stratégies « IA » et « cybersécurité » traduisent la volonté de l'Etat de s'emparer activement de ces sujets, et d'en porter un déploiement coordonné et suivi. Avec 1,5 milliards d'euros de financements publics prévu pour la stratégie IA, et 700 millions pour la stratégie cybersécurité, l'Etat fixe des objectifs ambitieux dans les deux domaines pour renforcer la souveraineté, la sécurité, l'innovation et la compétitivité de la France dans ces domaines émergents et stratégiques. Sont visés par exemple le doublement des emplois dans le domaine de la cybersécurité et l'émergence de 3 licornes, la formation annuelle de 1 900 étudiants de tous niveaux en IA, l'accompagnement de 400 entreprises dans l'accès à des solutions d'IA, etc. De manière générale, les deux stratégies accordent une attention particulière au développement de la formation, initiale ou continue, existante ou à créer.

En effet, ces stratégies entendent jouer à la fois sur l'offre - avec le développement de la recherche et de formations - et sur la demande, en impliquant l'Etat, les collectivités territoriales et les entreprises dans la consommation de services IA pour améliorer leur productivité, et cyber pour sécuriser leur activité.

– Le Diagnostic de la CCI sur les besoins des entreprises du 92 …

Le présent diagnostic adopte aussi un point de vue qui associe demande et offre.

D'un côté, il identifie d'importants besoins du côté des entreprises des Hauts-de-Seine en termes de métiers et compétences. Concernant la cybersécurité, la part d'entreprises qui continuent de développer leur protection numérique est de 63 %, garantissant une demande constante de compétences et services dans le domaine. Du côté de l'IA, l'étude retient une hypothèse d'entre 15% et 20% d'ETI qui l'auront intégré à leur activité dans les prochaines années. C'est d'ores et déjà 100% des grandes entreprises.

Majoritairement, les entreprises envisagent de combler ce fort besoin avec le recrutement de nouveaux salariés, ce qui nécessite l'existence de formations initiales adaptées sur notre territoire. Les profils les plus demandés sont de niveau BAC+5 (ingénieurs et chefs de projet), bien que le manque de main d'œuvre et la diversité des métiers laisse aussi une belle part à des études moins longues, si besoin, complétées par la formation interne.

- … est cohérent avec les besoins identifiés (et amplifiés) par les stratégies nationales.

Ces conclusions sont cohérentes avec les besoins identifiés par les stratégies nationales : le déficit de main d'œuvre en cybersécurité est pleinement identifié par la stratégie éponyme, sur des métiers et des niveaux de formations très divers. De plus, en souhaitant mieux protéger les collectivités territoriales, les services de l'Etat, et sensibiliser les entreprises, la stratégie amplifiera elle-même les besoins avec des financements en ce sens à hauteur de 156 millions d'euros.

La stratégie IA repère elle-aussi des besoins importants pour améliorer la compétitivité et la productivité des entreprises, qu'elle souhaite même amplifier. Pour accélérer le déploiement de l'intelligence artificielle dans l'économie, elle accompagnera directement 400 entreprises à adopter des solutions IA. Elle insiste par ailleurs sur l'engouement de nombreux secteurs (notamment des grands groupes) pour l'IA, ce que l'étude du présent diagnostic confirme.

De plus, les deux stratégies amplifieront les besoins en métiers et compétences en soutenant de grands projets comme le CyberCampus ou le calculateur Jean Zay. A plus petite échelle, France 2030 et les opérateurs de l'Etat prévoient aussi plusieurs appels à projets en lien avec la cybersécurité ou l'intelligence artificielle (aide à la certification SecNumCloud par exemple) pour accélérer le développement d'une offre française innovante. Cette accélération engendrera dans l'économie une augmentation de la demande de compétences IA / Cyber.

- Répondre à ces besoins par de la formation ciblée et massifiée, initiale ou continue.

Pour répondre à cette demande, il s'agira de développer l'offre de formation. Là encore, le plan d'action du présent diagnostic est cohérent avec les orientations des stratégies nationales.

Pour la cybersécurité, il s'agit de prévoir des parcours plus diversifiés, en attirant largement des profils encore éloignés du secteur par manque de médiatisation. La stratégie insiste notamment sur la formation continue, qui est un des axes du plan d'action proposé par le présent diagnostic.

Pour l'IA, la stratégie poursuit le double objectif d'une massification et d'une montée en qualité des formations. Avec la formation nationale annuelle de 1 500 étudiants en Master, le financement de 200 thèses, et le volet « Formations d'excellence », elle entend répondre spécifiquement aux besoins des entreprises en compétences de pointe. Cette ambition est cohérente avec les besoins de métiers très qualifiés formulés par les entreprises interrogées des Hauts-de-Seine.

En termes de massification et de diversification, la stratégie insiste sur l'interdisciplinarité, la création ou l'adaptation de cursus moins longs mais mieux adaptés et transversaux. Ce volet de massification présente une enveloppe de 276 millions d'euros. Le présent diagnostic s'inscrit précisément dans cette démarche, en proposant d'associer les sciences sociales, de la donnée, des mathématiques, de l'informatique.

Ainsi, en dressant un diagnostic précis des besoins des entreprises des Hauts-de-Seine concernant l'IA et la cybersécurité, le présent rapport confirme et affine les observations des stratégies nationales de France 2030. Ces besoins sont particulièrement développés dans le département avec la présence du Campus Cyber, d'un tissu économique dense et avec un fort volet numérique, duquel émergeront nécessairement de nombreux projets financés et amplifiés par France 2030.

Pour répondre à ces besoins, le présent diagnostic identifie déjà une offre de formation existante très développée sur notre territoire. Le plan d'action proposé pour amplifier cette offre s'inscrit dans la droite ligne des orientations définies par les stratégies nationales, en termes de création de formations ciblées, transversales et diverses, aussi bien dans leurs cibles de recrutement que dans leur niveau.

Annexes

GOUVERNEMENT

Liberté
Égalité
Fraternité

Contacts

Claire BERTHOMIEU, CCID Hauts-de-Seine : cberthomieu@cci-paris-idf.fr