À LA CROISÉE DES CHEMINS

Intelligence artificielle et cybersécurité

EXPLORATION DE LA DYNAMIQUE DE CES DEUX TECHNOLOGIES EN MATIÈRE D'EMPLOI, FORMATION ET COMPÉTENCES À BRUXELLES

Digitalcity.brussels
Pôle Formation Emploi des métiers du numérique

RAPPORT DE VEILLE

2024

ÉDITORIAL

Entre symbiose et effet de mode, ce rapport explore les liens entre l'intelligence artificielle (IA) et la cybersécurité, deux domaines cruciaux qui façonnent notre paysage numérique contemporain. À travers l'analyse de ce rapport, nous examinons l'impact mutuel de ces disciplines et de leur influence sur les métiers et la formation en technologies de l'information à Bruxelles.

L'IA et la cybersécurité sont étroitement liées, se renforçant mutuellement dans un cycle continu d'innovation. L'IA offre des outils prometteurs pour renforcer la sécurité des systèmes informatiques, tandis que la cybersécurité garantit la fiabilité et l'intégrité des solutions d'IA. Toutefois, cette relation n'est pas sans défis.

À Bruxelles, carrefour européen de l'innovation et de la technologie, ces questions revêtent une importance particulière. Les entreprises et les institutions doivent s'adapter rapidement aux évolutions technologiques tout en formant une main-d'œuvre qualifiée capable de relever ces défis complexes.

Ce document met en évidence les enjeux économiques majeurs liés à l'IA et à la cybersécurité, soulignant l'importance cruciale de ces secteurs pour la compétitivité et la résilience des entreprises et des infrastructures dans un environnement numérique en constante évolution.

Ensemble, en investissant dans la formation et en favorisant l'innovation, nous pouvons créer un avenir dans lequel les métiers du numérique sont, non seulement résilients aux défis technologiques, mais aussi porteurs d'opportunités sans précédent tant pour les chercheurs d'emploi que les entreprises. Digitalcity.brussels est au cœur de cette transformation, en offrant un environnement dynamique où les talents peuvent s'épanouir et contribuer à façonner un avenir numérique prometteur pour Bruxelles et au-delà.

JEAN-PIERRE RUCCI
Directeur de Digitalcity.brussels

PIERRE MERVEILLE
Président de Digitalcity.brussels

QU'EST-CE QUE DIGITALCITY.BRUSSELS ?

NOUS SOMMES

L'ASBL Pôle Formation-Emploi des métiers du numérique, Digitalcity.brussels, émane d'un partenariat public-privé fondé entre les partenaires sociaux sectoriels d'une part, et le service public de l'emploi bruxellois (Actiris) ainsi que les services publics de formation (Bruxelles Formation et VDAB), d'autre part. Digitalcity.brussels fédère une réelle concertation entre les entreprises et les acteurs du Pôle. Ses missions constituent sa raison d'être. Aussi Digitalcity.brussels se positionne comme un partenaire de référence unique et incontournable à Bruxelles dans le domaine de la formation et de l'emploi pour le secteur et les métiers du numérique et pour tous nos publics tant les entreprises, les travailleurs, que les CE, les étudiants, etc.

digitalcity.brussels

NOS VALEURS

Les cinq valeurs essentielles portées au sein de notre organisation multi-partenariale sont :

01 Collaboration
La Collaboration qui relie l'esprit d'équipe et la solidarité.

02 Amélioration continue
L'Amélioration continue qui doit montrer notre capacité à nous remettre en question et à gérer le changement.

03 Satisfaction
La Satisfaction des usagers bruxellois et du personnel du Pôle.

04 Orienté solution
La démarche Orientée solution qui permet une approche pragmatique de résolution des problèmes et la mobilisation de l'intelligence collective.

05 Innovation
L'Innovation qui renvoie à une façon imaginative de faire face au changement, de générer de nouvelles idées, d'améliorer les processus et de renouveler nos services.

Les collaborateurs et les partenaires de Digitalcity.brussels s'engagent fermement à refléter ces valeurs dans leur quotidien en les intégrant à toutes les facettes de leurs missions et responsabilités.

TABLE DES MATIÈRES

RAPPORT DE VEILLE 2024

Dans le monde numérique actuel, l'union entre l'intelligence artificielle (IA) et la cybersécurité sculpte un paysage où l'innovation et la résilience se mêlent. À Bruxelles, épicentre européen bouillonnant d'activités économiques et entrepreneuriales, cette convergence éveille des enjeux cruciaux et des débats intéressants. La montée des cybermenaces ainsi que les avancées technologiques mettent ces deux secteurs de l'IT sur le devant de la scène tout en interrogeant sur leurs portées, leurs utilisations, etc. Fort de ces constats, il semble alors nécessaire de questionner plusieurs points : quelles sont leurs relations et leurs interconnexions ? Quel est l'impact de l'IA sur la cybersécurité (au niveau des menaces et des protections) ? Comment sécuriser une IA en pleine expansion, notamment en évitant les biais et les utilisations malveillantes ? Surtout, quel est l'impact de ces deux domaines sur l'évolution des métiers IT, le marché du travail bruxellois et l'offre de formation existante et future ?

Dans ce rapport, nous explorons le cœur de cette symbiose, avec pour toile de fond le positionnement stratégique des entreprises, l'évolution des profils IT, et la refonte des offres de formations.

AGENDA

En septembre 2023, pour lancer cette thématique, nous avons diffusé un webinaire dans lequel cinq experts en IA et cybersécurité ont débattu ensemble des possibilités d'interaction de ces deux domaines.

- HUGUES BERSINI de l'ULB
- GRÉGORIO MATIAS de MCG
- MARTIN FOCKEDEY du CCB
- ISSAM EL HADDIOUI de Checkpoint
- MICHEL HERQUET de B12

YouTube

Le replay de ce webinaire est consultable sur la **chaine YouTube** de **Digitalcity.brussels**.

OBJECTIFS & MÉTHODOLOGIE DU RAPPORT

01

OBJECTIFS

Ce rapport de veille vise à explorer l'impact de l'IA dans le domaine de la cybersécurité en Belgique, et inversement, en mettant l'accent sur l'écosystème des sociétés bruxelloises. En analysant le marché, les solutions existantes, les perceptions des acteurs du secteur, les profils-métiers, et les enjeux de recrutement, ainsi que les formations disponibles, le rapport propose une vision globale de la situation actuelle. Il examine entre autres les opportunités futures pour l'IA dans la cybersécurité en Belgique, mais également les perspectives du marché de l'IA à Bruxelles en mettant l'accès sur les enjeux métiers et formations.

Notre rapport est le fruit d'une analyse minutieuse, alimentée par un grand nombre d'études, de rapports d'experts, de données provenant d'organismes d'analyse renommés, ainsi que de stratégies gouvernementales. Chaque observation est solidement étayée par une base de connaissances variée et approfondie, offrant ainsi une perspective complète et éclairée sur les sujets abordés dans ce rapport. En complément, nous avons effectué une série d'entretiens auprès d'experts et d'entreprises pour apporter des éléments supplémentaires sur la réalité du marché. La liste complète des experts interrogés est disponible à la fin du rapport.

En conclusion de notre étude, nous avons pris l'initiative de transformer nos conclusions non plus seulement en recommandations, mais en actions tangibles, alignées sur les objectifs de Digitalcity.brussels. Ces initiatives ciblent spécifiquement les défis rencontrés dans les domaines des métiers et de la formation numérique, avec pour ambition de devenir le moteur de l'unité dans le paysage numérique de Bruxelles.

Notre objectif principal est de relever les défis inhérents à ce domaine et de présenter des projets concrets qui catalyseront l'harmonisation des efforts dans le monde de la formation numérique à Bruxelles. Ces initiatives visent également à accroitre la visibilité du secteur des technologies de l'information, de l'offre de formation et de la diversité des carrières, notamment face à la pénurie de professionnels qualifiés, dans les domaines de l'IA et de la cybersécurité.

DÉFINITION DU CHAMP D'ANALYSE

02

02 INTRODUCTION

Pour bien comprendre le sujet, il est important de vous proposer une définition et une explication de ces deux domaines que nous allons analyser dans la suite du rapport.

Au-delà des définitions, ces thématiques sont associées à une série d'enjeux spécifiques qui mettent en lumière la complexité du monde numérique à travers des points clés tels que la sécurité, la sensibilisation, la gestion des données et l'attractivité économique. Ce chapitre évoquera ces points à travers les sujets de la cybersécurité et de l'intelligence artificielle.

2.1 Cybersécurité : définition et enjeux

Dans la stratégie cybersécurité Belgique 2.0, on y définit la cybersécurité comme *étant le résultat d'un ensemble de mesures de sécurité qui doivent minimiser le risque d'accès perturbé et non autorisé aux systèmes d'information et de communication (TIC)*[1]. Autrement dit, ce sont toutes les lois, les cadres, les dispositifs et les méthodes de gestion de risque qui **visent à protéger** les personnes et les actifs (matériels et immatériels) des États et des organisations.

La célèbre entreprise américaine de conseils et de recherches connue pour ses analyses des tendances technologiques, Gartner, définit la cybersécurité de la manière suivante : la cybersécurité[2] consiste *à déployer des personnes, des politiques, des procédures et des technologies pour protéger les organisations, leurs systèmes critiques et les informations sensibles contre les attaques numériques*.

La protection est donc une notion clé dans le domaine de la cybersécurité. Or, avec la dématérialisation de plus en plus massive des données privées, officielles et professionnelles, il y a un **véritable élargissement de la surface d'attaques des criminels**. L'un des enjeux essentiels du secteur de la cybersécurité est la prise de conscience de cette menace qui touche tant le citoyen que l'entreprise, petite ou grande. **L'aspect sensibilisation** est primordial dans ce contexte et le travail est encore long au vu de l'actualité bouillonnante en matière de cybersécurité. Pour ne citer qu'un exemple actuel, les nombreuses attaques récentes des institutions hospitalières en Europe qui sont de plus en plus visées par des attaques ciblées fragilisant leurs infrastructures. Il est aujourd'hui impératif que les pays - mais aussi les entreprises et les organismes publics - deviennent résilients et adoptent des mesures de gestion de crise en lien avec la cybersécurité. **Protéger les instances vitales, les entreprises et le citoyen est un des éléments cruciaux qui font partie de la priorité de la stratégie de cybersécurité en Belgique et, de facto, en Europe.**

La cybersécurité a également un enjeu d'ordre socio-économique. En raison de l'expansion de la menace cyber, les services professionnels de protection se développent en Belgique, en Europe et dans le monde entier. Dans les entreprises spécialisées et dans les autres entreprises qui déploient des départements entiers dédiés à la protection de l'entreprise et de ses clients, nous constatons **un véritable boom dans les demandes de sécurisation**. Cela entraine une **pénurie des talents** partout dans le monde estimée à **5.5 millions** de personnes selon une étude d'ISC2[3].

[1] CBB – Stratégie cybersécurité Belgique 2.0 – 2021 -2025.

[2] Gartner – What is cybersecurity?

[3] ISC2 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce – 2023.

2.2 IA : définition et enjeux

Dans sa proposition de règlement en 2021, la Commission Européenne définit l'intelligence artificielle (IA) comme *« un logiciel qui peut, pour un ensemble donné d'objectifs définis par l'homme,* ***générer des résultats*** *tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit*[4] *»*. Au Parlement Européen, on différencie deux types d'intelligences artificielles[5] :

L'IA *« logicielle »* comme les moteurs de recherche, les assistants virtuels, les systèmes de reconnaissances faciale et vocale, etc.

L'IA *« incarnée »* comme les robots, les voitures autonomes, l'Internet des objets, etc.

Mais on entend souvent parler également de Machine Learning (ML). Qu'est-ce que le ML ? Le *Machine Learning* ou *l'apprentissage automatique* est un sous-genre de l'IA qui mise sur **l'apprentissage et l'amélioration autonome** du système à partir de l'expérience sans être explicitement programmé. On utilise les algorithmes d'apprentissage dans le but d'entrainer les modèles d'IA.

L'IA générative ou GenAI, quant à elle, est une forme d'IA qui génère des données et du contenu (écrits ou visuels) en produisant de nouvelles données. On peut distinguer la GenAI de l'IA classique **(IA discriminative)**, car l'IA classique se concentre sur des tâches plus spécifiques comme la classification, la prédiction et la résolution de problèmes sur la base de données préexistantes. ChatGPT ou Midjourney sont des exemples de GenAI.

Les **grands modèles de langage** (large langage model - LLM) sont des républiques de données structurées qui sont spécifiquement destinées à la compréhension du langage naturel (NLP - natural language processing).

L'un des enjeux liés à l'IA est **l'éthique**. Il s'agit de la problématique la plus complexe de ces prochaines années en lien avec l'accélération des techniques d'IA pour les organismes. **Comment développer une IA plus éthique, plus sécuritaire et sans biais ?** L'IA d'aujourd'hui est-elle une technologie digne de confiance ? C'est dans ce contexte qu'il est aujourd'hui nécessaire de légiférer pour cadrer l'évolution de cette nouvelle technologie. Au niveau européen, c'est notamment l'objectif du **AI Act**.

Un autre enjeu est **l'attractivité de l'IA** dans le contexte d'une économie globale. Comment renforcer la compétitivité grâce à l'IA ? C'est une technologie puissante qui peut dans le monde du travail être au service de la santé, de la mobilité, de l'écologie et de la sécurité et d'autres secteurs encore. Elle peut même être au service de la rentabilité, de l'attractivité, de la compétitivité et de la productivité d'une entreprise.

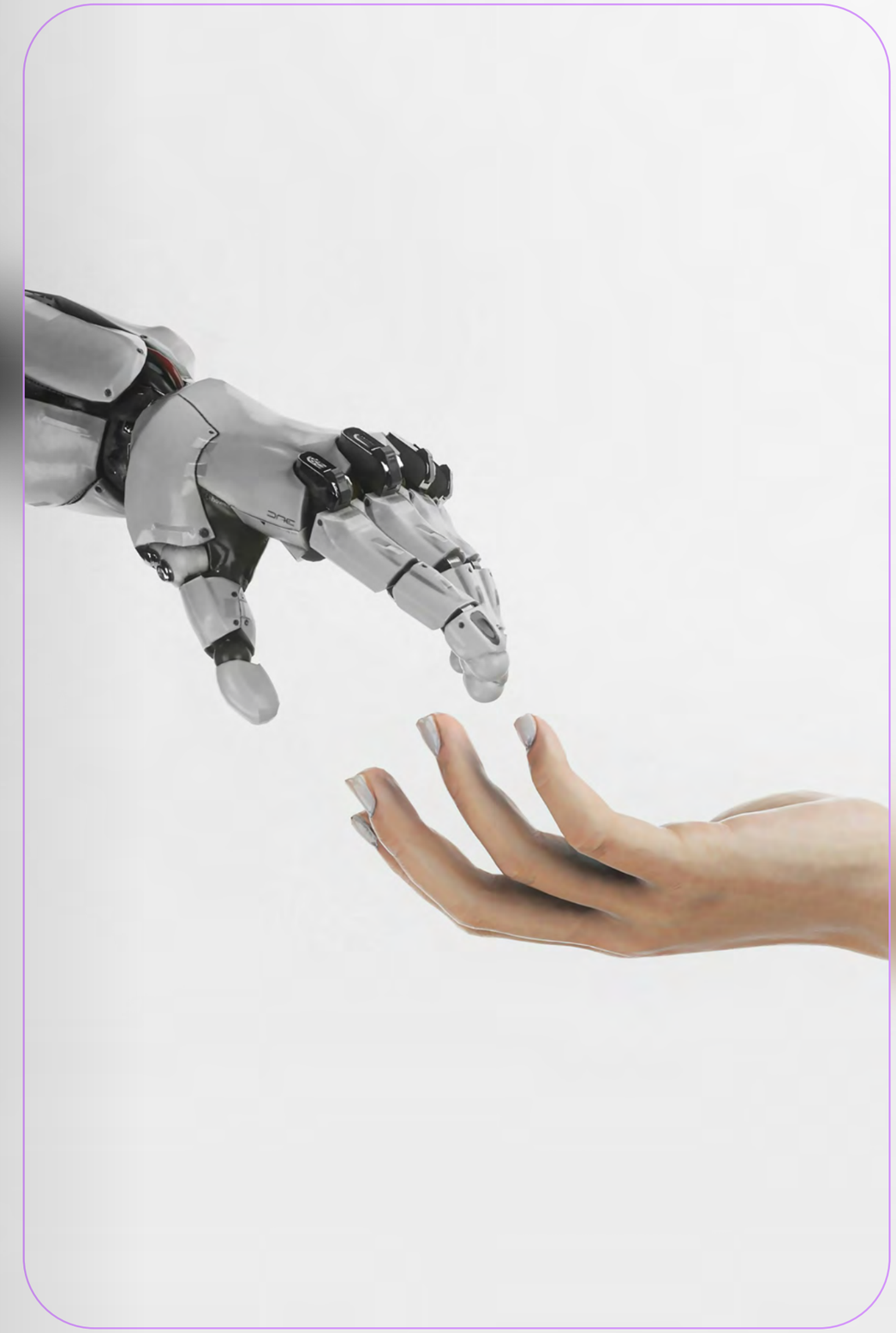
Elle apporte un réel potentiel économique, mais celui-ci doit être cadré dans une législation et règlementation structurée, notamment sur la protection des données. L'enjeu est actuellement considéré par les institutions européennes et les solutions qui posent les défis actuels et futurs.

iA [L'INTELLIGENCE ARTIFICIELLE]

Un logiciel qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit.

[4] Toute l'Europe - Intelligence artificielle : que fait l'Union européenne ? – 2024.

[5] European Parlement - Intelligence artificielle : définition et utilisation – 2021.



LES SECTEURS EN BELGIQUE

03

En 2022, Agoria, la fédération des industries technologiques, a conduit une étude sur l'état du secteur de la cybersécurité en Belgique[6].

3.1 Le secteur de la cybersécurité

Selon l'étude, ce secteur est composé de **441 entreprises belges** spécialisées en cybersécurité. Ces entreprises emploient à elles seules **6405 ETP (équivalents temps plein)**. Néanmoins, il n'y a pas que les entreprises de la cybersécurité qui recrutent des profils d'experts. Certains secteurs, comme le secteur bancaire et assurance ou encore le gouvernement recherchent également un grand nombre de profils en lien avec la cybersécurité.

Cela s'explique par la digitalisation accrue des entreprises - grandes ou petites ; ainsi que par un stockage des données dans le cloud en hausse. Cela entraine un risque accru en matière de sécurité étant donné que le terrain de jeu des hackers criminels s'étend également. Une enquête de StatBel sur l'utilisation des TIC dans les entreprises[7] estime que *« 23,2% des sociétés belges ont connu au moins une fois un problème dû à un incident de sécurité lié aux TIC »*. Cela se matérialise par l'indisponibilité de certains services, la destruction, la corruption ou la divulgation des données confidentielles. Dans ce contexte, les PME sont moins armées pour combattre les nouvelles menaces qui sont plus sophistiquées.

Pourtant, en 2022, selon une étude de Proximus[8], le nombre de grandes entreprises touchées par les cybermenaces est plus important que les petites. **45% des grandes entreprises interrogées déclarent avoir été confrontées à un ou plusieurs incidents cyber contre 25% pour les PME.** C'est sans prendre en compte le fait que les grandes sociétés sont bien mieux préparées aux attaques, car elles ont davantage de moyens (humains, financiers et stratégiques) pour se protéger et ont souvent une culture du digital et de la sécurité plus installée à travers des formations, de la sensibilisation et des plans de gestion de crises. De ce fait, ce sont les plus petites entreprises qui sont les plus impactées par ce type d'incidents.

Avec la menace croissante, le besoin de recrutement de spécialistes de la cybersécurité augmente et devient un enjeu sociétal. C'est un secteur en plein boom. Or, on constate en Belgique et partout dans le monde une importante pénurie de talents. L'étude d'Agoria pointe du doigt une pénurie de **plus de 1200 employés dans le secteur de la cybersécurité et même plus de 3000 employés tous secteurs confondus**[9].

L'un des enjeux, quand on évoque la question de la cybersécurité, c'est **la sensibilisation** (auprès des citoyens, des jeunes, mais aussi des entreprises). Selon l'enquête de Proximus, *« la sensibilisation n'est pas encore généralisée*[10] *»*. **22% des collaborateurs dans les grandes entreprises déclarent n'avoir jamais eu de formations de sensibilisation à la sécurité informatique contre 46% au sein des PME**. Ce chiffre, bien que peu étonnant, reste percutant au vu de la croissance exponentielle des menaces à destination des entreprises.

[6] Agoria – First socio-economic study on the cyber security sector in Belgium, 2022.

[7] Statbel – enquête sur l'utilisation des TIC et de l'E-commerce dans les entreprises, 2022.

[8] Proximus – Rapport d'enquête. L'impact de la cybersécurité sur les entreprises du Benelux, 2022.

[9] Agoria – 2022, First socio-economic study on the cyber security sector in Belgium.

[10] Proximus – 2022: Rapport d'enquête. L'impact de la cybersécurité sur les entreprises du Benelux.

45%

45% des grandes entreprises interrogées déclarent avoir été confrontées à un ou plusieurs incidents cyber contre 25% pour les PME.

6 405 ETP

Les entreprises belges spécialisées en cybersécurité emploient à elles seules 6 405 ETP (équivalents temps plein).

441

Selon l'étude, ce secteur est composé de 441 entreprises belges spécialisées en cybersécurité.

10%

10% des entreprises utilisaient au moins une technologie d'intelligence artificielle[13].

3.2 Le secteur de l'intelligence artificielle

C'est sur le portail du collectif AI4Belgium que nous pouvons avoir une estimation de l'écosystème de l'intelligence artificielle en Belgique. Dans l'étude menée par AI4Belgium en 2020, il y a, en Belgique, **441 entreprises** qui fondent leur business sur les technologies de l'IA[11]. D'emblée, on constate que la Flandre, avec ses 233 entreprises, présente de manière significative le plus grand nombre de sociétés spécialisées en IA. Ensuite vient la Wallonie avec 106 entreprises et enfin Bruxelles avec 102 sociétés. Dans cet écosystème, on note avant tout la présence de sociétés spécialisées dans le service, dans la santé et de la Biotech, mais aussi dans l'agriculture, la fintech et le droit, les industries, etc. En 2023, au niveau européen, on dénombre 6 000 sociétés fondées sur un business de l'IA. Ce chiffre est loin derrière les performances des États-Unis qui recensaient environ 15 000 entreprises dans ce domaine[12]. À l'analyse de ces données, et au vu des perspectives d'évolution et de démocratisation de l'IA, le nombre d'entreprises belges a certainement évolué depuis les derniers recensements datés de 2020.

À côté de cela, il y a également les sociétés qui utilisent l'intelligence artificielle au profit de leur business. Selon le SPF Économie, en Belgique, en 2021, **10% des entreprises utilisaient au moins une technologie d'intelligence artificielle**[13]. Et bien entendu plus la taille de l'entreprise est grande, plus l'intelligence artificielle est implémentée. 41% des grandes entreprises contre seulement 8% des petites entreprises l'utilisent. Nous n'avons pas de données pertinentes quant à l'évolution du marché de l'IA en Belgique, mais au vu des prédictions globales, nous pouvons affirmer que l'IA s'est largement implantée dans nos sociétés et a déjà un impact au sein des entreprises. En effet, selon une étude prévisionnelle de l'International Data Corporation (IDC), la valeur mondiale des logiciels d'IA connaitra une croissance exponentielle puisque nous passerons de 64 milliards de dollars estimés en 2022 à plus de 250 milliards de dollars prévisionnés pour 2027[14].

Fait intéressant, selon l'étude du SPF économie[15], en Belgique, l'IA est principalement utilisée dans les entreprises pour la sécurité des TIC et ensuite pour l'organisation des processus de gestion d'entreprise. On note donc un réel intérêt du secteur de la cybersécurité pour l'implémentation de l'intelligence artificielle.

[11] AI4Belgium – Panorama de l'IA.

[12] Statista 2023 – Number of artificial intelligence (AI) companies in major economies worldwide in 2023.

[13] SPF Économie - 2021, Baromètre de la société de l'information, technologies numériques avancées.

[14] Developpez.com - Le chiffre d'affaires Mondial des logicielsd'IA,... 2023

[15] SPF Économie - 2021, Baromètre de la société de l'information, technologies numériques avancées.

STRATÉGIES, RÈGLEMENTATIONS ET ENCADREMENTS

04

04 INTRODUCTION

La cybersécurité et l'évolution de l'intelligence artificielle représentent pour les pays des enjeux stratégiques déterminants. Aujourd'hui, l'Europe, mais aussi la Belgique, a développé des plans stratégiques et créés des ponts entre ces deux domaines pour mieux déterminer et catalyser le potentiel de ces technologies.

4.1 Cybersécurité en Europe et Belgique

4.1.1 Europe : fondation et mandat de l'ENISA (2004)

En 2004, le Parlement Européen fonde l'ENISA dans le but d'améliorer la résilience des infrastructures européennes et de maintenir la sécurité numérique de la société et des citoyens. Les missions de l'ENISA sont renforcées grâce au règlement de l'Union Européenne sur la cybersécurité en 2019 et notamment le **EU Cybersecurity Act**[16].

Les missions de l'ENISA consistent à[17] :

1. Créer un cadre de coopération européen et être le chef d'orchestre de cette unification stratégique.
2. Élaborer une politique en matière de cybersécurité.
3. Miser sur une coopération européenne opérationnelle efficace.
4. Investir dans le renforcement des compétences et de l'expertise en cybersécurité.
5. Augmenter la confiance des utilisateurs en l'environnement numérique.
6. Anticiper pour élaborer des stratégies d'endiguement de la menace dans le but d'augmenter la résilience de l'Europe.
7. Assurer le partage et l'approfondissement des connaissances dans l'écosystème de cybersécurité de l'Union.

[16] European Commission: The EU Cybersecurity Act – 2023.

[17] ENISA - L'Agence de l'Union européenne pour la cybersécurité.

4.1.2 Europe : la directive NIS (2016 - 2024)

La directive européenne **NIS (Network and Information Security**) est entrée en vigueur en 2016. Il s'agit d'un premier texte européen en matière de cybersécurité. En 2019, elle a été transposée dans la législation belge. Elle vise, entre autres, à inciter les états membres à élaborer des stratégies nationales de cybersécurité.

Après révision, cette première version est considérée incomplète (limites sur la clarté des champs d'application et les compétences, manque de partage d'information et directive peu accordée à l'évolution croissante des menaces).

En 2021, le Parlement Européen propose une version 2.0 : la directive **NIS2**. Sur la base de cette nouvelle version européenne, la Belgique devra élaborer une loi sur le NIS. La directive a été publiée le 14 décembre 2022[18] et traduite en législation belge le 26 avril 2024.

La directive NIS2, en s'appuyant sur les acquis de NIS1, élargit ses objectifs et son périmètre pour renforcer la protection contre des acteurs malveillants de plus en plus sophistiqués. Même si l'IA y est très peu mentionnée, cette extension est sans précédent dans la réglementation cyber et marque un changement de paradigme au niveau européen.

Il existe d'autres directives et cadres européens qui règlementent la sécurité des infrastructures et des données et qui ont un impact sur la croissance de l'IA comme la *General Data Protection Reglementation (GDPR)* ou encore la *European Cyber Resilience Act (CRA)*, le *Digital Operational Resilience Act* (DORA) et, d'autres encore, qui visent à poser un cadre stratégique et à règlementer la sécurité au sein de l'Europe à tous les niveaux[19].

NIS

[NETWORK AND INFORMATION SECURITY]

La directive européenne ***NIS*** *est entrée en vigueur en 2016. Il s'agit d'un premier texte européen en matière de cybersécurité. En 2019, elle a été transposée dans la législation belge. Elle vise, entre autres, à inciter les états membres à élaborer des stratégies nationales de cybersécurité.*

4.1.3 Belgique : stratégie cybersécurité 2.0 (2021-2025)

En 2012, la Belgique se dote de son premier plan stratégique concernant la cybersécurité[20]. Faisant suite à cette première stratégie, la Belgique publie en 2021, une mise à jour de la stratégie, visant à renforcer la sécurité du cyberespace à travers plusieurs actions :

1. Renforcer l'environnement numérique et accroitre la confiance.
2. Armer les utilisateurs et administrateurs.
3. Protéger les organisations vitales contre les cybermenaces.
4. Répondre à la cybermenace.
5. Améliorer les collaborations publiques, privées et universitaires.
6. Engagement international.

Par rapport au plan de 2012, la version 2.0 met en avant les secteurs vitaux (énergie, finance, mobilité, santé publique, eau potable, fournisseurs de services numériques, gouvernement). Il précise que ces secteurs sont vitaux en raison d'une menace et des répercussions plus importantes par rapport aux autres secteurs économiques. Enfin, **il est évident que la collaboration entre les acteurs de la cybersécurité (administration, secteur public, secteur privé, organismes de formations, etc.) est un élément clé.** Toutefois, dans ce plan, l'impact de l'intelligence artificielle sur la défense cyber est peu abordée, même si l'intérêt de la technologie n'est pas sans intérêt.

4.1.4 Belgique : Cybersecurity Coalition (2015)

En matière de collaboration et d'unification des forces, la création de la **Cybersecurity coalition** est un bon exemple de mise en commun des ressources. Fondée en 2015, cette ASBL est un partenariat entre le monde académique, les autorités publiques et le secteur privé. La mission de ce regroupement est de contribuer à renforcer la résilience de la Belgique en cybersécurité en construisant un écosystème solide.

[18] Eur-Lex - Directive (EU) 2022/2555 of the European Parliament & of the Council.

[19] European Cyber resilience Act – website.

[20] Belgium, Cybersecurity strategy, 2012.

[21] Plan national de convergence pour le développement de l'intelligence artificielle – 2022.

4.2 Intelligence artificielle en Europe et Belgique

4.2.1 Europe : AI Act (2024)

Le cadre juridique reste le **AI Act** qui a obtenu sa version finale en janvier 2024. Il s'agit de la **première régulation européenne sur l'intelligence artificielle**. Cela démontre que l'intelligence artificielle et son utilisation ont fait un bond énorme. L'IA nécessite donc des mesures coordonnées pour règlementer son usage, définir ses limites et protéger les utilisateurs des biais possibles de cette technologie. Il est majoritairement question de sécurité des données et de protection des utilisateurs.

À travers des règlementations comme le AI Act, l'Europe souhaite permettre le développement de l'IA et son adoption de la manière la plus sécuritaire possible.

4.2.2 Belgique : fondation de AI4Belgium (2019)

En 2019, le **collectif AI4Belgium** est fondé dans l'objectif de réunir les acteurs privés, publics et académiques de l'IA belge. Cette coalition a à cœur de positionner la Belgique dans le paysage européen de l'IA. À la fondation de la coalition, un plan d'action a été dévoilé et qui présente 4 objectifs principaux :

1. Mettre l'IA au sommet de l'agenda politique.
2. Inspirer le débat public. Accompagner le public à la compréhension des implications de l'IA.
3. Encourager et déployer l'IA orientée humain.
4. Première version d'une stratégie belge sur l'IA qui débouche sur le dévoilement du plan de convergence.

AI Act

Le AI Act est le premier cadre de loi qui vise la régulation européenne de l'intelligence artificielle. Il a été finalisé en janvier 2024.

4.2.3 Belgique : plan de convergence pour le développement de l'IA (2022)

En 2022, l'administration fédérale belge a publié un plan national de convergence pour le développement de l'IA avec 9 objectifs stratégiques[21] :

- Promouvoir une IA digne de confiance.
- Garantir la cybersécurité.
- Renforcer la compétitivité et l'attractivité de la Belgique grâce à l'IA.
- Développer une économie basée sur les données et une infrastructure performante.
- L'IA au cœur de la santé.
- Au service d'une mobilité plus durable.
- Préserver l'environnement.
- Former mieux et tout au long de la vie.
- Fournir aux citoyens de meilleurs services et une meilleure protection.

Notons que l'axe 2 du plan de convergence se concentre sur la relation entre IA et cybersécurité ce qui nous permet de nous rendre compte du lien et de l'impact de ces deux domaines et l'impact de l'un sur l'autre.

INFLUENCES CROISÉES - IA ET CYBERSÉCURITÉ

05

5.1 L'IA au service de la sécurité

Les récentes avancées technologiques de l'intelligence artificielle ont ouvert le champ des possibles concernant son utilisation en cybersécurité.

On évoque souvent l'utilisation de l'IA dans le domaine cyber pour plusieurs raisons :

1. L'**automatisation** de certaines tâches chronophages dans le but d'améliorer le temps de réponse et de réduire la charge de travail des analystes.
2. **L'apprentissage automatique** pour identifier des modèles récurrents.
3. Les **fonctionnalités de raisonnement** permettant de clarifier l'analyse des données, d'améliorer la modélisation de scénarios et d'anticiper des vecteurs d'attaques.

En d'autres mots, les entreprises utilisent également l'IA pour se protéger des cybermenaces.

L'objectif est de :

- **Découvrir des vulnérabilités** au niveau des infrastructures avant les malfaiteurs.
- **Détecter les attaques** : analyser les schémas d'attaques et les anomalies (analyse de logs).
- Analyser les malwares dans le but, entre autres, **d'anticiper les futures attaques et d'améliorer la réponse** (rapidité, automatisation d'une partie de la réponse, meilleur monitoring).
- Générer des exercices de gestion de crise.

5.2 L'IA au service de la criminalité

La croissance de l'intelligence artificielle a également profité aux cybercriminels qui utilisent cette technologie pour accroitre leur impact et leurs terrains de jeu. La démocratisation de l'IA et la dématérialisation de l'espace de travail des entreprises dans le cloud ont clairement augmenté la surface d'attaque des cybercriminels et l'ingéniosité dans la diversité des attaques.

Deep voice[22], deepfake[23] et automatisation des attaques permettent une rapidité de déploiement, une meilleure préparation des attaques, la possibilité de produire des attaques plus sophistiquées et, bien entendu, un terrain d'action agrandi.

L'IA est principalement utilisée pour des attaques de social engineering[24]. Dans le rapport de l'Enisa, on explique que *«l'innovation dans l'ingénierie sociale est principalement conduite par l'intelligence artificielle, spécialement depuis la sortie de ChatGPT*[25]*»*. L'IA contribue à améliorer les techniques des cyberattaques de trois manières différentes :

1. En utilisant l'IA pour créer des **mails de phishing**[26] convaincants et des messages qui reproduisent fidèlement des sources légitimes.
2. Le **deepfake** principalement utilisé pour cloner des enregistrements de voix (deep voice).
3. **L'exploration de données** basées sur l'IA.

Il est ainsi essentiel de surveiller l'intérêt des malfaiteurs pour les technologies de l'IA. Le rapport ENISA Threat Landscape 2023[27], dans son classement des menaces en cybersécurité, met en lumière l'impact des chatbots IA et plus généralement de l'IA capable de manipuler l'information.

Néanmoins, la menace la plus populaire, à ce jour, reste le **ransomware (34%)**. Viennent, ensuite, les **attaques DDoS**[28]**(28%)** et les **menaces sur les data (18%). L'IA est encore assez marginale.** Notons que les secteurs les plus ciblés sont principalement le **secteur public (19%)**, **les citoyens (11%)**, **le secteur de la santé (8%)** et enfin **les infrastructures digitales**[29] **(7%)**.

[22] Deep voice : technique utilisant l'IA pour reproduire la voix d'une personne afin de manipuler la victime.

[23] Deepfake : est une technique de synthèse multimédia reposant sur l'IA afin de créer de fausses informations.

[24] Social Engineering : stratégie utilisée par les cybercriminels pour manipuler les victimes dans le but d'obtenir des données personnelles ou sensibles.

[25] ENISA – Enisa Threat Landscape 2023.

[26] Phishing : ou hameçonnage, consiste à se faire passer pour un tiers de confiance afin de manipuler la victime pour lui voler des données personnelles (comme par exemple les codes d'accès à un compte bancaire).

[27] ENISA – Enisa Threat Landscape 2023.

[28] Attaque DDoS : (Denial-of-service attack) : attaque par déni de service qui permet d'empêcher un site web de fonctionner en envoyant un nombre important de requêtes dans le but de saturer la capacité du réseau.

[29] ENISA – Enisa Threat Landscape 2023.

CHIFFRES CLÉS

Les menaces les plus populaires sont :

% 34	Ransomware	
% 28	Attaques DDoS	
% 18	Menaces sur les data	

les secteurs les plus ciblés sont :

% 19	Secteur public
% 11	Les citoyens
% 8	Secteur de la santé

L'utilisation de l'IA est encore relativement rare au vu de la complexité de la technologie. Bien sûr, sur certaines attaques jouant sur l'humain, les stratégies de manipulation de la victime sont renforcées par des 'deepfakes' convaincants, générés par l'IA. Pour autant, les attaques classiques, se reposant sur l'exploitation simple de failles de sécurité ont encore de beaux jours devant elles sans forcément nécessiter d'IA.

VINCENT DEFRENNE
Director Cyber Strategy de la société de cybersécurité Nviso

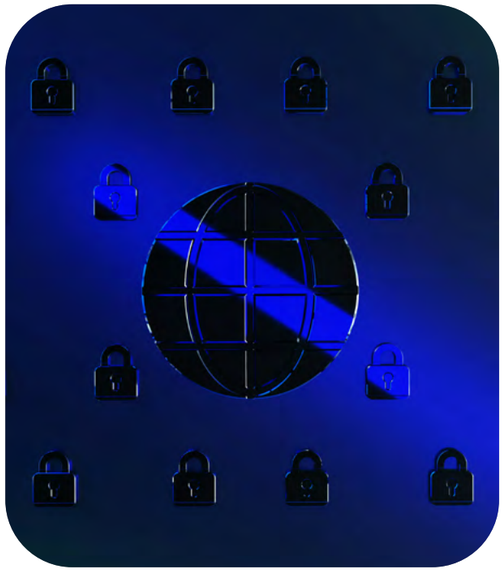
5.3 La sécurité de l'IA

Le défi majeur de cette décennie concerne l'évolution fulgurante de l'IA et ses enjeux en matière de confidentialité, d'intégrité et de disponibilité des services.

En effet, comme toute nouvelle technologie, l'IA génère son lot de nouveaux challenges en matière de sécurité. Dans ce cas, les attaques se focalisent généralement sur la corruption des données d'entrainement.

Pour fonctionner correctement et proposer des réponses pertinentes, une IA a besoin d'une grande quantité de données (les données d'entrainement). L'un des enjeux de cette technologie est la fiabilité et la neutralité de ces données. Cela est essentiel à tous les niveaux : la collecte des données, le stockage de celles-ci et le partage des informations.

La corruption de ces données d'entrainement peut susciter des **biais**[30] – injection de données biaisées (***data poisoning*** – modifier les données d'entrainement pour introduire des backdoors[31] créant des erreurs lors de la mise en production).



L'évolution récente de l'IA suscite des polémiques qui posent question en matière de protection des données. Les réflexions autour de l'intégration de l'IA dans le domaine de la cybersécurité, et inversement, sont intéressantes et requièrent une attention particulière dans l'écosystème IT belge.

Pour finir, l'un des enjeux d'actualité qui fait couler beaucoup d'encre en Europe est le besoin d'éthique avec ces questions fondamentales : comment encadrer les innovations des entreprises ? Et comment éviter les biais dans l'utilisation de ces outils numériques innovants ? Pour pallier cette difficulté, notamment dans les administrations publiques, un comité d'éthique a été créé en 2024 sous l'initiative du SPF BOSA[32]. Les objectifs de ce comité d'experts sont de :

1. Responsabiliser les services publics et les fonctionnaires.
2. Sensibiliser les fonctionnaires à l'éthique (utilisation des données et impact sur les droits des citoyens, garantir l'inclusion, la transparence et le respect des valeurs).
3. Montrer l'exemple aux citoyens via un traitement de données numériques éthique et innovant par les administrations fédérales.

[30] Les biais dans l'IA signifient que les ordinateurs ont parfois des biais parce qu'ils apprennent à partir de données injustes ou incomplètes.

[31] Backdoor : programme informatique malveillant donnant accès à un ordinateur infecté.

[32] SPF BOSA 2024 - Comité Consultatif d'Ethique des Données et de l'Intelligence artificielle de l'administration fédérale – appel à candidatures.

Comment avoir une IA qui est digne de confiance ?

Dans le contexte de la sécurité de l'intelligence artificielle, deux volets sont à prendre en compte : sécuriser l'IA car c'est une technologie avec de nouvelles vulnérabilités mais aussi utiliser l'IA pour la sécurité. Pour faire confiance à ces systèmes il faudra certainement créer un label de qualité et de fiabilité.

NOEMIE HONORÉ
Associate Partner et Responsable de Wavestone Belgique

CARTOGRAPHIE DES MÉTIERS ET DÉFIS DE LA PÉNURIE DES TALENTS

06

06 INTRODUCTION

6.1 Cartographie des métiers

Il est reconnu que les métiers de l'IT sont diversifiés et transversaux d'où la difficulté de les catégoriser de manière concrète. Dans ce chapitre, nous allons faire le point sur un panel de métiers liés à la cybersécurité et à l'intelligence artificielle.

6.1.1 Les métiers de la cybersécurité

Pour la cybersécurité, nous nous baserons sur le document produit par l'ENISA qui dresse le panorama des métiers de la cybersécurité[33].

Ce document classe les métiers de la cybersécurité en 12 catégories :

Chief Information Security Officer (CISO)
Responsable de la sécurité des services d'informations. Il met en place des stratégies pour protéger les données et les infrastructures d'une entreprise et évaluer les risques.

01

Cyber Incident Responder (CIRT)
Expert qui répond aux incidents de cybersécurité. Il repère les failles et les corrige en prévention d'une potentielle attaque, mais il propose également des solutions d'amélioration à la suite d'un incident.

02

Cyber Legal, Policy and Compliance Officer
Il s'agit du responsable et du garant de la conformité de l'entreprise des règles établies sur le plan local et international.

03

[33] ENISA - European Cybersecurity Skills framework (ECSF) - User Manual, 2022

Cyber Threat Intelligence Specialist (CTI)
Spécialiste qui commande le renseignement en cybermenace et des modes opératoires des adversaires. Il fait de la veille sur les tendances actuelles en cybermenaces et les vulnérabilités.

04

Cybersecurity Architect
Spécialiste qui construit les solutions de sécurité et les modèles architecturaux de la sécurité des systèmes d'information.

05

Cybersecurity Auditor
Il réalise des audits de sécurité et s'assure de la mise en conformité. Il se différencie du « compliance officer » par son orientation vers le contrôle de la conformité.

06

Cybersecurity Educator
Professionnel pédagogique de la cybersécurité.

07

Cybersecurity Implementer
Il se charge du développement et du déploiement des solutions en cybersécurité.

08

Cybersecurity Researcher
Il travaille dans la recherche et l'innovation dans le domaine de cybersécurité.

09

Cybersecurity Risk Manager
Il gère les risques de cybersécurité en fonction de la stratégie adoptée par l'entreprise.

10

Digital Forensics Investigator
Il enquête sur la cybercriminalité pour révéler les preuves d'une activité cybermalveillante.

11

Penetration Tester
Il évalue l'efficacité de la sécurité d'une entreprise en testant les limites du système en se comportant comme un cybercriminel.

12

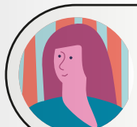
Ces métiers englobent tant les **métiers techniques** que les **métiers plus transversaux**, orientés stratégie et juridique.

Généralement, les métiers les plus populaires et « représentatifs » de la cybersécurité sont les métiers suivants : **CISO et penetration tester, etc.**, mais ils ne montrent que l'un des aspects de la cybersécurité. Comme nous l'avons vu, il existe une multitude d'autres métiers dans ce domaine contribuant à la sécurité informatique.

Les métiers plus légaux et stratégiques, liés à la mise en conformité sont de plus en plus demandés en raison de la mise en application des normes et de règlementations européennes concernant la protection des données. **Il est donc important de mettre en lumière la diversité des profils en cybersécurité.**

6.1.2 Les métiers de l'IA

Concernant les métiers de l'IA, il n'y a pas de cadres référentiels sur les métiers spécialisés, généralement **les profils suivants reviennent régulièrement dans les offres d'emploi :**

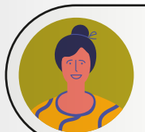


Data Scientist
Il développe les algorithmes pour importer, classer, nettoyer et analyser un set de données (structurées du type fichier Excel et non structurées du type texte libre ou vidéos).

01

Machine Learning Engineer (ML Engineer)
Son travail est fondamentalement proche de celui du Data Scientist mais le ML Engineer va concentrer son analyse sur la production de prédictions à travers les données.

02



Chief Data Officier ou Data Protection Officer
Directement lié à l'arrivée de la règlementation européenne GDPR, il s'assure que la société pour laquelle il travaille est bien en conformité avec les règlementations existantes sur la gestion des données en entreprise. Même si ce poste n'est pas directement lié à l'IA, il est essentiel et touche à ce domaine technologique.

03

Data Engineer
Il se concentre sur le management et l'organisation des données au contraire du Data Scientist qui va se focaliser sur la finalité d'analyse de données.

04

Data Analyst
Contrairement au Data Scientist, il part de données existantes et écrit les rapports d'analyse.

05

AI Developer
Il va construire les fonctionnalités de l'intelligence artificielle dans le développement d'application software.

06

6.1.3 Les profils aux doubles compétences

Il est essentiel de différencier les métiers impliqués dans la conception de l'IA de ceux qui sont formés pour son utilisation. **Le fait d'incorporer des solutions d'IA dans une entreprise ne requiert pas obligatoirement le recrutement de profils experts et techniques dans ce domaine.**

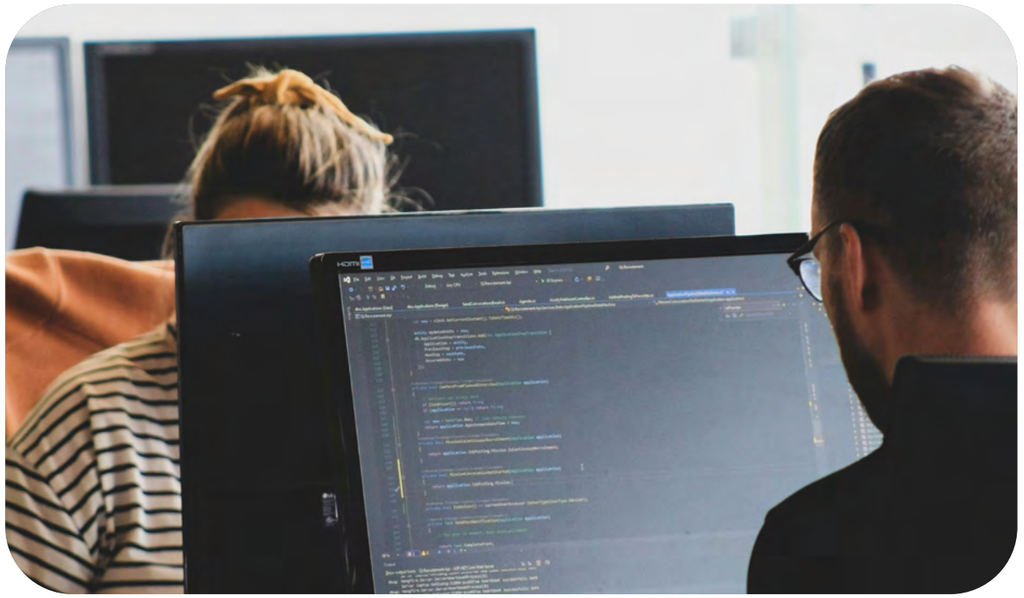
Dans le cadre de ce rapport, deux interrogations fondamentales se posent :

1. Existe-t-il une demande de profils dotés de compétences en intelligence artificielle (IA) dans le domaine de la cybersécurité ?
2. Observe-t-on une demande de recrutement de spécialistes possédant descompétences en sécurité dans le secteur de l'IA ?

Ces derniers temps, nous constatons que des offres d'emploi émergent dans les bases de données de recrutement à la recherche de profils possédant des compétences dans ces deux domaines. L'intelligence artificielle, notamment l'apprentissage automatique, est une compétence en forte demande selon l'enquête d'ISC2 sur la main-d'œuvre en cybersécurité[34]. Cette demande a augmenté de 28% depuis 2022, ce qui peut être attribué à la rapide évolution des technologies en IA depuis le début de 2023.

> *Cependant, cette compétence demeure encore relativement rare sur le marché, la demande n'est pas encore pleinement établie.*

VINCENT DEFRENNE
Director Cyber Strategy de la société de cybersécurité Nviso



[34] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

[35] AGORIA - First socio-economic study on the cyber security sector in Belgium, 2022.

[36] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

6.2 Les défis de la pénurie des talents

En ce qui concerne le marché de la cybersécurité belge, une étude d'Agoria pointe du doigt une pénurie de plus de 1 200 employés dans le secteur de la cybersécurité et même plus de 3 000 employés tous secteurs confondus en Belgique[35]. Au niveau mondial, la pénurie s'élève à 4 millions de personnes en déficit.

L'un des éléments évoqués dans une étude ISC2[36] sur la pénurie des talents dans la cybersécurité est la réduction des couts dans une économie incertaine entrainant des couts élevés pour l'entreprise ainsi qu'une réduction des salaires. Cela se matérialise par l'augmentation du délai d'implémentation de technologies, par la restructuration ou réduction de l'équipe sécurité et par la suppression des programmes de formations en sécurité. Cet enjeu a ainsi un effet de taille sur la problématique de la pénurie des talents qui touchent les métiers de la cybersécurité.

Dans son étude, ISC2 précise que le déficit de compétences peut avoir un impact plus important que l'incapacité à engager de nouveaux profils en cybersécurité. Il y a donc une nuance entre déficit de compétences et déficit de talents. C'est à ce moment-là; que la formation entre en jeu. **La pénurie des effectifs peut être en partie résolue par la formation et la sensibilisation des employés en matières de cybersécurité.** Dans cette étude, les répondants estiment que les meilleurs moyens de prévenir et d'atténuer la pénurie des effectifs en cybersécurité sont:

1. **La formation**
   72%
2. **La possibilité de fournir des conditions de travail plus flexibles**
   69%
3. **L'investissement dans la diversité, l'équité et l'inclusion**
   68%
4. **Investir dans les certifications et le recrutement de nouveau personnel**
   67%

De plus, offrir des compensations financières joue un rôle important en matière d'attractivité et de pérennité dans la société.

> **Les softs skills ont de l'importance dans ce contexte.**
>
> *Dans le domaine de l'intelligence artificielle, le grand enjeu en matière de recrutement c'est l'éthique et non la technologie. Il est plus difficile de recruter des personnes avec de bonnes compétences éthiques que des compétences techniques.*

GEOFFROY ALSTEENS
Cloud & AI Advisor chez Paradigm.brussels

> *La formation initiale et continue peut être considérée comme la meilleure des protections.*

YVES ROGGEMAN
Professeur d'informatique à l'ULB.

LA FORMATION, UN ENJEU DÉTERMINANT

07

07 INTRODUCTION

Dans l'étude 2023 de ISC2 *« How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce* [37] », on découvre que la formation a moins d'impact dans le recrutement que l'expérience professionnelle et les certifications.

C'est auprès du personnel émanant d'autres départements que la formation aura son plus grand impact. C'est bien auprès de ce public-là que les initiations à la cybersécurité prendront tout leur sens.

Avant de présenter notre réflexion sur les défis de la formation dans ce contexte, il est intéressant d'avoir un aperçu de l'offre de formation dans ces deux domaines à Bruxelles.

7.1 Cartographie des formations à Bruxelles

Voyons dans un listing non exhaustif les offres de formations disponibles à Bruxelles en IA et cybersécurité. Soulignons qu'aucune de ces formations n'est construite pour former tant à l'IA qu'à la cybersécurité. Cependant, il arrive que certaines formations abordent des notions de l'un des deux domaines sans rentrer dans le détail.

[37] ISC2 – 2023 - How the economy, skills gap and Artificial Intelligence are challenging the global cybersecurity workforce.

ULB

MASTER — 2 ANS

Master en cybersécurité à finalité conception et analyse de systèmes

(Collaboration avec École royale militaire, UCL, UNamur, Haute école Bruxelles Brabant, Haute école Ilya Prigogine)

Les + :
Legal aspect of IT security, éthique, Machine Learning et data mining, etc.

MASTER — 2 ANS — RENTRÉE 2024

Master en cybersécurité à finalité Erasmus Mundus joint master in Cybersecurity

(CYBERUS)

Les + :
Collaboration entre l'université de TalTech (Tallinn, Estonie) - aspect développement codage conception), UL (Luxembourg – aspect financier) et UBS (Lorient, France - centre français test militaire, salle de simulation d'attaques & forensics), pour l'ULB (aspect cryptologie).

MASTER — 1 AN

Master de spécialisation en science des données, Big data

Les + :
Current trends in Artificial intelligence, etc.

VUB

MASTER — 2 ANS

Master of science in applied sciences and engineering

Les + :
Dans ce master les aspects sécurité et IA sont abordés.

MASTER — 1 AN

Master – Aplied informatics : artificial intelligence

Les + :
Current trends in AI, cloud computing and Big Data processing, etc.

SUMMER TRAINING – 2023, MAIS AUSSI EN 2024?

Cybersecurity – law and practice

4 jours pour employés et étudiants.

Les + :
Cybersecurity law (EU cybersecurity laws, Nis2, Alact etc), Cybersecurity practice (firewalls, DNS & DNS attacks, etc), etc.

HAUTE ÉCOLE LÉONARD DE VINCI

BACHELIER — 3 ANS

Bachelier informatique – développement d'application

Les + :
Cours à options : Machine Learning, cybersécurité et malware, etc. (en troisième année).

BACHELIER — 1 AN

Bachelier Bussiness Data Analysis

(Collaboration avec Ephec)

Les + :
Statistique, data (récolte, gestion et visualisation), business (interprétation des data).

ERASMUS HOGESCHOOL BRUSSEL

MICRO-CRÉDIT SUR UN TRIMESTRE

Cybersecurity & ethical hacking

Les + :
Deux orientations network security et ethical hacking ou software security et ethical hacking.

1 AN APRÈS ÉTUDES

Toegepaste Artificiële intelligence

Les + :
Data science, IoT and Big Data, etc.

EPHEC

PROMOTION SOCIALE – 1 AN

Formation courte en cybersécurité

Les + :
5 cours intro, host security, incident response, network security, software security.

He2b

SPÉCIALISTE — 1 AN

Spécialiste en cybersécurité

Les + :
Niveau de spécialisation en cybersécurité.

ODISEE

SPÉCIALISTE — 1 AN

Cybersecurity specialist

Les + :
Security operations, CCNA cyberops associate certificate, security and automation, etc.

7.1.3 L'offre de formations pour adultes

DIGITALCITY.BRUSSELS AVEC BRUXELLES FORMATION

6 MOIS + 2 MOIS DE STAGE POUR CHERCHEURS D'EMPLOI

Développeur en IA

Les + :
Python, langage R pour IA, Power BI, méthodologie de projet spécifique à l'IA (agile et scrum), éthique et RGPD.

6 MOIS POUR CHERCHEUR D'EMPLOI

Cybersecurity analyst

Les + :
Cloud, analyse et test de pénétration, protocole et outils de sécurisation, réseaux, cadre légal et méthodologie (GDPR, Norme ISO2700x, gestion de crise, etc).

10 JOURS POUR CHERCHEUR D'EMPLOI

Summer school : cybersec

Les + :
Sensibilisation à la cybersécurité, étude de cas d'un déploiement d'une infrastructure Windows Server sécurisée, security gaming (tentative d'attaque et techniques de défense).

BECODE

7 MOIS POUR CHERCHEURS D'EMPLOI

Experts en data

Les + :
Initiation au Machine Learning, Deep Learning, computer vision, familiarisation au cloud.

7 MOIS POUR CHERCHEURS D'EMPLOI

Cybersecurity analyst

Les + :
System administration, networks, programming, analyst, pentest, etc.

MOLENGEEK

7 MOIS POUR CHERCHEURS D'EMPLOI

Soc analyst

Les + :
Architecture de la sécurité informatique, détection d'activité suspecte, gestion de projets en sécurité, certification Microsoft.

7 MOIS POUR CHERCHEURS D'EMPLOI

Data analyst

Les + :
Programmation Python, Machine Learning, computer vision etc.

LE WAGON

2 À 7 MOIS

Data engineer

Les + :
Fondation de la data ingénierie, management de BDD (data warehouse), data pour la visualisation, optimisation du volume de travail des data, etc.

2 À 7 MOIS

Data science and IA

Les + :
Python, Machine Learning, Deep Learning, ML engineering, generative AI, etc.

2 À 7 MOIS

Data analytics

Les + :
Fondation, SQL, extraction, data visualization, etc.

FARI (AI FOR THE COMMON GOOD)

Les + :
FARI AI Academy (pour cadres, troisième cycle, formation de formateurs), l'IA pour les DPD.

7.1.3 L'offre de formations pour adultes

Pour notre public d'entreprises, notre offre de formation en IA et cybersécurité est disponible dans notre catalogue de formation. Voici en lumière quelques formations intéressantes : techniques de l'intelligence artificielle ; applications et développement, Data science, Machine Learning avec Python, Cybersecurity fundamentals, analyse forensics, éviter le hacking sensibilisation à la sécurité informatique, etc[38].

Les écoles de coding bruxelloises ont également pris en marche le train de l'innovation et présentent désormais une offre de formation en cybersécurité et en IA.

7.1.4 Formation à Bruxelles : les défis

L'intelligence artificielle et la cybersécurité sont des thématiques populaires surtout dans le secteur de la formation. **Le véritable défi réside dans l'adaptation constante des programmes existants à la réalité du marché de l'emploi.** Cette adaptation nécessite une approche interdisciplinaire intégrant des compétences multiples en informatique, statistique, juridique, en stratégie et, bien sûr, de spécialisations en cybersécurité et IA.

Ce n'est pas tout. Pour aller au bout de cette démarche interdisciplinaire, il est important d'amorcer **un rapprochement entre les entreprises et le monde académique**. Cette relation doit être renforcée pour permettre aux organismes de la formation de s'adapter aux réalités et besoins des entreprises qui recrutent.

> *« Il est impératif de créer des liens entre les entreprises et les organismes de formation qui le prennent en compte comme AI4belgium et la Cybersecurity Coalition.*

AXEL LEGAY
Professeur à l'UCLouvain

Dans ce contexte, **Digitalcity.brussels, plateforme des métiers et de la formation à Bruxelles doit se positionner comme acteurs de ces rapprochements.** Il nous faut agir comme un pont solide et fiable. Il est nécessaire de sensibiliser les chefs d'entreprises aux enjeux de recrutement et de mener un travail collaboratif avec les entreprises pour que notre offre corresponde davantage à leurs enjeux et besoins en matière de recrutement.

En effet, aujourd'hui, et ce, malgré la pénurie croissante dans le secteur de la cybersécurité, il y a encore trop d'entreprises qui recherchent des profils surdiplômés quand bien même cela n'est pas toujours nécessaire. Les profils très diplômés et qui combinent des compétences approfondies en IA ou en cyber sont bien entendu essentiels dans des domaines très technologiques. Dans la plupart des cas, des profils moins diplômés, mais qualifiés sont largement suffisants.

Il est ainsi crucial de **privilégier la flexibilité des programmes et la complémentarité des offres de formations à Bruxelles.** Notre région se distingue par une offre de formation très diversifiée dans le domaine du digital, adaptable à tous les profils d'apprenants. C'est ce qui fait la force de Bruxelles, mais **il est essentiel de mettre les ressources en commun pour créer une offre couvrant le plus de profils**.

Parallèlement, un autre défi réside dans le **développement et la multiplication des formations en IA et cybersécurité** au vu des besoins de recrutement des entreprises. À Bruxelles, bien que ces formations se soient multipliées ces dernières années, **l'offre reste encore trop incomplète par rapport aux besoins du marché**.

D'autant plus que dans le milieu universitaire, par exemple, *« trop peu d'étudiants s'inscrivent dans les filières technologiques et leur nombre diminue au fil des années »* nous transmet **Yves Roggeman**, professeur d'informatique à l'ULB. Comment peut-on expliquer ce phénomène d'abandon de la formation ? S'agit-il d'un problème d'image d'un secteur, de représentation des métiers, un problème de compétences de bases ? Chez Digitalcity.brussels, ce constat nous interpelle. Dans le cadre de ses missions, en tant que pôle Formation-Emploi aux métiers du numérique, Digitalcity.brussels doit pouvoir contribuer à trouver les réponses à ces questionnements. Pourquoi ces étudiants abandonnent-ils leur orientation d'études en cours de route ? Comment déterminer de manière fiable la ou les raisons de ce changement ?

[38] Retrouvez toutes ces formations ainsi que d'autres dans notre catalogue de formations à destination des entreprises sur notre site web : Digitalcity.brussels.

CONCLUSION

08

08 INTRODUCTION

L'intelligence artificielle et la cybersécurité sont les deux grandes tendances technologiques du moment.

Depuis l'avènement de ChatGPT et d'autres systèmes de GenAI, l'intelligence artificielle continue de croitre à une vitesse exponentielle et acquiert une influence économique considérable. Du côté de la cybersécurité, les menaces s'intensifient de manière alarmante et les entreprises qui doivent faire face à ces attaques sont de plus en plus nombreuses et vulnérables.

L'utilisation de l'intelligence artificielle dans le domaine de la cybersécurité demeure encore peu répandue en Belgique. Cependant, l'interconnexion entre les deux domaines n'est pas à négliger. Chaque entreprise proposant des services de cybersécurité explore l'opportunité d'intégrer l'IA pour évaluer son efficacité.

Du côté des cybercriminels, l'utilisation de l'IA reste marginale, car les escroqueries classiques demandant moins d'expertises, continuent de progresser. Il est donc prématuré d'affirmer que l'IA aura un impact significatif sur la cybercriminalité.

Ce qui est certain, c'est que de plus en plus d'entreprises, au-delà du secteur de la cybersécurité, intègrent l'IA dans leurs processus de gestion pour optimiser leurs opérations. L'enjeu de l'interconnexion de l'IA et de la cybersécurité pour les entreprises se trouve dans ce point. Car l'IA a ses faiblesses de sécurité. Particulièrement, la sécurité liée à l'IA suscite de nombreuses réflexions. L'IA étant une technologie émergente, sa démocratisation souligne l'importance de structurer rapidement la sécurité des données.

Aussi, avec l'officialisation du AI Act, il est évident que les gouvernements européens doivent élaborer une stratégie robuste, mettant l'accent sur la sécurisation des données, notamment sur les données d'entrainement, les problèmes de biais, les sources des données, la gestion des données personnelles et confidentielles, etc.

Dans ce contexte, la recherche de profils en IA et cybersécurité est en augmentation. Cependant, les profils combinant les deux domaines de compétences restent encore rares et orientés vers la recherche et l'innovation.

En ce qui concerne l'offre de formation dans ces deux domaines, elle s'est développée à Bruxelles ces dernières années. Néanmoins, plusieurs défis majeurs méritent d'être soulignés :

1. Malgré les évolutions réalisées, il subsiste un **besoin pressant d'augmenter le nombre de programmes de formation disponibles** pour répondre à la demande croissante dans ces domaines spécifiques.
2. Un effort considérable reste à déployer pour **sensibiliser les jeunes**, particulièrement ceux en période de choix d'orientation professionnelle.
3. La **mise en avant de la diversité des offres de formation disponibles** à Bruxelles constitue un troisième aspect crucial.

Dans la construction de son offre de formation et de sensibilisation, Digitalcity.brussels, en tant que pôle Formation-Emploi de la région Bruxelles-Capitale, est vigilant envers ces trois défis.

Dans le paysage de la formation à Bruxelles, notons l'absence de besoins spécifiques de formations construites pour couvrir à la fois l'IA et la cybersécurité. Bien que le domaine reste relativement « niche » à l'heure actuelle, il y a une multitude de prises de parole de la part des experts et des entreprises de l'IA et de la cybersécurité. Il reste donc important de suivre l'évolution de cette thématique dans un contexte de besoins émergents.

LES PROJETS DE DIGITALCITY. BRUSSELS

09

09 CONCLUSION

Pour conclure ce rapport, Digitalcity.brussels a envisagé la mise en œuvre d'actions concrètes en réponse aux constats spécifiques énoncés tout au long de ce rapport. Ces actions s'inscrivent ainsi dans le cadre de ses missions liées à la formation, à l'emploi et à la sensibilisation.

À travers ces projets, Digitalcity.brussels souhaite créer des vocations dans les domaines de l'IA et de la cybersécurité auprès des chercheurs d'emploi et des jeunes. Le PFE (Pôle Formation-Emploi) souhaite également comprendre les enjeux en matière d'emploi et de formation de la part des entreprises qui investissent dans ces deux secteurs d'activités et être actifs dans la résolution des problématiques soulevées par ce sujet.

Voici les actions qui seront mises en place dès 2024-2025 :

connexion

9.1 COMPRENDRE les besoins

Pour être en phase avec les réalités du marché de l'emploi des entreprises recruteuses de profils IT, Digitalcity.brussels mettra en place une enquête à destination de ces entreprises avec l'objectif d'évaluer l'évolution de leurs besoins en matière de métiers et de formations. Il sera également proposé à ces entreprises de participer activement à la collaboration de la veille chez Digitalcity.brussels dans le but d'adapter son offre aux réalités du marché du travail IT bruxellois sous la forme d'un comité d'experts de consultation.

Lancement d'une enquête de besoins auprès des entreprises bruxelloises

1. **Objectifs :** déterminer les besoins émergents en matière d'évolution des métiers et des besoins de formations auprès des entreprises de Bruxelles. Ce projet fait écho aux constats évoqués dans le précédent rapport de veille de Digitalcity.brussels : digitalisation des PME bruxelloises[39].
2. **Publics :** entreprises bruxelloises.
3. **Calendrier :** lancement de la première enquête en 2025 – récurrence tous les deux ans.

Création d'un comité d'experts pour la veille

1. **Objectifs :** solidifier la relation entre Digitalcity.brussels et les entreprises IT de Bruxelles sur la question des métiers et des formations. Avec des possibilités de partenariats win-win (adaptation de formations aux besoins de l'entreprise sous la formation de Parcours Formation-Emploi, sponsoring d'évènements Digitalcity.brussels, mise en visibilité dans la communication de Digitalcity.brussels)
2. **Publics :** entreprises et experts
3. **Modalité de fonctionnement :** établissement du comité et consultations diverses dans le cadre des projets et réflexions autour des thématiques annuelles.
4. **Calendrier :**
   2024 : constitutions du comité et de la méthodologie.
   2025 : début des consultations.

[39] Digitalcity.brussels – publications : Digitalisation des PME bruxelloises : relevez les défis ensemble avec Digitalcity.brussels.

9.2 FORMER et adapter la formation

Digitalcity.brussels en tant que pôle Formation-Emploi des métiers du numérique tient à proposer auprès de son public de chercheurs d'emploi et d'entreprises des formations qui correspondent aux réalités métiers du secteur IT. C'est dans ce contexte que nous développons au fil des ans notre offre dans les deux domaines tendance et en pleine évolution de l'IA et de la cybersécurité.

Formations et élaboration du catalogue annuel

1. **Objectifs :** poursuivre une réflexion autour de la création de formations en phase avec les besoins en IA et cybersécurité, mais également dont la forme pédagogique de transmission des compétences est innovante et adaptée aux publics visés. Dans le cadre de cette réflexion, un constat est important à garder à l'esprit : Bruxelles est majoritairement composée de PME. Une bonne partie utilise les technologies pour améliorer leur productivité et rentabilité. Nous travaillons donc majoritairement en contact avec des petites entreprises à Bruxelles qui ne sont pas forcément sensibilisées aux enjeux cybersécurité et IA. Digitalcity.brussels renforcera et mettra en avant son offre de formation de sensibilisation/initiation à destination des employés.
   → Par exemple : cybersecurity fundamentals, évitez le hacking, prompt engineering.
2. **Publics :** chercheurs d'emploi, entreprises (dont des PME).

9.3 SENSIBILISER et informer

En complément d'une offre de formation en constante évolution et l'analyse des besoins des entreprises, la sensibilisation est un objectif essentiel dans le cadre des missions de Digitalcity.brussels.

Évènement : TechQuest

1. **Objectifs :** synergie des organismes de formation et des entreprises du secteur IA et cyber pour offrir des perspectives et vocations sur les métiers d'avenir du digital. Sensibilisation aux métiers de l'IA et de la cybersécurité.
2. **Publics :** jeunes chercheurs d'emploi, stagiaires de formations, personnes intéressées par ces thématiques qui souhaitent découvrir la diversité des débouchés professionnels.
3. **Calendrier :** 15 octobre 2024
4. **Modalité de fonctionnement :** ateliers d'initiation aux métiers de la cybersécurité et de l'intelligence artificielle. Ateliers destinés à un public de novices qui hésitent à se lancer dans ces carrières, mais également de stagiaires en cours de formation d'initiation dans ces domaines. Ces ateliers seront complétés par des témoignages et démonstrations qui apportent un aperçu des métiers dans ces domaines.

Séance d'information (SI) : focus sur la pénurie des métiers de la cybersécurité et de l'IA

1. **Objectifs :**
   - Démystifier les métiers de l'IT et promouvoir la diversité des métiers et la diversité des compétences dans les métiers techniques.
   - Présenter Digitalcity.brussels et ses missions.
   - Aider les agents des maisons de l'emploi dans leurs conseils.
2. **Publics :** chercheurs d'emploi et agents des organismes de formation et métiers.
3. **Calendrier :**
   2024 : séance d'information à destination des organismes de l'emploi et formation. Récurrence : 2 par an.

NOS EXPERTS

Pour construire ce rapport, nous avons fait appel à des experts lors d'entretiens individuels pour recueillir leur avis sur les sujets développés dans le travail d'analyse. Nous les remercions pour leur contribution et le temps qu'ils nous ont accordé.

NATHANAEL ACKERMAN
Chief Evangelist Officer - IA4Belgium

GEOFFROY ALSTEENS
Cloud and AI Advisor - Paradigm.brussels

GEORGES ATAYA
Professor - Solvay Brussels School

GUNTHRAM CORNERLIS
Program Manager Digital Business - Sirris

VINCENT DEFRENNE
Director Cyber Strategy & Architecture - Nviso

ALICE DEMARET
AI Impact Advisor - ULB

FRANCK DUMORTIER
Chercheur - VUB

NOÉMIE HONORÉ
Associate Partner et Responsable Wavestone Belgique

JEAN KERVYN
Project Manager - CCB

AXEL LEGAY
Professeur et Fondateur de Cyberwal by digital Wallonia – UCL/ CyberWal

YVES ROGGEMAN
Professeur en informatique - ULB

ERIC VAN CANGH
Senior Business Group Leader Digital - Agoria

Digitalcity.brussels

Pôle Formation Emploi des métiers du numérique

Digitalcity Brussels
Rue Jules Cockx 6
1160 Bruxelles
02 475 20 00
info@digitalcity.brussels
www.digitalcity.brussels

CRÉDITS ET MENTIONS LÉGALES

DIRECTION & EDITEUR
Jean-Pierre Rucci
jp.rucci@digitalcity.brussels

VEILLE & REDACTION
Christina Galouzis
christina.galouzis@digitalcity.brussels

DESIGN & COMMUNICATION
Noémie Valcauda
noemie.valcauda@digitalcity.brussels

TRADUCTION
Luc Huygh
luc.huygh@digitalcity.brussels

POST-PRODUCTION
Noémie Valcauda - Luc Huygh

CRÉDITS PHOTOGRAPHIQUES
Unsplash.com

CONCEPTION & MISE EN PAGE
PointRelay
vincent@pointrelay.be

Est une initiative de

actiris.brussels
BRUXELLES FORMATION former pour l'emploi
VDAB
AGORIA
Beci
SETCa-BBTK FGTB-ABVV
CNE L'avenir a son syndicat
CGSLB ACLVB

Avec le soutien de

RÉGION DE BRUXELLES-CAPITALE BRUSSELS HOOFDSTEDELIJK GEWEST
Francophones Bruxelles
béliris POUR BRUXELLES VOOR BRUSSEL
Avec le soutien du Fonds social européen
Met de steun van het Europees sociaal fonds