
Métiers de la cybersécurité : analyse selon le genre

Auteur : Tilman, Camille

Promoteur(s) : Cornet, Annie

Faculté : HEC-Ecole de gestion de l'Université de Liège

Diplôme : Master en sciences de gestion, à finalité spécialisée en stratégie et management des ressources humaines

Année académique : 2022-2023

URI/URL : <http://hdl.handle.net/2268.2/18872>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.



MÉTIERS DE LA CYBERSECURITY : ANALYSE SELON LE GENRE

Jury :

Promoteur :

Annie CORNET

Lecteurs :

Giseline RONDEAUX

Eddy HEINS

Mémoire présenté par

Camille TILMAN

En vue de l'obtention du diplôme de

Master en sciences de gestion, à

finalité spécialisée en stratégie et

management des ressources

humaines

Année académique 2022/2023

Tout d'abord, je tiens à remercier ma promotrice, Madame Annie Cornet, pour sa bienveillance et pour la suggestion du thème de ce mémoire.

J'adresse mes sincères remerciements à Madame Sandra Denghien, présidente du flux de main-d'œuvre dans le domaine de la cybersécurité chez Women4Cyber Belgium et Laurent Minne, fondateur de la Communauté pour la Cybersécurité en Belgique, Be.Cyber, pour leurs précieux conseils, leur temps et leur aide dans la recherche de travailleurs en cybersécurité et de professionnels en ressources humaines.

Je remercie également toutes les personnes interviewées pour leur disponibilité et leur implication dans ma recherche ainsi que pour la sympathie qu'ils m'ont accordée.

Je tiens à remercier ma sœur, Madame Aline Tilman et Monsieur Nathan Sépul pour la relecture de ce mémoire et leur soutien inconditionnel.

Enfin, je remercie mes parents, Madame Carine Vermeerbergen et Monsieur Pierre Tilman, mon parrain, Monsieur Christophe Orban et toutes les personnes de ma famille pour leur soutien et leurs encouragements tout au long de la réalisation de ce travail.

Résumé

Le secteur de la cybersécurité est en pleine expansion, surtout depuis la crise du COVID-19. En 2028, son chiffre d'affaire devrait atteindre 257 milliards de dollars US¹. Cependant, le secteur est en manque significatif de main-d'œuvre. Les entreprises tentent de combler le déficit mondial de 3,4 millions de travailleurs en cybersécurité² ((ISC)², 2022). Cette pénurie affecte autant les entreprises que la société en général. Les formations et les métiers dans le domaine de la cybersécurité sont divers et variés. Ils répondent à l'aspect multidisciplinaire de la cybersécurité. Pour travailler en cybersécurité, les candidats ont besoin tant de compétences techniques que de compétences non techniques. Les métiers de la cybersécurité requièrent autant de connaissances approfondies en *“architecture de sécurité de l'information ; gestion des risques et conformité; et en analyse du renseignement/de la menace”* (Caldwell, 2013, p. 6) que de connaissances en sciences sociales, sciences politiques et management. Pour exceller, les employés doivent aussi avoir un panel de *soft skills* telles que la curiosité, le sens éthique, la collaboration et la flexibilité.

Pour résorber ce déficit de main-d'œuvre, les entreprises sont encouragées à se tourner vers un bassin de candidats sous-exploités : les femmes. En effet, les femmes ne représentent que 24%³ de l'effectif en cybersécurité alors qu'elles représentent 50%⁴ de la population active mondiale. Ce faible ratio est dû à plusieurs barrières mises sur les chemins des femmes tels que la rémunération, l'image perçue du secteur de la cybersécurité, les constructions sociales, le harcèlement et la discrimination. L'avenir de la cybersécurité dépend de sa capacité à attirer, retenir et promouvoir les femmes (Poster, 2018). Pour ce faire, la littérature donne quelques pistes comme les mouvements promouvant les femmes dans la cybersécurité, la création d'une culture plus inclusive dans le monde scolaire et universitaire, une modification du processus de recrutement et une mise-à-jour de l'image de la cybersécurité. De plus, la diversité est devenue un élément essentiel à la réussite des entreprises. 97%⁵ des entreprises interrogées par Forbes ont développé des stratégies formelles de diversité et d'inclusion. Des entretiens réalisés auprès de quinze professionnels de la cybersécurité en Belgique permettent d'étayer les particularités du monde de la cybersécurité et de sa main-d'œuvre ainsi que l'importance d'investir dans la diversité et, notamment, dans la représentation des femmes dans la cybersécurité.

¹ Nguyen, P-H. (2023). Cybersecurity - Market data Analysis & Forecasts | Statista. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

² Ibid.

³ (ISC)². (2018). Women in Cybersecurity : Young, Educated and Ready to Take Charge. (ISC)². p.4 <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38>

⁴ Gammarano, R. (2019). 100 statistiques sur l'OIT et le marché du travail pour célébrer le centenaire de l'OIT. ILOSTAT. point 62 <https://ilostat.ilo.org/fr/100-statistics-on-the-ilo-and-the-labour-market/>

⁵ *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce.* (2021). Forbes Insight. p.11

Abstract

The cybersecurity sector is booming, especially since the COVID-19 crisis. By 2028, its turnover is expected to reach 257 billion US dollars⁶. However, there is a significant shortage of labour in the sector. Companies are trying to make up the global shortfall of 3.4 million cybersecurity workers⁷ ((ISC)², 2022). This shortage affects both businesses and society in general. Cybersecurity training and careers are diverse and varied. They reflect the multidisciplinary nature of cybersecurity. To work in cybersecurity, candidates need both technical and non-technical skills. Cybersecurity jobs require in-depth knowledge of "*information security architecture; risk management and compliance; and intelligence/threat analysis*" (Caldwell, 2013, p. 6) as well as knowledge of social sciences, political science and management. To excel, employees also need a range of soft skills such as curiosity, ethics, collaboration and flexibility.

To make up for this labour shortage, companies are being encouraged to turn to an under-exploited pool of candidates: women. Women account for only 24%⁸ of the cybersecurity workforce, whereas they represent 50%⁹ of the world's working population. This low ratio is due to a number of barriers standing in the way of women, such as pay, the perceived image of the cybersecurity sector, social constructs, harassment and discrimination. The future of cybersecurity depends on its ability to attract, retain and promote women (Poster, 2018). To do this, the literature gives a few avenues such as movements promoting women in cybersecurity, creating a more inclusive culture in schools and universities, changing the recruitment process and updating the image of cybersecurity. What's more, diversity has become an essential element in the success of companies. 97%¹⁰ of the companies surveyed by Forbes have developed formal diversity and inclusion strategies. Interviews with fifteen cybersecurity professionals in Belgium highlight the particularities of the world of cybersecurity and its workforce, as well as the importance of investing in diversity and, in particular, in the representation of women in cybersecurity.

⁶ Nguyen, P-H. (2023). Cybersecurity - Market data Analysis & Forecasts | Statista. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

⁷ Ibid.

⁸ (ISC)². (2018). Women in Cybersecurity : Young, Educated and Ready to Take Charge. (ISC)². p.4 <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38>

⁹ Gammarano, R. (2019). 100 statistiques sur l'OIT et le marché du travail pour célébrer le centenaire de l'OIT. ILOSTAT. point 62 <https://ilostat.ilo.org/fr/100-statistics-on-the-ilo-and-the-labour-market/>

¹⁰ *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce*. (2021). Forbes Insight. p.11

Liste des figures

Figure 1 : Votre équipe cybersécurité a-t-elle embauché de nouvelles personnes pour soutenir votre département cette année ?.....	6
Figure 2 : Industries demandant des professionnels en cybersécurité.....	7
Figure 3 : Niveaux de spécialisation en cybersécurité.....	9
Figure 4 : Orientation des études des cyber-professionnels.....	11
Figure 5 : Qualification minimum requise pour un emploi dans la cybersécurité.....	12
Figure 6 : Le plus haut niveau d'étude atteint en fonction du genre.....	13
Figure 7 : Exemples de différentes certifications (Furnell, 2021, p.3).....	15
Figure 8 : Les compétences requises pour s'épanouir en cybersécurité selon différents rôles (Tessian, 2021, p.8).....	16
Figure 9 : Fiche métier des experts en cybersécurité adaptée (Indeed, 2023).....	17
Figure 10 : Les savoirs, compétences et aptitudes non techniques des rôles techniques en cybersécurité selon le modèle NICE [Traduction libre].....	19
Figure 11 : Nombre total d'individus ayant obtenu une qualification dans le domaine des TIC en fonction du genre (OECD Stat, 2020).....	22
Figure 12 : Nombre total de diplômés des pays de l'OCDE et leur filière d'étude en fonction du degré et de leur genre (OECD Stat, 2020).....	23
Figure 13 : Parcours professionnels en cybersécurité (Cyber Seek, 2023).....	25
Figure 14: Distribution du genre en fonction du poste ((ISC) ² , 2018, p.7).....	26
Figure 15 : Les hommes et les femmes font le même travail ((ISC) ² , 2018, p.9).....	27
Figure 16 : Nombre d'années d'expériences requises pour un emploi en cybersécurité sur le marché sud-africains (Parker et Brown, 2019, p. 186).....	27
Figure 17 : Proportion de travailleurs en cybersécurité en fonction de l'âge et du genre ((ISC) ² , 2022, p.39).....	29
Figure 18 : Types de discriminations reportées (Poster, 2018, p.578).....	30
Figure 19 : Les femmes plus jeunes connaissent moins d'inégalités salariales ((ISC) ² , 2018, p.6).....	31
Figure 20: Comment attirer des femmes dans les professions de la cybersécurité? (Tessian, 2021, p.9)	34
Figure 21 : Le top trois des priorités de carrière des femmes selon leur région (Panhans et al., 2022)...	35
Figure 22 : Les différents chapitres de Women4Cyber (Brugman, 2022, p.4).....	35
Figure 23 : Les flux de travail de Women4Cyber (Women4Cyber, 2022).....	36
Figure 24 : Nombre d'étudiantes servies par programme (Girls Who Code, 2022, p.3).....	37
Figure 25 : Présence de Girls Who Code à travers le monde(Girls Who Code, 2022, p.4).....	37
Figure 26 : Résultats à court terme de leur programme pour les étudiantes universitaires (Girls Who Code, 2022, p.7).....	37
Figure 27 : L'expérience des femmes au sein de leur entreprise du domaine de la technologie (Accenture & Girls Who Code, 2019, p.17).....	39
Figure 28 : Doubler le nombre de femmes en tech d'ici 2030 (Accenture & Girls Who Code, 2019, p.22).....	39
Figure 29 : Actions pouvant retenir les femmes dans leur emploi dans la technologie (Accenture &	

Girls Who Code, 2019, p.26).....	40
Figure 30 : l'expérience des femmes en STIM à l'université (Accenture & Girls Who Code, 2019, p.13). 43	
Figure 31 : Programme actuellement en place dans les entreprises afin de développer une main-d'oeuvre diversifiée (Forbes Insight, 2021, p.9).....	45
Figure 32 : Evaluation des entreprises par leur employés en termes de diversité de genre ((ISC) ² , 2022, p.43).....	46
Figure 33 : Ressenti des employés en cybersécurité par rapport à la DEI au sein de leur entreprise en fonction du genre et de la tranche d'âge ((ISC) ² , 2022).....	47

Liste des abréviations

US	Américain
(ISC) ²	International Information Systems Security Certification Consortium
CCB	Centre pour la Cybersécurité Belgique
RSSI	Responsable de la sécurité des systèmes d'information
OCDE (anglais : OECD)	Organisation de Coopération et de Développement Economiques (anglais : Organization for Economic Cooperation and Development)
TIC	Technologies de l'Information et de la Communication
STIM	Sciences, Technologie, Ingénierie et Mathématiques
W4C	Women4Cyber
Tech	Le secteur des technologies

Table des matières

Résumé.....	4
Abstract.....	5
Introduction.....	1
Chapitre 1 : revue de littérature.....	3
1. La cybersécurité.....	3
1.1. Définition.....	3
1.2. Le marché de la cybersécurité.....	4
1.2.1. Le marché du travail en cybersécurité : une pénurie de main-d'oeuvre.....	6
2. Les métiers et les compétences requises en cybersécurité.....	8
2.1. Les études et certificats.....	8
2.1.1. Les études et formations en Belgique.....	9
2.1.2. Les certificats reconnus venant d'organismes privés.....	13
2.2. Les compétences.....	15
2.1.1. Les compétences techniques.....	16
2.1.2. Les compétences non techniques.....	17
2.1.2.1. Passion, curiosité et formation continue.....	19
2.1.2.2. Travail d'équipe.....	19
2.1.2.3. Sens éthique irréprochable.....	20
2.1.2.3. Penseurs systémiques.....	20
2.1.2.4. Communication et présentation.....	20
2.1.2.5. Formateur.....	20
2.1.2.5. Leadership et influence sociale.....	21
2.1.2.5. Flexibilité et adaptabilité.....	21
2.1.3. La divergence des compétences en fonction du genre.....	21
2.3. Les métiers.....	24
2.3.1. La représentation des genres selon l'emplois.....	26
2.4. L'expérience.....	27
3. La situation des femmes en cybersécurité.....	28
3.1. Les freins à la diversité de genre.....	30
3.1.1. La rémunération.....	30
3.1.2. La cybersécurité, c'est pour les hommes.....	31
3.1.3. L'accès aux études STIM, le choix de carrière et les constructions sociales.....	32
3.1.4. Le harcèlement et la discrimination.....	33
3.2. Les pistes pour remédier au problème de représentation du genre.....	34
3.2.1. Les communautés de femmes dans la cybersécurité.....	35
3.2.2. La création d'une culture plus inclusive.....	38
3.2.3. Le recrutement : ouvrir les portes à différents talents.....	40
3.2.4. Le développement de modèles féminins au sein de l'industrie.....	41
3.2.5. La visibilité sur les différentes compétences nécessaires en cybersécurité.....	41

3.2.6. L'évolution des établissements d'enseignement supérieur.....	42
3.2.7. Le changement de la perception des femmes en ce qui concerne la cybersécurité... 43	
4. Investir dans la diversité.....	44
4.1. Investir dans la diversité de genre.....	45
4.2. La diversité au service du recrutement et de la rétention.....	46
Chapitre 2 : partie empirique.....	48
1. Méthodologie.....	49
2. Présentation des résultats.....	50
2.1. Les études.....	50
2.2. La présence des femmes dans le secteur de la cybersécurité belge.....	51
2.3. Les compétences et les traits de caractères requis pour travailler en cybersécurité.....	53
2.4. Les relations au travail.....	55
2.5. Les initiatives pour promouvoir les femmes dans la cybersécurité.....	57
2.6. Les recommandations pour un environnement de travail inclusif.....	61
2.7. La diversité de genre au sein des équipes.....	63
3. Discussion.....	63
4. Recommandations.....	67
5. Conclusion.....	69
Bibliographie.....	70

Introduction

Ces dernières années, la cybersécurité est devenue un sujet de premier plan dans les médias, souvent suscitée par des violations de divers systèmes d'information, tels que les compagnies aériennes, les organismes de santé, les agences de crédit, les administrations, les institutions financières, les opérateurs de télécommunications, et bien d'autres encore (EU, 2017 cité dans Blažič, 2021). Pendant un certain temps, la cybersécurité était considérée comme un défi des technologies de l'information et de la communication (TIC), plutôt qu'un risque commercial. Cependant, avec les attaques cybernétiques et les pertes subies par de nombreuses entreprises, gouvernements et particuliers, cette perception a commencé à changer (Blažič, 2021). La protection des données et des infrastructures est devenue une priorité majeure. Le marché mondial de la cybersécurité a connu une croissance robuste au cours des dernières années, avec un chiffre d'affaires passant de 83 milliards de dollars US en 2016¹¹ à 162 milliards de dollars US en 2023¹². Ce dernier devrait atteindre un chiffre d'affaires d'environ 257 milliards de dollars d'ici 2028¹³ (Nguyen, 2023).

Cependant, le secteur de la cybersécurité rencontre un besoin énorme de main-d'œuvre. De fait, les organisations tentent de combler le déficit mondial de 3,4 millions de travailleurs en cybersécurité¹⁴ ((ISC)², 2022). Parmi les nombreux facteurs pouvant causer ce déficit, l'un des éléments les plus intrigants et pertinents de cette dynamique est la représentation des femmes dans le domaine de la cybersécurité. Bien que des initiatives aient été mises en place pour développer l'égalité de genre dans de nombreux secteurs, celui de la cybersécurité reste largement dominé par les hommes, créant ainsi des déséquilibres potentiels en termes de compétences, de perspectives et de solutions innovantes. Pour ces raisons, la diversité est un enjeu que les entreprises commencent à prendre de plus en plus au sérieux. Les liens entre diversification des équipes et amélioration de la productivité sont prouvés par des nombreuses recherches. Presque toutes les entreprises de l'enquête de Forbes Insight (2021) (97%¹⁵) ont développé des stratégies formelles de diversité et d'inclusion.

Ce mémoire explore la relation entre la cybersécurité et la représentation des femmes dans ce domaine. Dans un premier temps, ce travail décrit le monde de la cybersécurité, tant son marché, les études et compétences requises que les métiers relatifs au secteur. Ensuite, il vise à comprendre les différents enjeux se rapportant à la diversité de genre dans ce domaine en analysant les raisons derrière cette sous-représentation des femmes, les implications de cet écart et comment y remédier. En mettant en évidence les avantages potentiels d'une représentation plus équilibrée des femmes en

¹¹ Statista. (s. d.). *Cybersecurity - Worldwide* | Statista market forecast. <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

¹² Nguyen, P-H. (2023). *Cybersecurity - Market data Analysis & Forecasts* | Statista. Statista. p.16 <https://www.statista.com/study/124902/cybersecurity-report/>

¹³ Nguyen, P-H. (2023). *Cybersecurity - Market data Analysis & Forecasts* | Statista. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

¹⁴ (ISC)². (2022). *Cybersecurity Workforce Study*. p.3. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

¹⁵ *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce*. (2021). Forbes Insight. p.11

cybersécurité, je souhaite contribuer au développement de la réflexion d'une meilleure cybersécurité, plus robuste et inclusive.

Cette recherche s'appuiera sur une analyse de la littérature existante ainsi que sur quinze entretiens réalisés auprès de différents acteurs de la cybersécurité en Belgique. Ce mémoire a pour but de favoriser des discussions ainsi que des actions concrètes permettant de développer une main-d'œuvre performante et prête à répondre à tous les défis de l'ère numérique.

Chapitre 1 : revue de littérature

1. La cybersécurité

La cybersécurité est un domaine transverse, essentiel pour protéger le patrimoine numérique de l'individu, des organisations et de l'Etat. Son enjeu est stratégique, au carrefour de sujets d'actualité passionnants et indissociables de changement (Cercle des Femmes de la Cybersécurité, 2019). La transformation numérique de notre société est en train de changer radicalement la manière dont les systèmes informatiques sont utilisés. Une grande partie de la population est connectée en permanence à Internet, utilisant un nombre important de services. Simultanément, nous sommes exposés en permanence à des attaques : nos données personnelles peuvent être volées, modifiées ou détruites. Nous courons également le risque de divulguer par erreur et de façon irréversible nos données personnelles sur Internet. Les entreprises, les États et leurs infrastructures critiques, qui sont aujourd'hui interconnectés, sont également vulnérables. Les dommages économiques et sociétaux des cyber attaques réussies peuvent être considérables. La cybersécurité est ainsi devenue une préoccupation générale pour tous, citoyens, professionnels et décideurs (Kremer et al., 2019 ; Nguyen, 2023).

1.1. Définition

La cybersécurité peut se définir comme le processus qui assure et maintient la confidentialité, l'intégrité, la disponibilité et la protection de la vie privée. Elle a pour but d'identifier les menaces potentielles et d'élaborer des politiques de sécurité pour contrer ces menaces. Ces dernières peuvent viser différents aspects tels que le matériel, le réseau, le système d'exploitation, les applications ou même les utilisateurs¹⁶ (Kremer et al., 2019 ; Nguyen, 2023). Cependant, la cybersécurité est un domaine vaste et en constante évolution. La définition de ce domaine n'est donc quasiment jamais la même en fonction de la source utilisée. Au travers d'un processus de groupes de discussions et de revue littéraire, Craigen et ses collaborateurs (2014) ont tenté de parvenir à une définition plus largement acceptable et conforme à la véritable nature interdisciplinaire de la cybersécurité.

“La cybersécurité est l'organisation et l'ensemble des ressources, des processus et des structures utilisés pour protéger le cyberspace et les systèmes basés sur le cyberspace contre les événements qui déséquilibrent les droits de propriété de jure et de facto.” [Traduction libre] (Craigen et al., 2014).

Cette définition peut être déconstruite comme ceci :

“...l'organisation et l'ensemble des ressources, des processus et des structures...” (Craigen et al, 2014). Cette partie de la définition met en évidence la complexité de la cybersécurité, impliquant les interactions entre les individus, entre les systèmes ainsi qu'entre les individus et les systèmes. En évitant de citer des ressources, des processus ou des structures, la définition n'est pas normative et reflète l'aspect dynamique de la cybersécurité (Craigen et al., 2014).

¹⁶ Cf. Annexe A : Exemples de différents cyberattaques

“...contre les événements...” (Craig et al., 2014). Cette partie reconnaît que la “*protection*” vise à couvrir tous les événements intentionnels, accidents et catastrophes naturelles. Cela montre également que certains événements sont imprévisibles (Craig et al., 2014).

“...qui déséquilibrent les droits de propriété de jure et de facto.” (Craig et al., 2014). Cet aspect implique deux idées différentes : la propriété et le contrôle¹⁷. En effet, lorsque nous possédons un bien numérique (un fichier, une photo, etc.), nous avons certains droits sur ce dit bien comme le modifier, le consulter, le partager ou le supprimer. Si un tiers essayait de contrôler ce bien sans notre autorisation ou de réaliser des choses non autorisées avec ce dernier, ce serait un problème de cybersécurité. En d'autres termes, tout ce qui désaligne les droits que nous avons réellement sur ce bien (en pratique¹⁸) par rapport à ce que nous sommes censé avoir (selon le droit¹⁹), que ce soit intentionnel ou accidentel, est considéré comme un incident de cybersécurité (Craig et al., 2014).

Kaspersky²⁰ (2019 ; cité par Peslak et Hunsinger, 2019) relève les six principaux domaines inclus dans la cybersécurité :

- La sécurité des réseaux implique la protection d'un réseau informatique contre les intrusions.
- La sécurité des applications se focalise sur la défense des logiciels et des dispositifs contre les menaces.
- La sécurité de l'information vise à préserver l'intégrité et la confidentialité des données.
- La sécurité opérationnelle se rapporte aux processus et aux décisions relatifs à la manipulation et à la protection des données.
- La reprise après sinistre et la continuité des activités déterminent la manière dont une entreprise répond à un problème de cybersécurité entraînant l'arrêt des activités ou à une perte de données.
- La sensibilisation des utilisateurs finaux permet de former le facteur le plus imprévisible de la cybersécurité c'est-à-dire, l'Homme. Tout individu peut inconsciemment introduire un virus dans un système sécurisé en ne suivant pas les pratiques de sécurité.

1.2. Le marché de la cybersécurité

La cybersécurité est un sujet que pratiquement toutes les entreprises doivent aborder afin d'assurer et de renforcer le succès de la transformation numérique de leurs activités opérationnelles (processus automatisés, outils basés sur le cloud, support logiciel...). Par le passé, il était courant de considérer la cybersécurité comme une tâche réservée au département informatique. Aujourd'hui, elle occupe une place de plus en plus importante dans l'ensemble de l'entreprise ainsi que dans les décisions stratégiques dans les hautes sphères de l'organisation (Nguyen, 2023).

¹⁷ Ces concepts sont basés sur les travaux d'Ostrom et Hess (2007) sur les droits de propriété cités dans Craig et al. (2014)

¹⁸ De facto

¹⁹ De jure

²⁰ Entreprise privée internationale de cybersécurité dont la société holding est domiciliée au Royaume-Uni. (À propos de nous | Kaspersky. (s. d.). <https://www.kaspersky.be/about>)

Le marché mondial de la cybersécurité a connu une croissance robuste au cours des dernières années, avec un chiffre d'affaires passant de 83 milliards de dollars US en 2016²¹ à 162 milliards de dollars US en 2023²². Ce dernier devrait atteindre un chiffre d'affaires d'environ 257 milliards de dollars d'ici 2028²³ (Nguyen, 2023). En plus de l'essor du télétravail depuis la crise COVID-19 (Sussman, 2020 ; Alawida et al., 2022), la croissance du secteur de la cybersécurité est également alimentée par l'évolution des technologies numériques, le développement de modèles d'entreprise numériques ainsi que par la sensibilisation progressive aux risques et menaces liés aux données²⁴. Sans oublier qu'avec la croissance du nombre d'utilisateurs d'Internet au cours des dernières années²⁵, la cybersécurité s'impose de plus en plus à travers le monde (Nguyen, 2023). En 2023, Statista identifie quatre principaux sujets d'actualité concernant le marché de la cybersécurité à savoir la sécurité basée sur le cloud, le modèle *Zero Trust*, l'évolution de l'Internet des objets et la pénurie de personnel dans le domaine de la cybersécurité.

L'offre de solutions de cybersécurité est très diversifiée, couvrant un large éventail de besoins allant des particuliers-consommateurs jusqu'aux ministères de la Défense, ce qui crée une forte disparité au niveau de la demande. L'offre peut être divisée en deux catégories : les solutions de cybersécurité²⁶ et les services de sécurité²⁷. Parmi les acteurs clés de ce marché, on retrouve de grands systémiers-intégrateurs²⁸ tels qu'IBM, Microsoft, HP, Cisco, Dell, etc., ainsi que des équipementiers²⁹ tels que Qualcomm, ST Microelectronics, Schneider Electric, Siemens, etc. Les éditeurs de logiciels spécialisés comme Symantec, CheckPoint, Kaspersky, etc., jouent également un

²¹Statista. (s. d.). *Cybersecurity - Worldwide | Statista market forecast*. <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

²² Nguyen, P-H. (2023). *Cybersecurity - Market data Analysis & Forecasts | Statista*. Statista. p.16 <https://www.statista.com/study/124902/cybersecurity-report/>

²³ Nguyen, P-H. (2023). *Cybersecurity - Market data Analysis & Forecasts | Statista*. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

²⁴ Exemples : En Belgique, le programme Cyberwal by Digital Wallonia incarne l'ambition de la Wallonie en matière de cybersécurité. Il fédère les acteurs wallons de la cybersécurité, dans le domaine de la recherche, de l'innovation et de la formation. En France, l'Agence nationale de la sécurité des systèmes d'information organise en octobre chaque année le cybermoi/s, une grande campagne de sensibilisation aux enjeux de la cybersécurité. Elle fait intervenir de nombreux acteurs pour partager les conseils et bonnes pratiques à adopter.

²⁵ Statista. (2023, 3 mai). *Nombre d'utilisateurs d'Internet dans le monde 2014-2023*. <https://fr.statista.com/statistiques/985232/nombre-utilisateurs-internet-monde/>

²⁶ "Les solutions de cybersécurité sont des technologies automatisées qui aident à surveiller, détecter, signaler, contrer et sécuriser les organisations contre le risque de cyberattaques, qui peuvent être à l'origine d'hameçonnage, d'extorsion d'informations, de violations de données, etc. Ces solutions comprennent la sécurité des applications, la sécurité du cloud, la sécurité des données et la sécurité des réseaux. Exemples d'entreprises : McAfee, Palo Alto Networks, CrowdStrike Holdings." (Nguyen, 2023, p.6)

²⁷ "Les services de cybersécurité font référence à un traitement global ou à une large gamme de services qui renforcent la protection et la stratégie de sécurité de l'organisation contre les cybercrimes courants tels que le phishing, les logiciels malveillants ou les ransomwares. Ces services comprennent la conception et l'intégration, le conseil, la mise en œuvre, l'évaluation des risques et des menaces, ainsi que la formation professionnelle et l'éducation. Exemples d'entreprises : Palo Alto, Capgemini, CrowdStrike Holdings." (Nguyen, 2023, p.6)

²⁸ Un systémier ou assembleur est une entreprise qui intègre les différentes pièces détachées d'un système en se spécialisant dans la conception, le développement et le maintien en opération de ce système (Wikipédia, 2019). Un intégrateur, en informatique, est la personne chargée d'intégrer différents composants informatiques pour faire fonctionner un service ou une application complexe (Wikipédia, 2021).

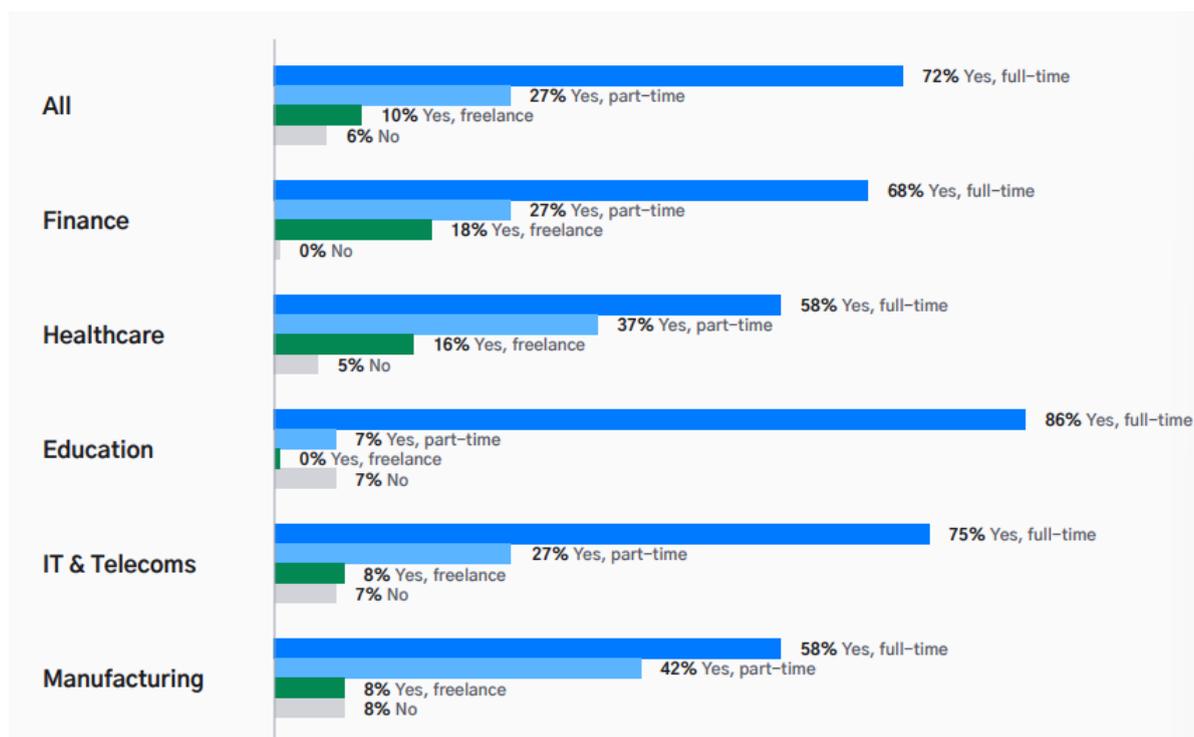
²⁹ Une entreprise fabriquant des pièces détachées, principalement pour le compte d'une autre entreprise, l'intégrateur ou l'assembleur (Wikipédia, 2023).

rôle majeur dans ce domaine. Parallèlement, les entreprises de services du numérique profitent de leur proximité avec les clients pour déployer leurs solutions de cybersécurité. Parmi ces entreprises, on peut citer Atos, Capgemini ou Sopra-Steria. Ces derniers apportent leur expertise ainsi que leur savoir-faire afin de répondre aux divers besoins des clients concernant leur sécurité numérique (Martin, 2019 ; Nguyen, 2023).

1.2.1. Le marché du travail en cybersécurité : une pénurie de main-d'oeuvre

L'impact de la COVID-19 sur le marché de l'emploi a été significatif. Contrairement à d'autres secteurs, le domaine de la cybersécurité a connu une expansion, ce qui a engendré une forte demande pour les professionnels de l'informatique et de la sécurité. En réalité, d'après le rapport *2020 Emerging Jobs Report* de LinkedIn (cité par Tessian, 2021, p.4), 10 des 15 professions enregistrant la plus forte croissance annuelle sont directement liées aux logiciels informatiques, à l'informatique ou à la sécurité des réseaux. De fait, 94 %³⁰ des équipes de cybersécurité ont embauché de nouveaux collaborateurs en 2020 (Tessian, 2021).

Figure 1 : Votre équipe cybersécurité a-t-elle embauché de nouvelles personnes pour soutenir votre département cette année ?³¹



Note : Tessian a demandé à Opinion Matters de sonder 200 femmes professionnelles de la cybersécurité (100 au Royaume-Uni et 100 aux États-Unis).

³⁰ Tessian. (2021). *The Future is Cyber : Opportunity in Cybersecurity Report 2021*. p.4

³¹ Tessian. (2021). *The Future is Cyber : Opportunity in Cybersecurity Report 2021*. p.4

Lors de leur étude du marché sud-africain de la cybersécurité³², Parker et Brown (2019) ont aussi identifié plusieurs industries qui recherchent des professionnels de la cybersécurité. Les services financiers représentaient 27% de la demande (fig.2), suivis du secteur des technologies et services de l'information qui représentait 24% de la demande (fig.2). D'autres industries telles que l'aviation et l'agriculture avaient au moins un emploi, ce qui illustre le besoin de professionnels de la cybersécurité dans d'autres secteurs.

Figure 2 : Industries demandant des professionnels en cybersécurité³³

Industry	Frequency	Frequency %
Financial services	53	27.0%
Information Technology and Services	47	24.0%
Not Specified	37	18.9%
Management consulting	11	5.5%
Telecommunications	7	3.6%
Government Parastatals	6	3.1%
Insurance	6	3.1%
Manufacturing	5	2.6%
Other	24	12.2%

Selon un rapport de l'((ISC)² ³⁴en 2022, la main-d'œuvre mondiale en matière de cybersécurité est de 4,7 millions de personnes³⁵. Cependant, le domaine de la cybersécurité a toujours énormément besoin de professionnels. En effet, les organisations tentent de combler le déficit mondial de 3,4 millions de travailleurs en cybersécurité³⁶ ((ISC)², 2022). La pénurie mondiale de main-d'œuvre en cybersécurité impacte directement et significativement les entreprises et leur protection (Meier & Roy, 2022). Près de 70% des employés en cybersécurité³⁷ pensent que leur entreprise ne possède pas assez d'employés dans le domaine pour être efficace ((ISC)², 2022). De plus, en lien avec cette pénurie, le secteur de la cybersécurité observe une augmentation de la charge de travail, du recours à des aides extérieures et des plans de recrutement de plus en plus agressifs (Meier & Roy, 2022 ; Sussman, 2020).

³² Analyse de 196 annonces d'emploi concernant la cybersécurité en Afrique du Sud

³³ Parker, A., & Brown, I. (2019). Skills requirements for Cyber security professionals : A content analysis of job descriptions in South Africa. *Communications in computer and information science*. p.183. https://doi.org/10.1007/978-3-030-11407-7_13

³⁴ International Information Systems Security Certification Consortium ((ISC)²) est une organisation à but non lucratif dont le siège social est situé à Palm Harbor (Floride, USA). Cet organisme fournit des certifications pour les professionnels de la sécurité de l'information telle que Certified Information Systems Security Professional (CISSP).

³⁵ ((ISC)². (2022). *Cybersecurity Workforce Study*. p.3. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

³⁶ Ibid.

³⁷ ((ISC)². (2022). *Cybersecurity Workforce Study*. p.9. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

Cette pénurie impacte négativement autant les entreprises que la société dans son ensemble. Les grandes entreprises et les prestataires de services possédant de grandes ressources peuvent attirer le cyber-personnel qualifié, acquérir des technologies de sécurité et profiter d'un accompagnement professionnel en matière de protection. Cependant, les petites entreprises ainsi que les organisations à but non lucratif rencontrent des difficultés à attirer les talents et les connaissances essentielles pour protéger leurs activités. Les compétences en matière de cybersécurité deviennent de plus en plus cruciales, et la disparité entre l'offre et la demande de professionnels spécialisés dans ce domaine continue de s'accroître (Blažič, 2021).

2. Les métiers et les compétences requises en cybersécurité

Il existe différents types de cybermenaces, et chacun nécessite des mesures de protection distinctes permettant de prévenir les dommages causés à une entreprise et à ses activités, ses revenus et ses employés (Nguyen, 2023). Ainsi, la diversité des menaces induit une demande diversifiée de compétences, de savoirs et de savoir-faire.

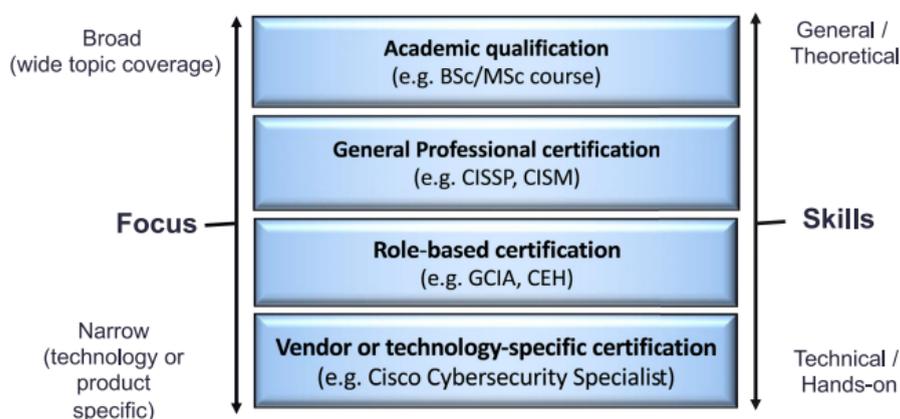
2.1. Les études et certificats

Il existe une multitude d'études ainsi que de certificats permettant de se spécialiser dans la cybersécurité. Ces derniers sont fournis autant par des établissements d'enseignement supérieur que par des organismes privés reconnus. En effet, la figure 3 représente les différentes formations et certifications ainsi que ce qu'elles apportent aux individus. Certaines sont centrées sur une technologie spécifique alors que d'autres développent une connaissance théorique et générale du domaine étudié. Bien qu'il existe de nombreuses voies d'accès à la profession, de nombreuses fonctions au sein du secteur de la cybersécurité requièrent un bachelier ou un master. Pour d'autres, un diplôme d'associé³⁸ peut suffire si les individus disposent aussi de certifications industrielles (Sussman, 2020).

Une étude réalisée en 2017 par Tittel et al. a révélé l'existence de plus de 100 certifications et a observé une augmentation de 17 % par rapport aux deux années précédentes (Tittel et al., 2017 cité par Furnell, 2021, p.2). Ces certifications peuvent différer dans toutes les dimensions, y compris ce qu'elles couvrent, qui elles ciblent, et comment elles sont évaluées. Ainsi, il est clair que les certifications ne sont pas directement interchangeables (Furnell, 2021).

³⁸ Diplôme qui sanctionne un programme d'études supérieures d'une durée de deux ans suivi dans un collège ou une université, et qui conduit à l'obtention de soixante crédits qui sont transférables dans un programme universitaire de premier cycle. (*Diplôme associé.* (2019). GDT. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26552626/diplome-associe>)

Figure 3 : Niveaux de spécialisation en cybersécurité³⁹



2.1.1. Les études et formations en Belgique

Il convient également de reconnaître que les contributions à la cybersécurité peuvent s'inscrire dans une perspective pluridisciplinaire, avec des liens clairs et des apports pertinents dans des domaines aussi divers que l'économie, l'éducation, le droit et la psychologie (Furnell, 2021 ; Graham et Lu, 2022). Du point de vue des qualifications académiques, de nombreux cours proposent désormais un contenu sur la cybersécurité. Plusieurs universités offrent également des diplômes de premier et de deuxième cycle dans ce domaine. Une qualification appropriée ne signifie pas nécessairement que le terme "sécurité" figure dans le titre du diplôme. Néanmoins, il ne suffit pas d'avoir un ou deux modules qui mentionnent la sécurité dans l'ensemble du cursus. La reconnaissance d'un contenu et d'une couverture appropriés peut être un défi pour les établissements qui souhaitent proposer des cours et pour les employeurs qui cherchent à recruter des diplômés. Plusieurs initiatives ont donc été mises en place pour apporter un peu de clarté comme *European Cybersecurity Skills Framework* développé par ENISA⁴⁰ en Europe et *NICE Framework* développé par NICCS⁴¹ aux Etats-Unis (Furnell, 2021)⁴².

Van den Berg, Van Zoggel, Snels, Van Leeuwen, Boeke, van de Koppen et De Bos ont examiné les procédés d'élaboration d'un programme de master en cybersécurité et ont constaté que les activités en ligne étaient vulnérables non seulement aux défaillances informatiques, mais aussi à diverses autres menaces, dont l'erreur humaine et les obstacles organisationnels (cités par Graham et Lu, 2022). Le programme de l'USNA⁴³ est illustratif. Afin de former ses agents spécialisés en cybersécurité, ils incluent dans leur programme des cours de politique, de droit et de psychologie associés à la sécurité informatique (Libicki et al, 2014). En 2013, le rapport *UK Cyber Security Strategy : Landscape Review*⁴⁴ développe qu'il est important d'avoir dans les équipes de cybersécurité des

³⁹ Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, 100, 102080. p.4. <https://doi.org/10.1016/j.cose.2020.102080>

⁴⁰ European Union Agency for Cybersecurity

⁴¹ National Initiative for Cybersecurity Careers and Studies

⁴² Cf. Annexe B : European Cybersecurity Skills Framework et NICE Framework (Etats-Unis)

⁴³ United States Naval Academy

⁴⁴ sur la stratégie du gouvernement en matière de cybersécurité réalisé par le National Audit Office (Royaume-Unis)

scientifiques plus "soft" tels que "les psychologues, les responsables de l'application des lois, les stratégies d'entreprise et les gestionnaires de risques" (Libicki et al, 2014 p. 26).

Le site Internet du CCB⁴⁵ recense les différentes études et formations qui peuvent être entreprises en Belgique afin de mener aux différents métiers de la cybersécurité. Ces dernières sont dispensées par différents acteurs du monde de l'éducation supérieure en Belgique tels que les universités de Liège, de Namur, de Bruxelles, de Leuven ou d'Hasselt ainsi que des différentes hautes écoles (Haute École en Hainaut, Howest, Haute Ecole de Namur-Liège-Luxembourg, etc.). Ces établissements offrent à toute personne souhaitant développer des compétences et des savoir en cybersécurité des formations de différents degrés (master, bachelier, master de spécialisation, etc.) et différentes spécialisations. Généralement, ces études se centrent sur les sciences informatiques, la gestion des réseaux et la sécurité⁴⁶. Cependant, comme montré dans la figure ci-dessous, d'autres études peuvent mener les individus à travailler dans la cybersécurité. La majorité des experts en cybersécurité qui ont été sondés dans l'étude sur la main-d'œuvre en cybersécurité réalisée par (ISC)² en 2022 ont orienté leur formation vers l'informatique et les sciences de l'information. En effet, la majorité, soit, 51%⁴⁷ d'entre eux, ont obtenu un bachelier et 56%⁴⁸ un master dans ce domaine spécifique. Ensuite, en deuxième position, nous retrouvons le domaine de l'ingénierie avec 19%⁴⁹ ayant obtenu un bachelier et 15 %⁵⁰ un master. Les 30%⁵¹ restants regroupent une variété de domaines tels que le commerce, la communication, les sciences sociales, les mathématiques, l'économie, les sciences biologiques et biomédicales, ainsi que d'autres disciplines en dehors du champ des technologies de l'information (fig.3) ((ISC)², 2022).

⁴⁵ Centre pour la Cybersécurité Belgique

⁴⁶ Cf Annexe C : Les différentes études menant aux métiers de la cybersécurité en Belgique

⁴⁷ (ISC)². (2022). *Cybersecurity Workforce Study*. p.54.

<https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

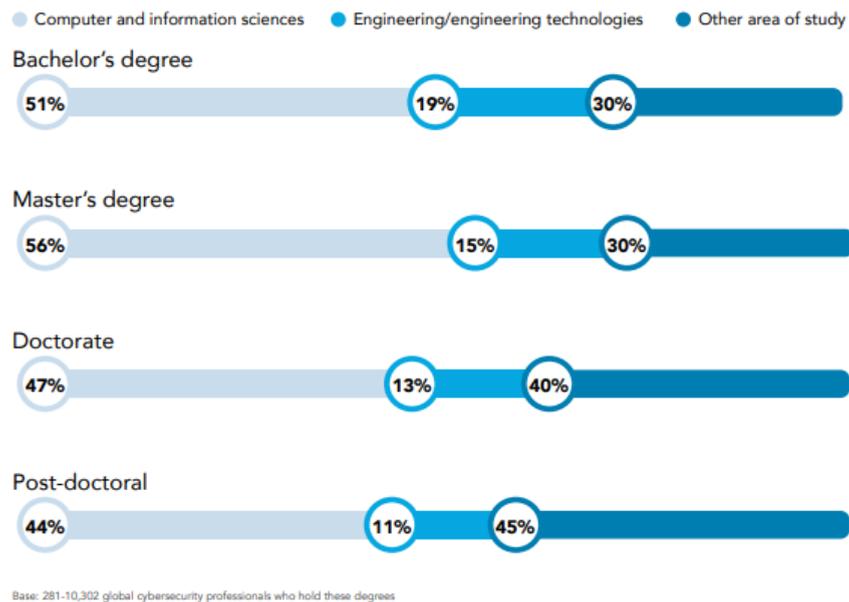
⁴⁸ Ibid.

⁴⁹ Ibid

⁵⁰ Ibid.

⁵¹ Ibid.

Figure 4 : Orientation des études des cyber-professionnels⁵²



Dès 2017, plus de 93 %⁵³ des cadres et des responsables du recrutement ont prédit une importante pénurie de compétences dans les entreprises de cybersécurité, de même qu'une importante difficulté à recruter des personnes possédant les compétences et l'expertise requises (Lapena, 2017 cité par Sussman, 2020). De ce fait, il est important de développer et de faire évoluer les savoirs et les compétences relatifs à la cybersécurité ainsi que d'attirer les jeunes vers cette filière. Les programmes éducatifs et de formation en cybersécurité doivent rapidement ajuster leur cursus en fonction des avancées technologiques pour répondre aux exigences du marché de l'emploi. Cependant, cela n'a rien d'aisé vu que les différents établissements d'enseignement supérieur n'arrivent pas à trouver un corps enseignant qualifié qui leur permettrait de mettre à jour leurs divers programmes (Blažič, 2021). Actuellement, le CCB est en train de mettre en place le programme *CySec Education & Research Development*, qui débutera à l'automne 2023. L'objectif de ce programme est d'assurer la compétitivité de la Belgique en termes de connaissances en cybersécurité et de renforcer son autonomie numérique dans ce domaine. Cette initiative se concentrera spécialement sur la promotion et le soutien de la recherche ainsi que de la formation. Selon les prévisions du CCB, cela contribuera à augmenter le nombre de professionnels qualifiés en cybersécurité (Centre pour la Cybersécurité Belgique, 2023).

Dans le marché sud-africain, plus de la moitié (52%⁵⁴) des annonces d'emploi en cybersécurité analysées par Parker et Brown (2019) exigeaient un bachelier en informatique, en systèmes

⁵² (ISC)². (2022). *Cybersecurity Workforce Study*. p.54.

<https://www.isc2.org/~/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

⁵³ Sussman, L. (2020). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that may expand the expectations of the Cyber Workforce. *ResearchGate*. p.20 https://www.researchgate.net/publication/348352243_Exploring_Non-Technical_Knowledge_Skills_and_Abilities_KSA_that_May_Expand_the_Expectations_of_the_Cyber_Workforce

⁵⁴ Parker, A., & Brown, I. (2019). Skills requirements for Cyber security professionals : A content analysis of job descriptions in South Africa. *Communications in computer and information science* (p.187). https://doi.org/10.1007/978-3-030-11407-7_13

d'information ou en ingénierie comme qualification minimale. 9,2%⁵⁵ des annonces citent les certifications de l'industrie comme exigence minimale pour le poste, suivies de 8,7%⁵⁶ qui citent toute "qualification tertiaire pertinente" dans les études en informatique. 2,0%⁵⁷ ont indiqué avoir besoin du diplôme de l'enseignement secondaire pour un emploi, tandis que 1,5%⁵⁸ de l'échantillon exigeaient au minimum un master (fig.5).

Figure 5 : Qualification minimum requise pour un emploi dans la cybersécurité⁵⁹

Minimum qualification	Frequency	Frequency %
Bachelor's Degree	102	52.0%
Not Specified	26	13.3%
Certifications	18	9.2%
Relevant tertiary qualification	17	8.7%
Diploma	10	5.1%
Bachelor's Degree or Postgraduate Degree	7	3.6%
Postgraduate Degree	6	3.1%
Matric	4	2.0%
IT Related	3	1.5%
Master's Degree	3	1.5%

Note : "Matric" représente l'obtention de son diplôme de secondaire (Collins English Dictionary, 2023).

En ce qui concerne le marché australien de la cybersécurité, Potter et Vickers (2015) exposaient que tous les emplois nécessitaient des qualifications supérieures, comprenant soit un diplôme en informatique ou dans un domaine apparenté, ou une combinaison équivalente d'études et d'expérience⁶⁰.

Dans le domaine des études, les femmes tendent proportionnellement à obtenir plus de diplômes et de certifications que les hommes. D'après l'enquête de (ISC)² sur la main-d'œuvre dans le domaine de la cybersécurité en 2018, il ressort que les femmes attribuent une importance supérieure à la cybersécurité ou aux diplômes d'études supérieures dans ce domaine par rapport aux hommes. De plus, en moyenne, les femmes obtiennent davantage de certifications en cybersécurité ((ISC)², 2018).

⁵⁵ Parker, A., & Brown, I. (2019). Skills requirements for Cyber security professionals : A content analysis of job descriptions in South Africa. *Communications in computer and information science* (p.187). https://doi.org/10.1007/978-3-030-11407-7_13

⁵⁶ Ibid.

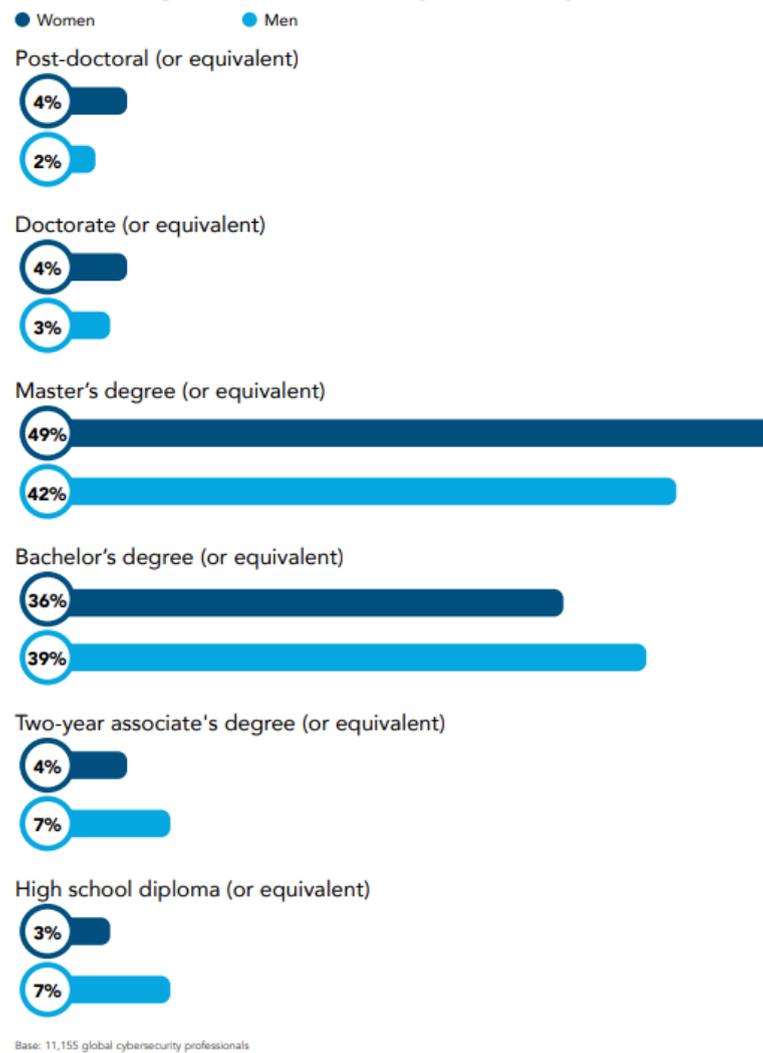
⁵⁷ Ibid.

⁵⁸ Ibid.

⁵⁹ Ibid.

⁶⁰ La recherche a été menée en janvier 2015, en utilisant des listes datées de décembre 2014 à début janvier 2015. Cette enquête a généré 60 listes de postes, qui ont été réduites à 33 après l'élimination des doublons et des offres d'emploi non liées à la cybersécurité. Parmi ces 33 annonces, 18 employeurs distincts étaient représentés, la plupart d'entre eux provenant de grandes entreprises australiennes ainsi que d'entreprises internationales ayant des antennes en Australie.

Figure 6 : Le plus haut niveau d'étude atteint en fonction du genre⁶¹



2.1.2. Les certificats reconnus venant d'organismes privés

Dans le domaine de la cybersécurité, les certifications jouent un rôle complémentaire à la formation en validant une expertise spécifique à un aspect particulier du métier. Les compétences certifiées sont devenues essentielles pour les entreprises, d'autant plus qu'elles peuvent influencer le niveau de rémunération. Les métiers de la cybersécurité requièrent généralement tous un haut niveau de compétences et de connaissances. De nombreuses certifications sont disponibles pour attester de cette expertise, telles que le certificat CISSP⁶², CISM⁶³, CRISC⁶⁴ et CISA⁶⁵. Posséder une certification

⁶¹ (ISC)². (2022). *Cybersecurity Workforce Study*. p.53.

<https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

⁶² Certified Information Systems Security Professional

⁶³ Certified Information Security Manager

⁶⁴ Certified in Risk and Information Systems Control donné par ISACA

⁶⁵ Certified Information Systems Auditor donné par ISACA

ajoute une crédibilité significative au curriculum vitae, étant un indicateur pour les employeurs des compétences du candidat (Gardia Cybersecurity School, 2023).

Il existe de nombreuses certifications en cybersécurité. Chacune correspond à un niveau d'expérience et à un domaine spécifique (Furnell, 2021 ; Gardia Cybersecurity School, 2023). Les candidats doivent donc nécessairement choisir une certification relative à leurs objectifs et leurs compétences. De plus, beaucoup de certifications nécessitent un investissement financier allant de 500 euros à plus de 3.000 euros. À titre d'exemple, les particuliers voulant obtenir le du certificat CISSP⁶⁶ devront déboursier 800 euros (Gardia Cybersecurity School, 2023).

Le Centre canadien pour la Cybersécurité (2022) a regroupé dans un guide les organismes de certifications en cybersécurité parmi les plus populaires et les plus connus tels que CertNexus, Cisco Systems, Computing Technology Industry Association (CompTIA), Council for Registered Ethical Security Testers (CREST), Certified Wireless Networks Professionals (CWNP), EC-Council, Global Information Assurance Certification (GIAC), International Information Systems Security Certification Consortium ((ISC)²), ISACA, itSM Solutions, McAfee Institute, Offensive Security, PECB et Security & Continuity Institute (SECO). Pour chaque organisation, le Centre canadien pour la Cybersécurité décrit les différents certificats qu'elles délivrent ainsi que les candidats ciblés par les certifications. Bien que la majorité des organismes de certification soient basés aux États-Unis, leurs certificats sont largement reconnus mondialement. De plus, les candidats peuvent suivre leur formation auprès de prestataires locaux et, dans de nombreux cas, ont la possibilité de passer les examens dans des centres d'examen ou en ligne (Centre canadien pour la Cybersécurité, 2022).

Dans leur étude, Parker et Brown (2019) ont rapporté que 49,5 %⁶⁷ de l'échantillon d'annonces d'emploi spécifiaient qu'en plus d'une qualification minimale, le candidat avait également besoin d'une certification de l'industrie. Parmi 16,84%⁶⁸ de l'échantillon, les auteurs ont notifié qu'une certification de l'industrie serait considérée comme un avantage. Les certifications de l'industrie les plus exigées par les organisations de l'étude étaient le Certified Information Systems Security Professional (CISSP), le Certified Information Security Manager (CISM), le Certified Information Systems Auditor (CISA), ainsi que d'autres liées aux normes de cybersécurité telles que celles de l'Organisation internationale de normalisation (ISO) et de l'Institut national des normes et de la technologie (NIST). Enfin, d'autres certifications, apparues de manière récurrente, étaient l'Information Technology Infrastructure Library (ITIL) et le Cisco Certified Network Associate.

⁶⁶ Certified Information Systems Security Professional

⁶⁷ Parker, A., & Brown, I. (2019). Skills requirements for Cyber security professionals : A content analysis of job descriptions in South Africa. *Communications in computer and information science* (p.187). https://doi.org/10.1007/978-3-030-11407-7_13

⁶⁸ Ibid.

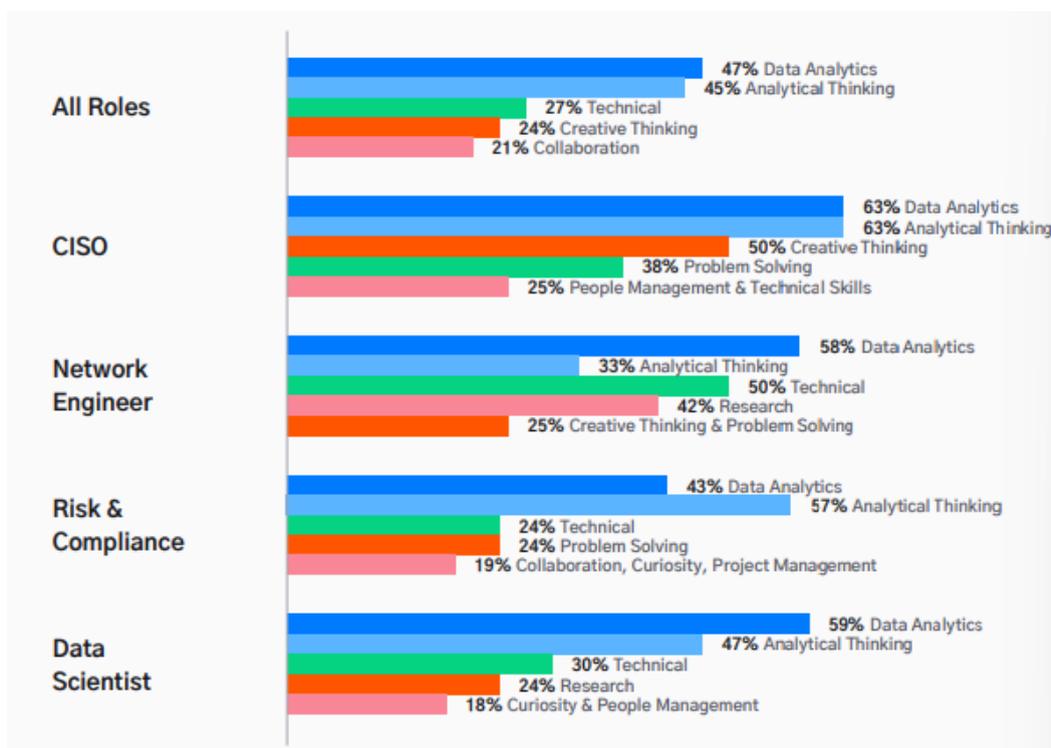
Figure 7 : Exemples de différentes certifications (Furnell, 2021, p.3)

Certification	Security+	GIAC Security Essentials (GSEC)	Certified Ethical Hacker (CEH)	Certified Information Security Manager (CISM)	Certified Information Systems Security Professional (CISSP)
Provider	CompTIA	SANS	EC-Council	ISACA	(ISC) (Furnell and Bishop, 2020)
Level	Entry-level	Entry-level	Intermediate	Advanced	Advanced
Role/aim	"a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career" (CompTIA, 2019)	"Candidates are required to demonstrate an understanding of information security beyond simple terminology and concepts" (GIAC, 2019)	"certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective" (EC-Council, 2019)	"promotes international security practices and recognizes the individual who manages, designs, and oversees and assesses an enterprise's information security" (ISACA, 2019)	"for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles" ((ISC)2 2019)
Target group	IT Professionals	Security Professionals that want to demonstrate they are qualified for IT systems hands-on roles with respect to security tasks	Security officers, auditors, security professionals, site administrators	Information Security Managers, aspiring Information Security Managers, IS/IT Consultants, Chief Information Officers	Chief Information Security Officer, Chief Information Officer, Director of Security, IT Director/Manager, Security Systems Engineer, Security Analyst, Security Manager, Security Auditor, Security Architect, Security Consultant, Network Architect
Examination	Examined via 90-min exam with up to 90 multiple choice and performance-based questions	A proctored exam, of 180 questions in up to 5 h	Examined via 4-h multiple choice exam, with 125 questions	4-h exam, with 150 questions	English: 3-h Computer Adaptive Testing with 100-150 items Non-English: 6-h linear exam with 250 items
Eligibility	Recommended CompTIA Network+ and two years of experience in IT administration with a security focus	N/A	Candidates must have either completed an official EC-Council training course or must have at least 2 years of work experience in the Information Security domain	At least 5 years professional work experience in the field of information security, with at least 3 years in the role of information security manager	At least five years of cumulative, paid work experience in two or more of the eight domains of the CISSP Common Body of Knowledge

2.2. Les compétences

Il est essentiel de comprendre que la cybersécurité englobe une vaste gamme de compétences. Les cyber-travailleurs ont besoin de *"comprendre la sécurité des réseaux, l'atténuation des risques et la protection des informations, et être préparés aux activités futures en matière d'intelligence artificielle, d'apprentissage automatique et de cartographie de la réalité virtuelle. Ils doivent gérer des projets, s'y retrouver dans les codes juridiques et de conformité, et travailler dans des secteurs allant des soins de santé à l'application de la loi"* [Traduction libre] (Poster, 2018, p.577) (Furnell, 2021 ; Poster, 2018). Le domaine de la cybersécurité est donc multidisciplinaire. Il inclut autant l'informatique que les mathématiques, l'économie, le droit, la psychologie et l'ingénierie. Des recherches ont démontré que les professionnels de la cybersécurité réussissent en combinant une compréhension pointue des technologies et des systèmes d'information avec la capacité d'apprendre et de s'adapter en permanence. En effet, tous les emplois en cybersécurité nécessitent une combinaison de compétences techniques et non techniques (fig...) (Ben-Asher et Gonzalez, 2015 cité par Le Roy, 2021 ; Dawson et Thomson, 2018 ; Tessian, 2021).

Figure 8 : Les compétences requises pour s'épanouir en cybersécurité selon différents rôles (Tessian, 2021, p.8)



2.1.1. Les compétences techniques

Les experts en cybersécurité doivent détenir une expertise approfondie en matière de systèmes d'exploitation informatiques et de solutions d'analyse pour mener à bien des activités telles que la numérisation des réseaux, la cartographie de ces derniers et l'évaluation des vulnérabilités (Dawson & Thompson, 2018 ; Potter et Vickers, 2015). Une enquête menée auprès de 40 RSSI⁶⁹, qui gèrent environ 6100 employés en cybersécurité, a indiqué que les trois principaux domaines de compétences les plus demandés sont *“l'architecture de sécurité de l'information ; la gestion des risques et conformité; et l'analyse du renseignement/de la menace”* (Caldwell, 2013, p. 6). Potter et Vickers (2015) ont regroupé en plusieurs catégories les différents métiers de la cybersécurité et définit plus précisément les besoins relatifs aux compétences pour chaque classe de métiers en cybersécurité⁷⁰.

Le premier site d'emploi mondial, Indeed.com, dispose lui aussi d'une liste de compétences requises aux métiers de la cybersécurité. Ces dernières sont regroupées dans une fiche métier.

⁶⁹ Responsable de la sécurité des systèmes d'information

⁷⁰ Cf. 2.3. Les métiers

Figure 9 : Fiche métier des experts en cybersécurité adaptée (Indeed, 2023)

Savoirs	<ul style="list-style-type: none"> ● Des connaissances techniques en développement de systèmes, en normes de sécurité informatique et en administration réseau ● Les méthodes d'analyse (systémique, de risques ou fonctionnelles, notamment) ● Les principes d'intégration de matériels et de logiciels ● La modélisation informatique ● L'urbanisation des systèmes d'information ● Les technologies de l'accessibilité numérique ● L'évaluation des risques sécurité informatique et télécoms
Savoir-faire	<ul style="list-style-type: none"> ● Maîtriser les outils informatiques ● Définir les caractéristiques techniques du produit ● Concevoir les solutions techniques et l'architecture d'un système d'information ● Evaluer le résultat de ses actions ● Mettre en œuvre les procédures techniques d'utilisation, d'exploitation et de sécurité des équipements informatiques ● Procéder aux phases de tests et de recettes des applications développées ● Définir et contrôler l'application des procédures de sécurité et la qualité des systèmes d'information et de télécoms ● Procéder à une assistance technique ● Mettre à jour une documentation technique

Les compétences techniques jouent un rôle crucial et sont intégrées à toutes les annonces d'emploi. Il faut noter que ces compétences techniques requises varient en fonction des spécificités de chaque poste (Potter et Vickers, 2015).

2.1.2. Les compétences non techniques

En ce qui concerne les études techniques, les compétences non techniques sont souvent reléguées au second plan par rapport aux compétences techniques dans les programmes. Les compétences non techniques des diplômés sont souvent peu développées. Ils n'ont qu'une faible reconnaissance de leur importance (Hall et Rao, 2020 ; Jang, 2016 cité par Sussman, 2020). Plusieurs recherches soutiennent que la connaissance technique seule est insuffisante pour développer la main-d'œuvre en cybersécurité. La négligence des aspects sociaux engendre non seulement un manque de connaissances, mais également, des lacunes en matière de sécurité ainsi qu'un manque d'efficacité (Dawson et Thomson, 2018 ; Hall et Rao, 2020 ; Sussman, 2020). De ce fait, les entreprises commencent à embaucher des travailleurs non qualifiés dotés de solides compétences non techniques et à investir dans leur formation à des tâches techniques (Lapena, 2020 cité par Sussman, 2020; Panhans et al., 2022). Le Forum économique mondial (2018) répertorie le leadership, l'influence sociale, la pensée critique, la créativité et les compétences interpersonnelles parmi les dix compétences les plus demandées dans tous les secteurs.

Il est évident que les professionnels de la cybersécurité doivent avoir une compréhension approfondie de la technologie utilisée pour défendre un système. Cependant, les compétences en

gestion de projet et en travail d'équipe pour mener à bien un projet de cyberdéfense, les compétences en communication et en leadership pour s'engager avec l'organisation au sens large, ainsi que la créativité et la flexibilité nécessaires pour adapter une solution à une situation spécifique, sont tout aussi appréciées que les compétences techniques (Hall et Rao, 2020 ; Sussman, 2020).

A titre d'exemple, une des plus grande vulnérabilité exploitable de la cyberdéfense sont les utilisateurs finaux (Peslak et Hunsinger, 2019 ; Dawson & Thomson, 2018 ; Le Roy, 2021). Un cyber-travailleur devrait donc être capable d'envisager toutes les façons dont ses collègues et/ou clients pourraient être exploités par un tiers malintentionné et de communiquer la vulnérabilité d'une manière facilement compréhensible par les personnes peu éveillées au domaine de la cybersécurité (Dawson & Thomson, 2018 ; Le Roy, 2021). En effet, la plupart des emplois de *junior* en cybersécurité sont des postes d'auditeur, d'analyste, d'intervenant et de technicien qui nécessitent un certain niveau d'interaction avec les clients (Cyberseek Career Pathways, n.d., cité par Sussman, 2020).

Dans ces compétences non techniques, il ne faut pas seulement citer les *soft skills*⁷¹. Les cyber-défenseurs sont encouragés à avoir dans leur panel de *hard skills*⁷² des connaissances en management, psychologie, en politique, et/ou en droit afin de répondre à l'aspect multidisciplinaire de la cybersécurité (Graham et Lu, 2022 ; Libicki et al. , 2014 ; Dawson et Thomson, 2018).

Le fournisseur de solutions de sécurité, Tripwire, a commandé une enquête auprès de 315 professionnels de la sécurité de plus de 100 entreprises américaines sur les failles en matière de compétences en cybersécurité. Tous les participants ont souligné le manque crucial de compétences non techniques ainsi que leur importance (Lapena, 2017 cité par Sussman, 2020). De plus, développer les compétences non techniques des cyber-professionnels peut avoir un effet positif et notable sur sa compétence, sa confiance et son efficacité (Sussman, 2020).

⁷¹ "Les soft skills sont des qualités et des traits de caractère qui définissent une personne dans sa façon de travailler. Difficiles à quantifier et plus subjectifs, ce sont des données qui figurent moins souvent sur un CV mais qui sont de plus en plus recherchées" (Équipe éditoriale d'Indeed, 2023).

⁷² "Les hard skills sont les connaissances techniques que vous avez acquises tout au long de votre parcours éducatif, académique et professionnel" (Équipe éditoriale d'Indeed, 2023).

Figure 10 : Les savoirs, compétences et aptitudes non techniques des rôles techniques en cybersécurité selon le modèle NICE [Traduction libre]⁷³

	Savoirs, compétences et aptitudes non techniques
Hard	<ul style="list-style-type: none"> ● Connaître et respecter la loi et les réglementations ● Gérer des situations de crises telles que les incendies, les problèmes liés aux employés et invités, les tornades, etc. ● Utiliser efficacement les ordinateurs
Soft	<ul style="list-style-type: none"> ● Résolution de problèmes liés au service client ● Développement de relations positives avec les clients ● Facilitation des équipes et du travail d'équipe ● Compétences en leadership ● Gestion du stress personnel ● Techniques de négociation ● Compétences en présentation ● Comportement et apparence professionnels ● Utilisation de l'éthique dans la prise de décision ● Collaboration efficace avec les pairs ● Compétences en communication écrite
Mixed	<ul style="list-style-type: none"> ● Utilisation de l'information pour la prise de décision ● Formation les employés

2.1.2.1. Passion, curiosité et formation continue

En raison de la rapidité de l'évolution des technologies, les professionnels en cybersécurité doivent constamment se former pour rester au fait des nouvelles technologies (logiciels, langage de programmation, algorithmes, matériels) et des nouvelles méthodes d'attaque. Une éducation informelle supplémentaire est souvent considérée comme nécessaire pour réussir dans leur carrière (Potter et Vickers, 2015 ; Dawson et Thomson, 2018 ; Hall et Rao, 2020). Les cyber-travailleurs devront ainsi être passionnés, avoir la volonté d'apprendre tous les jours afin d'être toujours éveillés (Potter et Vickers, 2015 ; et Dawson et Thomson, 2018). En effet, les connaissances acquises sur les menaces, les stratégies de défense et les technologies actuelles en cybersécurité deviennent souvent obsolètes un à deux ans après l'obtention du diplôme (Hall et Rao, 2020).

2.1.2.2. Travail d'équipe

En raison de la complexité de leur environnement de travail, les experts en cybersécurité ont besoin de travailler en équipe. Au regard de cette complexité croissante, il devient nécessaire que la future main-d'œuvre apprenne à travailler en équipe (Dawson & Thompson, 2018). Lors de l'étude de Sussman (2020), plus de la moitié des participants ont souligné l'importance de la collaboration avec

⁷³ Sussman, L. (2020). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that may expand the expectations of the Expectations of the Cyber Workforce. *ResearchGate*. p.25 https://www.researchgate.net/publication/348352243_Exploring_Non-Technical_Knowledge_Skills_and_Abilities_KSA_that_May_Expand_the_Expectations_of_the_Cyber_Workforce

leurs collègues ainsi que l'échange de connaissances. Au cours des entretiens, Sussman (2020) a observé que les participants accordent une importance particulière aux qualités qui les ont aidés à s'intégrer plus efficacement au sein de l'équipe de cybersécurité. Cela leur a permis de trouver de meilleures solutions - plus efficaces - aux problèmes des clients.

2.1.2.3. Sens éthique irréprochable

A cause de la complexité inhérente au domaine de la cybersécurité, les experts dans ce domaine doivent avoir un sens éthique développé. Par exemple, au sein d'une organisation, les cyber-travailleurs peuvent choisir de mettre en œuvre leurs compétences de manière altruiste (*hackers* éthiques) ou malveillante, ou encore adopter une position intermédiaire. Il est donc impératif de tenir compte des motivations des défenseurs de la cybersécurité dans le processus de sélection, afin de réduire les risques de menaces internes (Dawson & Thompson, 2018 ; Le Roy, 2021).

2.1.2.3. Penseurs systémiques

Les différents systèmes informatiques, réseaux et technologies sont de plus en plus interdépendants et interconnectés les uns avec les autres. Du fait de cette interconnexion, toute personne évoluant dans la cybersécurité doit être capable de prendre du recul par rapport à l'équipement spécifique sur lequel elle se concentre, et ainsi avoir une vision globale. Par exemple, les professionnels de la cybersécurité doivent avoir une compréhension des divers systèmes susceptibles d'être impactés par des mises à jour logicielles simples (Dawson & Thompson, 2018).

2.1.2.4. Communication et présentation

La main-d'œuvre active dans le domaine de la cybersécurité doit savoir communiquer des informations techniques à un public peu éveillé dans le domaine. Ces employés doivent donc être capables de dialoguer avec les responsables budgétaires pour expliquer leurs besoins, et d'affirmer clairement les conséquences désastreuses en termes de sécurité qu'une certaine idée pourrait amener auprès de leurs supérieurs (Dawson et Thomson, 2018 ; Potter et Vickers, 2015). A noter que les entreprises souffrent du manque de personnel compétent pour expliquer les cybermenaces aux décideurs (Dawson et Thomson, 2018). S'ils ne parviennent pas à communiquer de manière claire et compréhensible, leur efficacité dans l'accomplissement de leurs tâches diminue (Dawson et Thomson, 2018 ; Potter et Vickers, 2015). De plus, la cybersécurité est rarement un effort solitaire, et les travailleurs doivent présenter des informations à leurs collègues. Les compétences orales et écrites sont donc essentielles pour travailler efficacement dans des rôles de cybersécurité (Sussman, 2020).

2.1.2.5. Formateur

Les participants à l'étude de Sussman (2020) ont affirmé qu'une certaine capacité à former les autres était un élément essentiel du développement professionnel des travailleurs en cybersécurité (Sussman, 2020). De plus, les individus qui reçoivent une formation sur le terrain et qui bénéficient d'un mentorat tendent à obtenir de meilleurs résultats et à évoluer davantage dans leur carrière (Dawson et Thomson, 2018).

2.1.2.5. Leadership et influence sociale

Le leader joue le rôle de médiateur entre chaque personne de l'équipe. Il est capable de motiver ses collègues ainsi que de maintenir une certaine cohésion de groupe afin de réussir leurs tâches et de performer. En entreprises, les personnes sont sujettes à collaborer ensemble. Il s'installe alors une dynamique de pouvoir. Les leaders ont la capacité d'influer sur le comportement et les décisions de leurs collègues (Tedongmo Teko et Bapes Ba Bapes, 2010). L'effort en cybersécurité est loin d'être solitaire. Pour avoir des solutions efficaces, les cyber-travailleurs doivent conjuguer leurs forces et expertises. Avoir la capacité de diriger un groupe est donc une compétence nécessaire en cybersécurité.

2.1.2.5. Flexibilité et adaptabilité

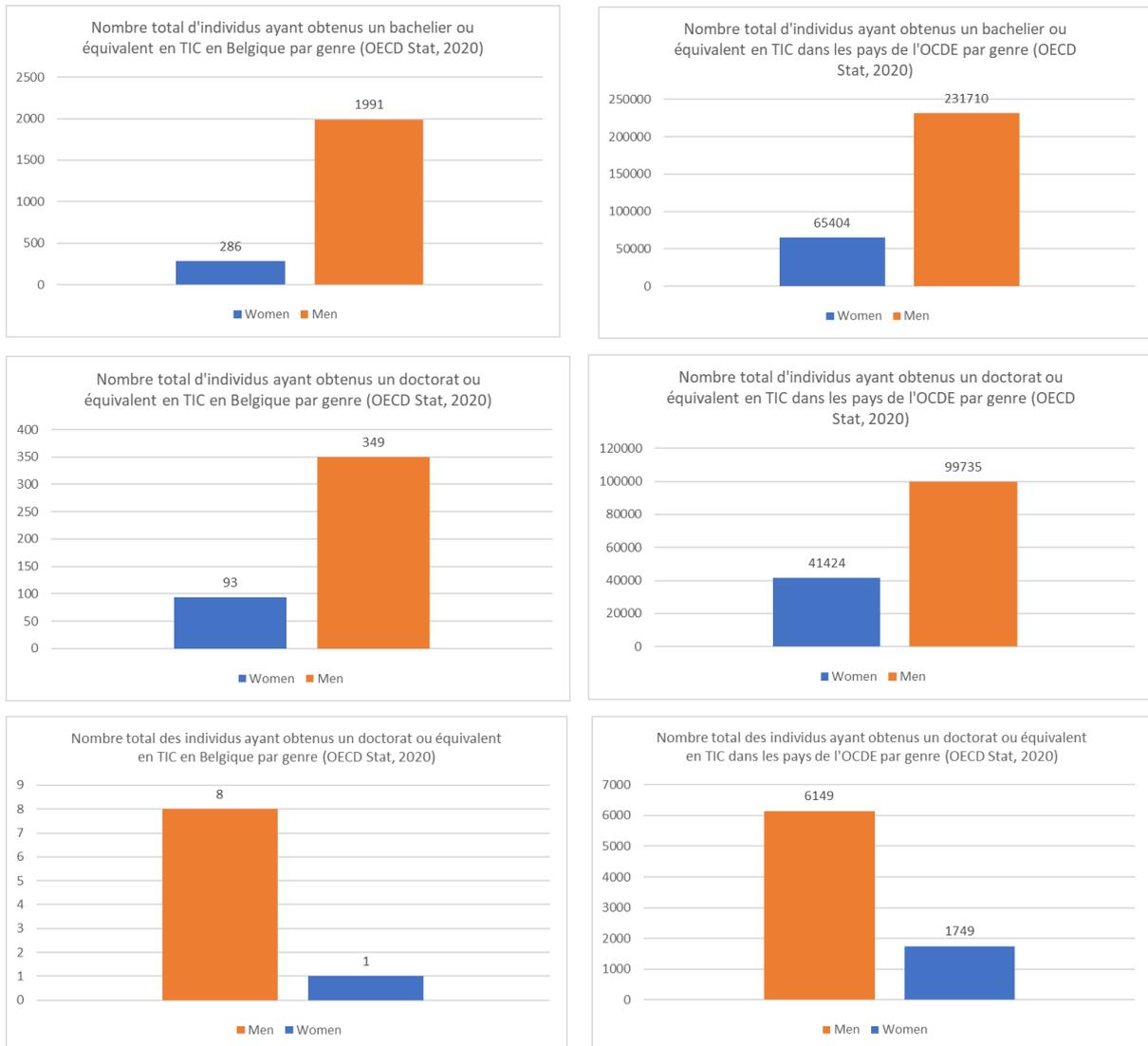
Les cyber-menaces évoluant chaque jour, les professionnels de la cybersécurité doivent être capables d'adapter et de modifier leurs approches. Ils doivent être en mesure de s'adapter facilement à tout type de modifications de leur environnement et des technologies utilisées (ECC University, 2023).

2.1.3. La divergence des compétences en fonction du genre

Les *hard skills* apportées aux métiers de la cybersécurité diffèrent en fonction du genre. En effet, les graphiques ci-dessous montrent la faible représentation féminine dans les études relatives aux technologies de l'information et de la communication (TIC). Selon les données de l'OCDE pour 2020, 22% des femmes des pays membres de l'OCDE réalisent un bachelier dans ce domaine, 29,3% un master et 22,1% un doctorat (fig.11). La Belgique suit la même tendance. Ce résultat démontre clairement un écart significatif en termes de diversité de genre dans ces études. On peut déduire que les femmes sont moins enclines à se former dans des domaines dits techniques et informatiques. Comme expliqué ultérieurement, les métiers de la cybersécurité requièrent un bagage technique important, à cause de la nature complexe et dynamique du secteur. Ce déséquilibre peut donc avoir un impact direct sur les compétences techniques disponibles sur le marché de l'emploi. En effet, vu que les femmes représentent 50%⁷⁴ de la population mondiale en âge de travailler, le fait d'avoir peu de femmes dans ces études contribue à la pénurie de main-d'œuvre qualifiée dans le domaine des TIC ainsi qu'à un manque de diversité dans les bassins de candidats en cybersécurité.

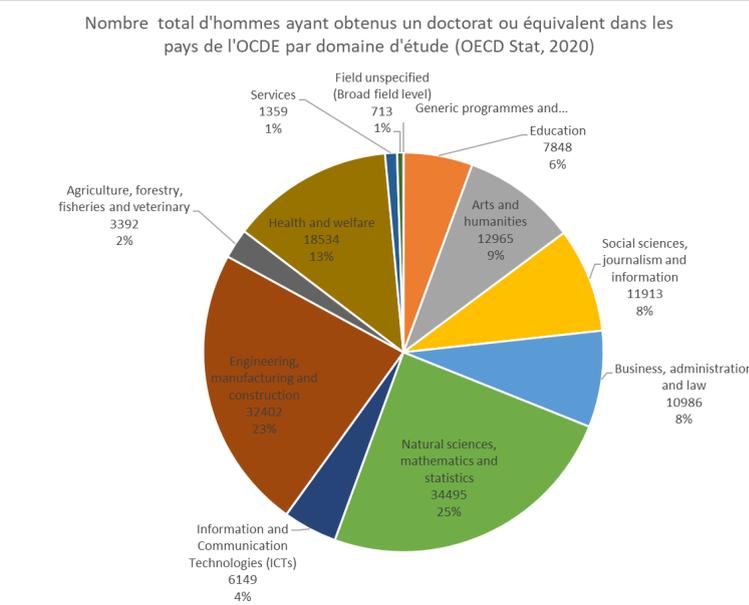
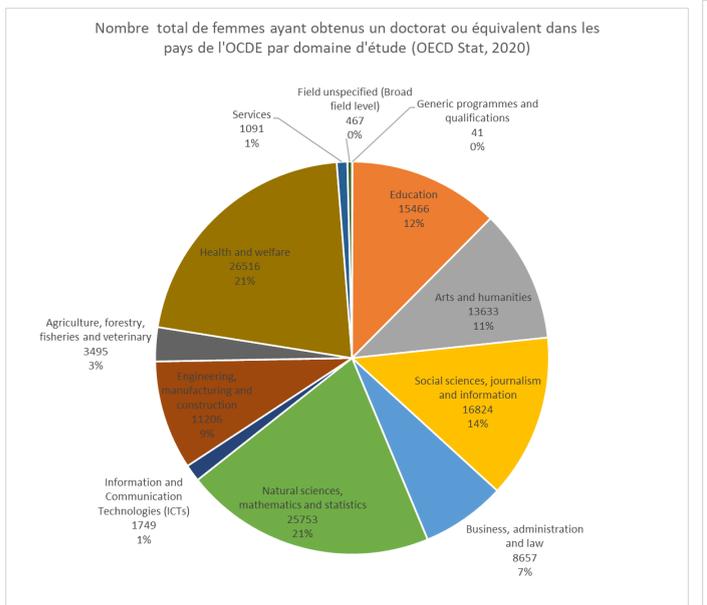
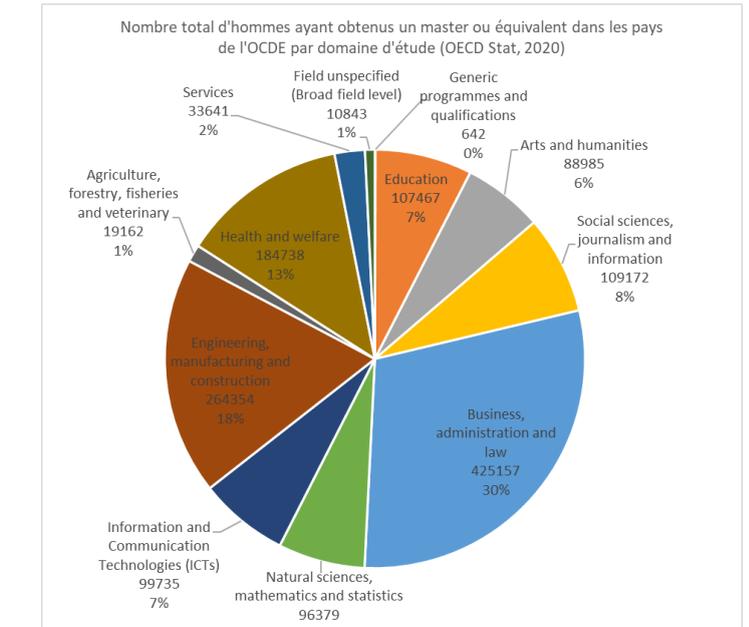
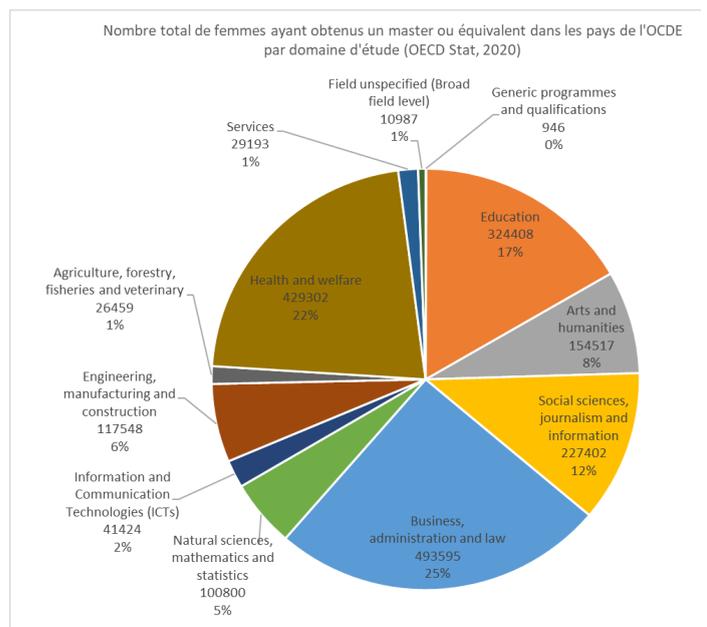
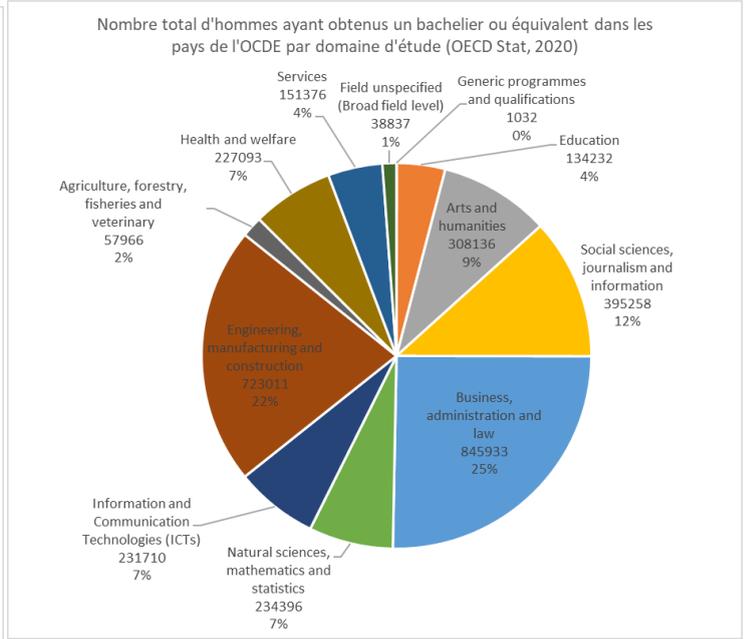
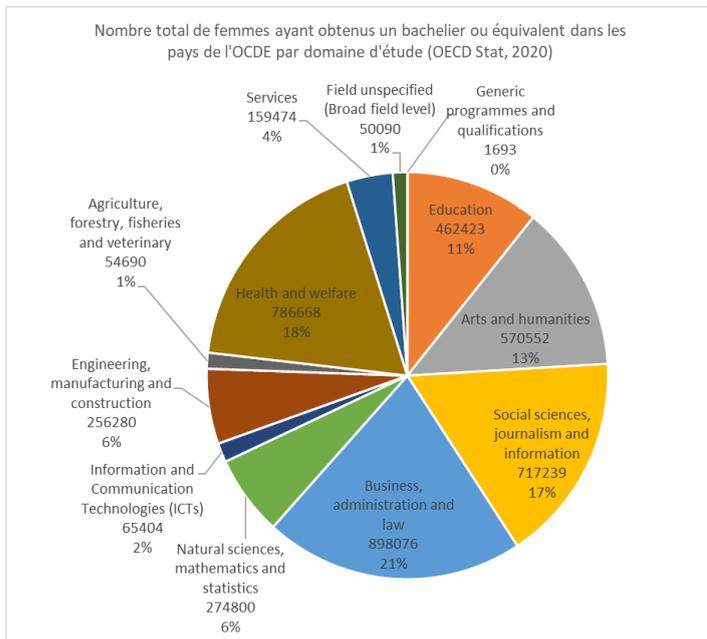
⁷⁴ Gammarano, R. (2019). 100 statistiques sur l'OIT et le marché du travail pour célébrer le centenaire de l'OIT. ILOSTAT. point 62 <https://ilostat.ilo.org/fr/100-statistics-on-the-ilo-and-the-labour-market/>

Figure 11 : Nombre total d'individus ayant obtenu une qualification dans le domaine des TIC en fonction du genre (OECD Stat, 2020).



Cependant, il a été prouvé par différentes études que les employeurs ne cherchent plus seulement des compétences purement techniques mais aussi des compétences non techniques. La cybersécurité requiert aussi des compétences techniques dans d'autres domaines tels que le management, la psychologie, la politique et/ou le droit afin de répondre à toutes ses facettes (analyse du comportement des utilisateurs finaux, gestion des risques, gestion des relations, communication...) (Graham et Lu, 2022 ; Libicki et al. , 2014 ; Dawson et Thomson, 2018). Dans la figure 12, les femmes ont une tendance à préférer les études de sciences sociales, de journalisme, d'art, de santé, de management et d'éducation qu'importe le degré alors que les hommes ont plus tendance à se diriger vers des études de management, de droit, d'ingénierie et, dans une moindre mesure, les sciences sociales, le journalisme et la santé.

Figure 12 : Nombre total de diplômés des pays de l'OCDE et leur filière d'étude en fonction du degré et de leur genre (OECD Stat, 2020)



2.3. Les métiers⁷⁵

Potter et Vickers (2015) ont identifié dans leur recherche six catégories de professionnels de la cybersécurité.

1. Les analystes

Les analystes offrent des conseils d'expertise et fournissent des informations aux différentes parties prenantes. Ils apportent aussi un soutien à l'équipe cybersécurité en cas d'incidents. Les analystes sont également impliqués dans tout ce qui tourne autour de la gestion des risques et les services de support concernant la sécurité. Pour être performant dans cette fonction, les employés doivent posséder différentes compétences comme le travail en équipe, la conception de processus, l'analyse, l'innovation, la motivation et l'indépendance. Ceux-ci doivent aussi posséder des qualifications et certifications ainsi que de l'expérience et une expertise technique.

2. Les consultants

Les consultants sont des travailleurs indépendants qui apportent leur aide à différentes équipes via leurs analyses et leurs recherches techniques complexes. Ils participent également à l'identification, au développement et à la gestion des relations avec les clients ainsi qu'au développement de solutions. Pour performer, les consultants ont besoin de différentes compétences comme le leadership, les techniques de présentation, la gestion du temps, l'expertise technique, la gestion des risques, l'indépendance, la capacité d'analyse, la communication. Comme pour les analystes, ils doivent avoir certaines qualifications et/ou certifications ainsi que de l'expérience et une expertise technique.

3. Les ingénieurs en sécurité

La fonction d'ingénieur en sécurité est organisée autour de la sécurité des réseaux, la réponse aux menaces, la détection des intrusions et l'évaluation des vulnérabilités. Les ingénieurs en sécurité doivent donc posséder une grande expertise technique ainsi que de bonnes compétences d'analyse. Il est indispensable, pour exercer ce poste, de disposer des qualifications.

4. Les conseillers/évaluateurs de la sécurité

Les conseillers sont principalement impliqués dans la réalisation d'évaluations de la sécurité, de tests de pénétration, d'évaluations de la vulnérabilité et de tâches de conception. Les conseillers et évaluateurs en sécurité ont donc besoin de certaines compétences clés notamment l'analyse, la gestion des relations, la motivation, de bonnes techniques de présentation, la communication. Pour ce genre de fonction, les employés doivent avoir de l'expérience, une (des) qualification(s) et une expertise technique.

5. Les managers

Les emplois de managers concernent les postes de directeur exécutif, de directeur de la cybersécurité, de directeur des opérations ainsi que de responsable des opérations. Ces derniers s'impliquent dans la gestion des équipes, des unités et des centres de sécurité. Pour une bonne gestion, les managers doivent posséder les compétences suivantes : gestion des

⁷⁵ Cf. Annexe D : Les métiers de la cybersécurité

événements/incidents, techniques de présentation, innovation, leadership, gestion des risques, gestion de projet, création et gestion de processus, compétences en matière de conseil, gestion d'équipe. Pour ce faire, ils possèdent une (des) qualification(s) et certification(s), de l'expérience, une bonne expertise technique ainsi qu'en gestion des relations..

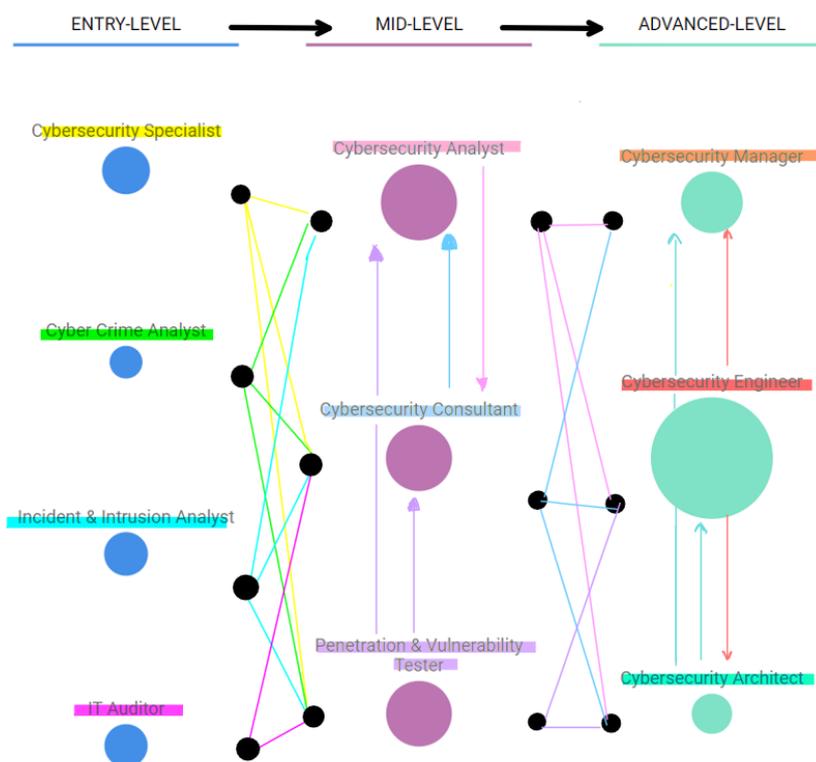
6. Les commerciaux

Les postes de vente ont été décrits comme correspondant à la fonction de responsable du développement commercial, qui est chargé de développer une série de grands comptes d'entreprise dans le domaine de la cybersécurité. Les compétences nécessaires s'étendent de l'expertise technique à l'innovation, en passant par des compétences en présentation, en gestion des relations et en communication. Pour cette position, il est souvent demandé d'avoir une (des) certification(s) et de l'expérience.

Tout au long de leur carrière, les professionnels de la cybersécurité peuvent évoluer et changer de poste. Grâce à un schéma interactif (fig.13), Cyber Seek⁷⁶ représente les principaux emplois en cybersécurité, ainsi que les possibilités de transition fréquentes entre ces fonctions.

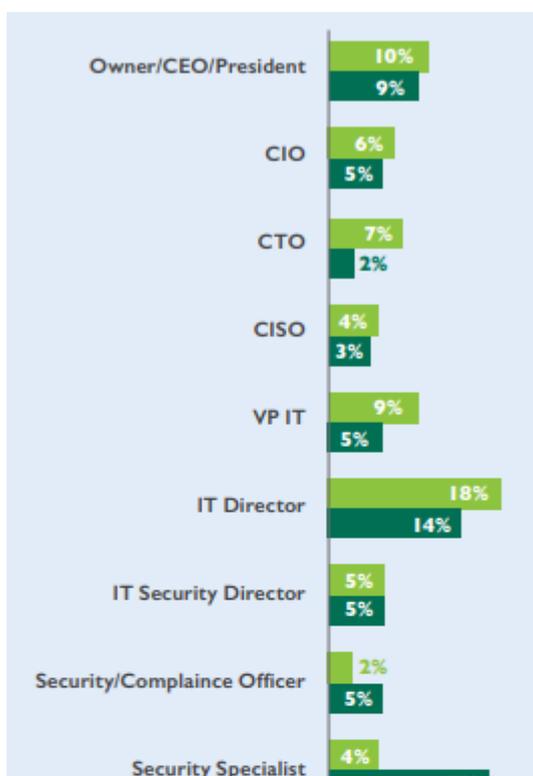
⁷⁶ Cyber Seek fournit des données détaillées sur l'offre et la demande sur le marché de l'emploi dans le domaine de la cybersécurité aux Etats-Unis. Sur leur site Web, il est possible de voir pour chaque emploi le salaire moyen, la demande, les études pour y parvenir, les certifications demandées ainsi que les compétences techniques et non-techniques requises.

Figure 13 : Parcours professionnels en cybersécurité (Cyber Seek, 2023)



2.3.1. La représentation des genres selon l’emplois

Figure 14: Distribution du genre en fonction du poste ((ISC)², 2018, p.7)

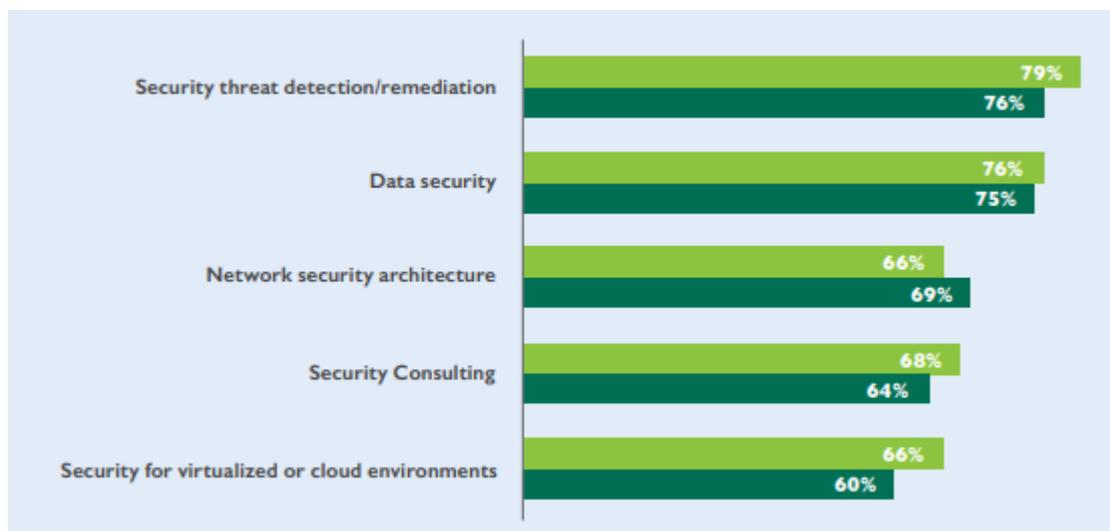


Dans ce graphique (fig.14), (ISC)² a analysé le rapport entre la proportion d'hommes et de femmes en fonction du poste qu'ils occupent dans le secteur de la cybersécurité. Il indique clairement que proportionnellement les femmes occupent plus de postes de direction que les hommes et se situent plus haut dans la hiérarchie de l'entreprise. Cela reflète une plus grande diversité dans les rôles de leadership en cybersécurité.

Cependant, elles restent minoritaires dans les fonctions comme les spécialistes de la sécurité, les administrateurs réseaux/système ou les responsables

de la sécurité et conformité. Ces domaines plus axés sur la technique et les opérations sont encore peu diversifiés. Cet écart peut s'expliquer par la divergence des préférences en termes de carrière ou par les idées préconçues sur ce type de métiers (stéréotypes de genre).

Figure 15 : Les hommes et les femmes font le même travail ((ISC)², 2018, p.9)



Quand l'(ISC)² (2018) a interrogé les hommes et les femmes sur les tâches spécifiques de cybersécurité qu'ils réalisent, ces derniers ont indiqué des responsabilités quasiment identiques (fig.15). Ces résultats démontrent que les femmes ne sont pas cantonnées à des responsabilités spécifiques ou limitées en termes de tâches. Cela prouve que, sur le terrain et peu importe le genre, les responsabilités sont identiques. Cela permet d'approfondir la réflexion sur la figure.... Si les femmes sont sous-représentées dans certains domaines, ce n'est pas à cause de leurs compétences.

2.4. L'expérience

Au fur et à mesure de l'analyse du monde de l'emploi en cybersécurité, nous pouvons constater que l'expérience est extrêmement importante. En effet, dans presque toutes les offres d'emploi concernant la cybersécurité, les employeurs précisent un nombre minimum d'années d'expérience requises (Potter et Vickers, 2015 ; Peslak et Husinger, 2019 ; Parker et Brown, 2019) . En effet, sur le marché australien, toutes les offres d'emploi demandaient un minimum d'expérience en termes de cybersécurité ou de capacité à utiliser une technologie précise (Potter et Vickers, 2015).

Figure 16 : Nombre d'années d'expériences requises pour un emploi en cybersécurité sur le marché sud-africains (Parker et Brown, 2019, p. 186)

Minimum years experience	Frequency	Percentage
2 Years	14	7.1%
3 years	35	17.9%
4 years	16	8.2%
5 Years	46	23.5%
6 Years	9	4.6%
7 Years	8	4.1%
8 Years	19	9.7%
10 Years	11	5.6%
10+Years	2	1.0%
15 Years	3	1.5%
Not Specified	33	16.8%

3. La situation des femmes en cybersécurité

Selon (ISC)², seulement 11%⁷⁷ de femmes travaillent dans le domaine de la cybersécurité en 2017. En 2018, l'(ISC)² a revu sa méthodologie en 2018. Ils ont décidé de redéfinir les véritables acteurs de la cybersécurité afin d'obtenir une image plus précise des personnes effectuant un travail relatif à la cybersécurité c'est-à-dire, des personnes qui ont des responsabilités dans ce domaine (25% de leur temps accordé à des tâches de cybersécurité). Grâce à cette approche plus inclusive, le pourcentage de femmes participant à leur étude s'élève désormais à 24 %⁷⁸ ((ISC)², 2018).

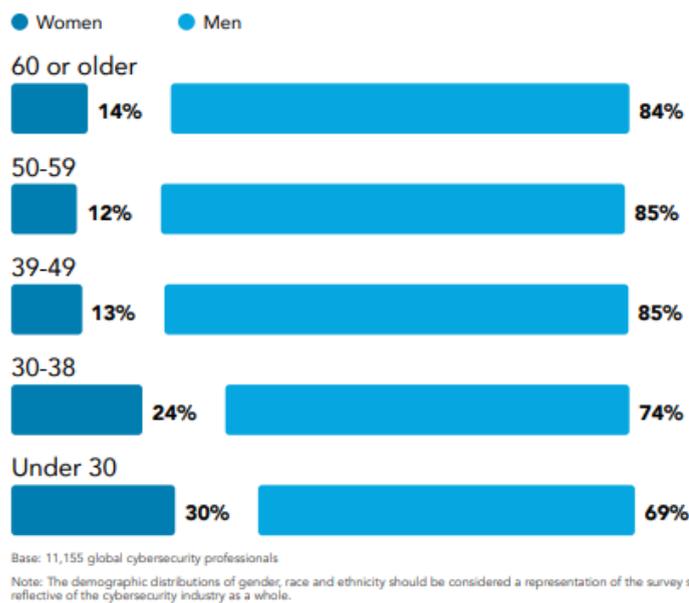
De plus en plus de femmes choisissent des métiers en lien avec la cybersécurité. En effet, comme le montre la figure 17, la plus jeune tranche d'âge des femmes représente 30% de l'effectif en cybersécurité alors que, dans la plus vieille, elles ne représentent que 14% du personnel. Ceci est une conséquence d'une ségrégation professionnelle que les femmes ont subie dans le monde de la cybersécurité (Wirth, 2019). Cette dernière se définit comme *“une situation où les travailleur-ses sont assigné-es, de droit ou de fait, à des professions différentes en fonction de leur sexe”* (Briard, 2020, p.35). De fait, différents types d'obstacles freinent l'entrée des femmes dans certains emplois (Briard, 2020). Cette ségrégation professionnelle explique la surreprésentation des femmes dans les

⁷⁷ (ISC)². (2018). Women in Cybersecurity : Young, Educated and Ready to Take Charge. (ISC)². p.4 <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38>

⁷⁸ Ibid.

niveaux *junior* et dans les classifications d'emploi inférieures⁷⁹. Depuis la phase de recrutement jusqu'à la phase de promotion et de gestion des performances, les femmes font face à des défis. Ce climat peut les mener à quitter le domaine (Wirth, 2019 ; Poster, 2018). Accenture et Girl Who Code ont affirmé dans leur rapport *Resetting tech culture : 5 strategies to keep women in tech* que "50 % des femmes qui acceptent un poste dans la technologie l'abandonnent avant l'âge de 35 ans, contre environ 20 % dans d'autres types d'emplois." (Accenture & Girl Who Code, 2019, p.5).

Figure 17 : Proportion de travailleurs en cybersécurité en fonction de l'âge et du genre ((ISC)², 2022, p.39)



Malgré cette évolution dans le domaine de la cybersécurité, les femmes continuent à se faire discriminer en fonction de leur genre. Dans leur rapport⁸⁰, le Boston Consulting Group cite une étude de (ISC)² et explique que la majorité des femmes qui ont travaillé dans ce domaine déclare avoir été impactée par des discriminations fondées sur le sexe (30%⁸¹). 87%⁸² disent avoir subi de la

⁷⁹ emplois nécessitant moins d'expériences

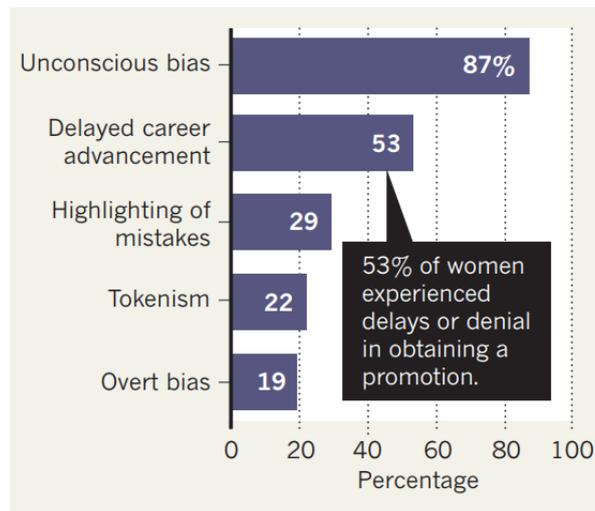
⁸⁰ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

⁸¹ (ISC)². (2022). Cybersecurity Workforce Study. (ISC)². p.42 <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

⁸² Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

discrimination inconsciente⁸³, tandis que 19%⁸⁴ ont subi des discriminations manifestes⁸⁵. Les femmes ont également pointé du doigt des retards inexplicables en termes de promotion et de progression dans leur carrière (53%⁸⁶) ainsi que des réactions exagérées à leurs erreurs (29%⁸⁷) (Panhans et al., 2022). Sue Williamson, professeur associée en gestion des ressources humaines à l'école de commerce de l'UNSW Canberra, décrit la cybersécurité comme un "secteur extrême" dans lequel les préjugés inconscients et la discrimination à l'égard des femmes sont récurrents (Wirth, 2019).

Figure 18 : Types de discriminations reportées⁸⁸ (Poster, 2018, p.578)



3.1. Les freins à la diversité de genre

Une publication par le Ministère australien du Premier Ministre et du cabinet de *Women in Cyber Security Literature Review*, réalisée par une équipe d'universitaires de l'UNSW Canberra, a révélé que le secteur de la cybersécurité n'a cessé de développer au fil du temps des défis persistants et durables pour les femmes. La publication cite la discrimination, l'intransigeante culture organisationnelle (24h/24, 7j/7), l'inégalité salariale, le harcèlement sexuel et le manque de rôles

⁸³ Ce type de discrimination se rapporte aux différents biais inconscients ou préjugés implicites que nous pouvons avoir. En effet, il fait référence aux préjugés et stéréotypes automatiques qui influencent notre comportement.

⁸⁴ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

⁸⁵ Ce type de discrimination désigne des actions intentionnellement discriminatoires envers un individu. Les traitements inégaux et le harcèlement en sont des exemples.

⁸⁶ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

⁸⁷ Ibid.

⁸⁸ 19.641 salariés en cybersécurité échantillonnés.

modèles comme principales causes de la sous-représentation des femmes dans le secteur (Wirth, 2019).

3.1.1. La rémunération

En 2017, 17 %⁸⁹ des femmes ont déclaré gagner entre 50.000 et 99.999 dollars américains, soit 12 points de pourcentage de moins que les hommes (29 %⁹⁰). L'écart de représentation se réduit dans les fonctions disposant d'un plus haut salaire (100.000 \$US et plus). 16 %⁹¹ des femmes annoncent appartenir à cette fourchette contre 20 %⁹² pour les hommes. Malgré cette réduction de l'écart, elles restent proportionnellement moins nombreuses dans cette catégorie. Cette disparité peut en partie s'expliquer par des différences liées à l'âge et à l'expérience professionnelle. Les femmes professionnelles de la cybersécurité sont souvent plus jeunes que leurs homologues masculins (fig17.) et ont généralement moins d'années d'expérience dans ce domaine. Cependant, ces facteurs ne doivent pas minimiser la réalité. A poste égal dans la direction en cybersécurité, les femmes gagnent en moyenne 5.000 dollars US de moins que leurs collègues masculins. Cela indique qu'il subsiste encore des problèmes à résoudre en termes d'égalité salariale et d'équité dans ce secteur ((ISC)², 2018).

“Globalement, les femmes plus jeunes sont confrontées à des écarts de rémunération moins importants que les femmes plus âgées. 21 % des femmes Millennials⁹³ gagnent entre 50.000 et 99.999 dollars [US], contre 29 % des hommes de la même génération. En revanche, seules 10 % des femmes de la génération du baby-boom⁹⁴ gagnent autant, contre 30 % des hommes de la même génération. Il existe un écart de 12 % entre le nombre de femmes de la génération X⁹⁵ qui gagnent entre 50.000 et 99.999 dollars et les hommes de la même génération, et un autre écart de 12 % entre le nombre de femmes du baby-boom qui gagnent plus de 100 000 dollars et les hommes du baby-boom. L'un des écarts salariaux les plus faibles est l'avance de 3 % que les femmes Millennials ont sur les hommes Millennials qui gagnent plus de 100.000 dollars” [Traduction libre] ((ISC)², 2018, p.6).

⁸⁹ (ISC)². (2018). *Women in Cybersecurity - young, educated and ready to take charge*. p.5 <https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38>

⁹⁰ Ibid.

⁹¹ Ibid.

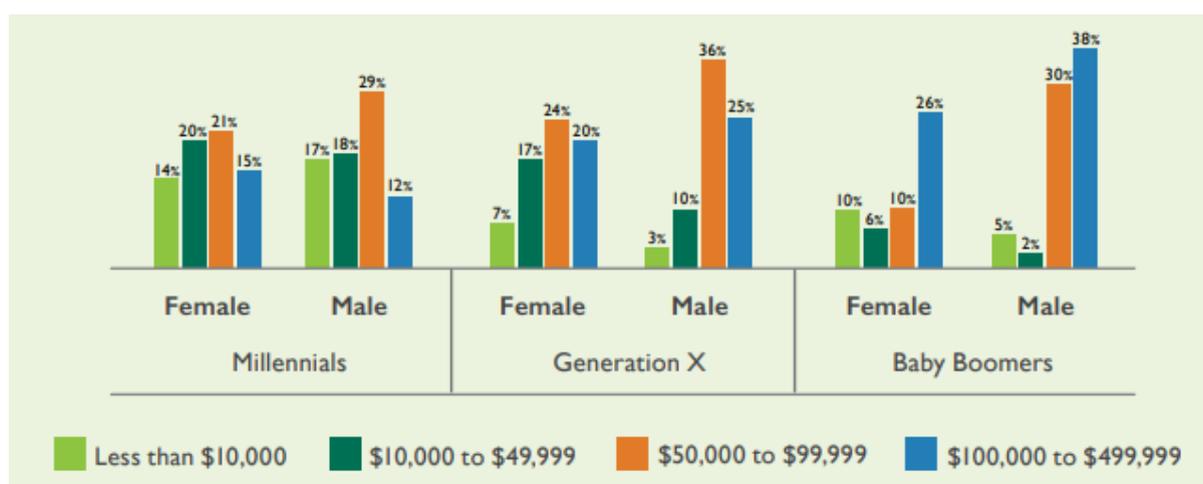
⁹² Ibid.

⁹³ Génération débutant en 1981 et se terminant en 1994 (Lissitsa & Laor, 2021).

⁹⁴ Génération débutant en 1946 et se terminant en 1965 (Lissitsa & Laor, 2021).

⁹⁵ Génération débutant en 1966 et se terminant en 1980 (Lissitsa & Laor, 2021).

Figure 19 : Les femmes plus jeunes connaissent moins d'inégalités salariales ((ISC)², 2018, p.6)



3.1.2. La cybersécurité, c'est pour les hommes

Ce secteur est souvent considéré comme un "club de garçons". Betsy Bevilacqua, ancienne responsable des programmes et opérations de sécurité de l'information chez Facebook, affirme: "Quand les gens pensent à la cybersécurité, ils imaginent un type en sweat à capuche assis devant un ordinateur dans la cave de ses parents en train de pénétrer dans des systèmes." [Traduction libre]⁹⁶

Selon Stanford University's Clayman Institute for Gender Research (2017), "l'image culturelle de la technologie en tant qu'espace pour les gars obsédés par le codage et les geeks contribue plus fortement aux écarts importants entre les hommes et les femmes dans le domaine de la technologie"⁹⁷ [Traduction libre]. En s'appuyant sur un rapport⁹⁸ de Tessian⁹⁹, Bishop (2020) confirme que les professionnels de la cybersécurité ont cette image de jeunes hommes blancs travaillant dans des sous-sols, vêtus de sweats à capuche. Les femmes désirant suivre des études et faire carrière dans la technologie peuvent avoir le sentiment de ne pas faire partie de ce "club masculin". Cette marginalisation entraîne l'isolement des femmes et, donc, est une raison de cette sous-représentation féminine (Deloitte, 2021 ; Stanford University's Clayman Institute for Gender Research, 2017 ; Panhans et al., 2022 ; Weingarten et Garcia, 2015).

⁹⁶ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

⁹⁷ The Clayman Institute for Gender Research. (2017). Alignment with gender stereotypes predicts success in tech. *Stanford University*. <https://gender.stanford.edu/news/alignment-gender-stereotypes-predicts-success-tech>

⁹⁸ Ils ont interrogé 200 femmes professionnelles de la cybersécurité aux États-Unis et au Royaume-Uni

⁹⁹ "Tessian est une plateforme cloud de sécurité des emails qui protège intelligemment les organisations contre les menaces avancées et la perte de données sur les emails, tout en informant les employés sur les menaces de sécurité à l'instant même". (Tessian. (s. d.). Tessian | LinkedIn. <https://www.linkedin.com/company/tessian/?originalSubdomain=fr>)

Par ailleurs, le Boston Consulting Group a mené une enquête mondiale en 2022 auprès de 2.000 étudiantes de premier cycle en sciences et technologies. 47 %¹⁰⁰ des femmes interrogées ont simplement affirmé qu'elles n'étaient pas intéressées par une carrière dans ce secteur. En cherchant leurs raisons, Panhans et al. (2022) ont ressorti de leur enquête qu'elles n'y avaient jamais pensé. Cela laisse deviner que l'idée qu'elles se faisaient de la cybersécurité ne correspondait pas à leurs attentes concernant leur vie professionnelle. Tout cela mène au fait qu'il existe peu de possibilités pour les femmes de participer à des projets, des stages et d'autres expériences dans le domaine de la cybersécurité afin de remettre en question leurs propres préjugés sur les professions du secteur (Panhans et al., 2022 ; Tessian, 2021).

3.1.3. L'accès aux études STIM¹⁰¹, le choix de carrière et les constructions sociales

Les stéréotypes concernant les femmes et les domaines scientifiques et technologiques commencent dès l'école primaire. Dès leur plus jeune âge, les enfants sont influencés dans leur manière d'appréhender les sciences, les mathématiques et l'ingénierie. Ils pensent que ces domaines sont réservés aux garçons (Wirth, 2019). Malgré cela, 82 %¹⁰² des étudiantes interrogées par le Boston Consulting Group ont affirmé avoir une certaine ou une grande connaissance de la cybersécurité. De plus, 58 %¹⁰³ affirment avoir accès à une formation en cybersécurité et 68 %¹⁰⁴ ont déjà suivi un cours relatif à la cybersécurité. Le monde de la cybersécurité n'est donc pas invisible à leurs yeux. Elles s'y intéressent pendant leurs études. Le problème n'est donc pas l'accès aux différentes formations. Le vrai problème, ce sont les règles de la société ou de la culture qui empêchent les femmes de choisir librement leurs études et/ou leurs emplois.

Certaines femmes ne voient pas la cybersécurité comme un bon choix de carrière. En effet, selon l'étude du Boston Consulting Group (2022), les femmes ont trois principaux critères lorsqu'elles choisissent leur voie professionnelle : leur contribution à la société, un salaire élevé et l'équilibre vie professionnelle et vie privée. 37 %¹⁰⁵ des participantes considèrent que la cybersécurité est un domaine où il est difficile d'atteindre cet équilibre. Pour illustrer l'importance de l'équilibre vie professionnelle et vie privée pour les femmes, Weingarten et Garcia (2015) mettent en lumière que, dans le monde du travail, les femmes sont encore forcées de faire le choix entre les soins à une personne tiers et leur carrière. Les responsabilités familiales et autres travaux domestiques non rémunérés sont un frein à l'entrée des femmes ou à leur évolution dans le domaine exigeant de la cybersécurité. En effet, les femmes sont toujours celles qui font le plus de tâches ménagères et de soins non rémunérés, en moyenne trois fois plus que les hommes. Cela s'illustre par la baisse du taux

¹⁰⁰ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*.

¹⁰¹ Sciences, technologie, ingénierie et mathématiques

¹⁰² Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*.

¹⁰³ Ibid.

¹⁰⁴ Ibid.

¹⁰⁵ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*.

de participation des femmes sur le marché de l'emploi. D'ici 2030, il sera de 46%¹⁰⁶, le niveau le plus bas depuis 40 ans contre 72%¹⁰⁷ pour les hommes.

En outre, les femmes qui travaillent dans des domaines où la plupart des employés sont des hommes peuvent se sentir exclues et douter de leurs compétences quand bien même elles soient compétentes et aient prouvé leur légitimité par diverses réussites.

Les règles et les attentes injustes de la société continuent de les empêcher de rentrer pleinement dans les domaines des STIM, dont la cybersécurité. Si les mentalités n'évoluent pas, il faudra plus de 130 ans pour réduire les différences entre hommes et femmes dans le monde (Panhans et al., 2022).

3.1.4. Le harcèlement et la discrimination

Le harcèlement sexuel ainsi que les discriminations sont encore monnaies courantes dans les différentes professions de la cybersécurité. En 2017, un mémo d'un employé masculin de Google fuite. Il y était inscrit que *"les femmes sont biologiquement inadaptées au domaine technologique"*¹⁰⁸. Les conférences sur la cybersécurité sont largement dominées par les hommes que ce soit numériquement ou dans le ressenti. Souvent, il arrive qu'une femme se retrouve seule parmi une centaine d'hommes. Deux des conférences les plus importantes dans le domaine de la cybersécurité, DEF CON et Black Hat, se déroulent à Las Vegas (Nevada, USA). Plusieurs femmes participant à ces conférences ont rapporté à des chercheurs ou à leur communauté sur les réseaux sociaux qu'elles ont été touchées de manière inappropriée et confrontées à des commentaires désobligeants de la part d'hommes. Ces derniers les considéraient simplement comme des secrétaires ou, encore, des prostituées (Poster, 2018).

3.2. Les pistes pour remédier au problème de représentation du genre

Pour augmenter leur diversité de genre, les entreprises doivent entreprendre un changement dans leur stratégie de recrutement ainsi que développer plusieurs initiatives pour attirer et retenir leurs minorités. Ce changement de perspective doit également s'accompagner d'une modification de la manière dont les médias et d'autres acteurs décrivent généralement le *"visage de la sécurité"*. Il est important de mettre en avant les vraies compétences et responsabilités relatives aux professions de la cybersécurité. Cette transition permet aussi d'élargir la discussion sur l'équité au sein de l'industrie de la cybersécurité et sur les différents acteurs qui la promeuvent. Actuellement, les femmes représentent moins de 25% de la main-d'œuvre dans ce domaine, selon les données du rapport de 2018 d'(ISC)². Afin d'encourager plus de femmes à entrer dans le secteur de la cybersécurité, il est important de transformer les perceptions et les environnements de travail. Il faut que les femmes perçoivent ces carrières comme étant inclusives et porteuses d'opportunités. Dans le rapport de

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

¹⁰⁸ Poster, W. R. (2018). Cybersecurity needs women. *Nature*, 555(7698), p.579

Tessian, les femmes donnent déjà quelques pistes que les entreprises pourraient suivre afin d'augmenter la représentation des femmes dans leurs bureaux (fig.20).

Figure 20: Comment attirer des femmes dans les professions de la cybersécurité? (Tessian, 2021, p.9)

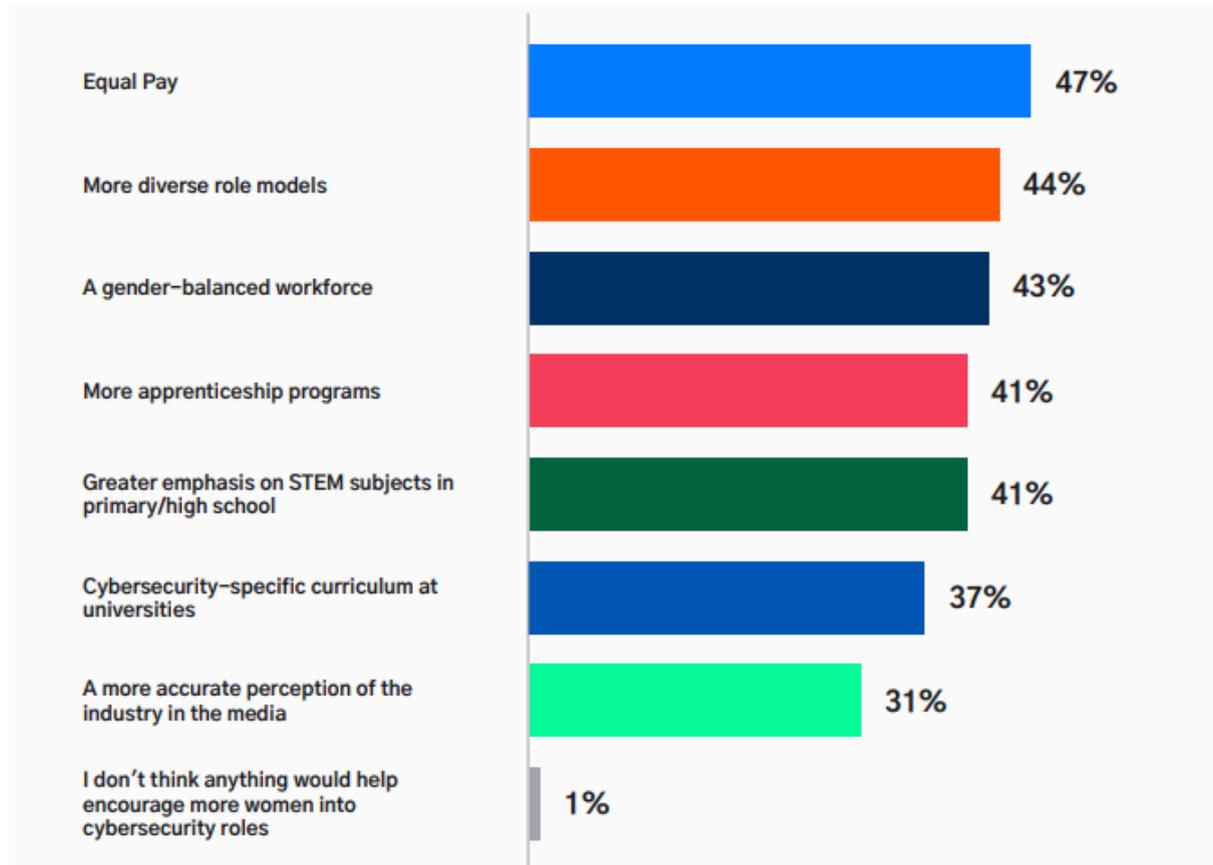


Figure 21 : Le top trois des priorités de carrière des femmes selon leur région (Panhans et al., 2022)

	Having flexibility to balance work and family needs	Having a high-paying job	Making a meaningful contribution to society	Having opportunities for promotion and advancement	Being in a workplace that is welcoming to people like me	Having a job that others respect and value
Asia-Pacific	1	2	3			
Latin America		1	2	3		
Europe	2		3		1	
Middle East and North Africa				1	3	2
North America	1	3	2			
Sub-Saharan Africa			1	2		3

Source: BCG research.

3.2.1. Les communautés de femmes dans la cybersécurité

Il est important d'encourager les initiatives visant à promouvoir la technologie auprès des femmes et des adolescentes. Ces mouvements sont importants pour accroître leur représentation dans le domaine de la cybersécurité. Ces dernières années, ils ont été de plus en plus soutenus par des organisations internationales œuvrant pour l'égalité des sexes (Panhans et al., 2022 ; Poster, 2018).

Exemples de différents organismes impliqués dans le développement de la main-d'oeuvre féminine en cybersécurité

- *Women4Cyber (Women4Cyber, 2023)*

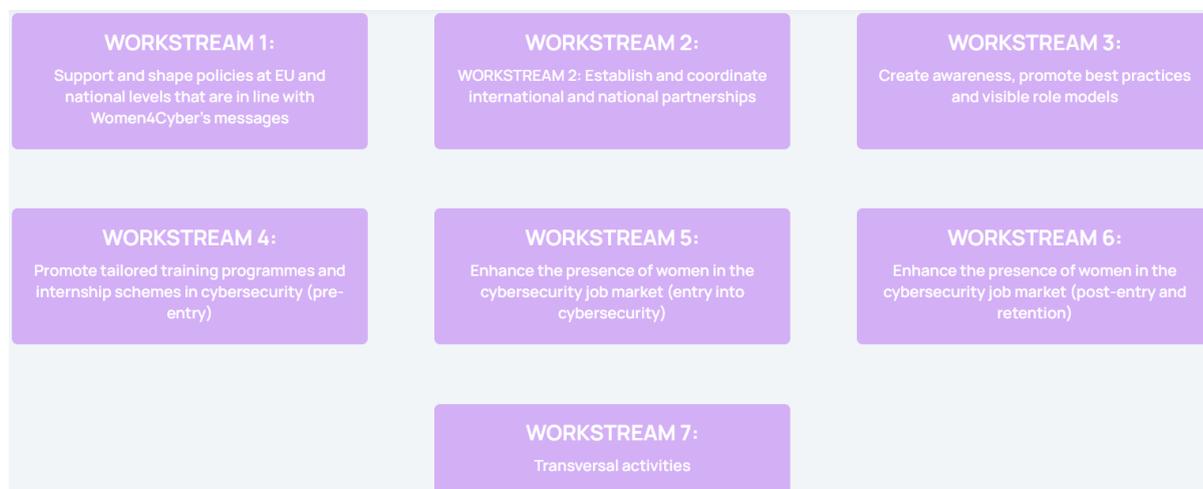
Figure 22 : Les différents chapitres de Women4Cyber (Brugman, 2022, p.4)



Women4Cyber est une fondation privée européenne à but non lucratif. Elle a pour but de promouvoir, d'encourager et de soutenir la participation des femmes dans le domaine de la cybersécurité. Avant tout, *Woman4Cyber* est une communauté. Cette dernière s'est énormément développée ces dernières années. L'organisation a ouvert le chapitre belge l'année dernière. Toute cette communauté se compose de près de 35.000 membres à travers l'Europe. La communauté LinkedIn a doublé en 2022. Elle est passée de 4.800 membres à près de 9.000. W4C collabore directement avec la DG CNECT de la Commission européenne pour son registre

Women4Cyber, une base de données d'expertes en cybersécurité en Europe.

Figure 23 : Les flux de travail de *Women4Cyber* (*Women4Cyber*, 2022)



Women4Cyber travaille tant sur la promotion des femmes en cybersécurité que sur la création de partenariat avec des agents influents (gouvernement, université...) et sur la création de programmes de mentorat soutenus par de forts modèles féminins en cybersécurité (fig...). Par exemple, en février 2022, W4C a publié son livre *"Hacking gender barrier : Europe's top cyber women"* afin de mettre en lumière une centaine de *cyber-femmes* européennes. Un autre exemple d'initiatives menées par *Women4Cyber* est une newsletter bimensuelle. Cette newsletter est envoyée à plus de 600 personnes et partagent toutes les dernières nouvelles sur leurs activités, les chapitres, les informations sur la cybersécurité, les événements prévus, etc. *Women4Cyber* prend régulièrement part à des groupes de discussions et à des événements à travers l'Europe.

- *Girls Who Code* (*Girls Who Code*, 2023)

Girls Who Code est une organisation à but non lucratif qui se consacre à encourager et à accroître la présence des femmes dans le domaine de l'informatique. Afin de développer cette main-d'œuvre féminine, elle fournit aux jeunes femmes les compétences techniques et non techniques essentielles pour saisir les opportunités du 21e siècle. En plus de promouvoir la parité dans les métiers de l'informatique, *Girls Who Code* souhaite changer l'image associée aux développeurs informatiques. *Girls Who Code* développe plusieurs programmes, notamment un stage de sept semaines en été, un programme universitaire spécialisé de deux semaines et des clubs parascolaires. De cette façon, ils ont aidé, depuis leur fondation en 2012, près de 580.000 étudiantes.

En 2022, ils ont développé des programmes à suivre en ligne afin d'augmenter le taux de participation. En effet, cet enseignement virtuel a permis de toucher toutes les femmes et jeunes filles contraintes par un emploi, des responsabilités de soins et d'autres activités. Pour les étudiantes universitaires, ils ont aussi développé deux programmes : *Technical Interview Prep* (préparation à l'entretien technique) et *Leadership Academy* (développement de compétences de mentorat et de gestion de projet).

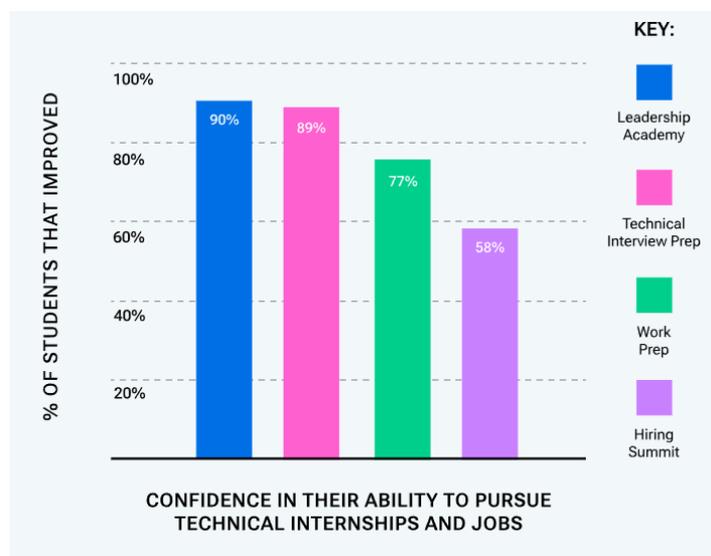
Figure 24 : Nombre d'étudiantes servies par programme (Girls Who Code, 2022, p.3)



Figure 25 : Présence de Girls Who Code à travers le monde (Girls Who Code, 2022, p.4)

Albania	Colombia	Indonesia	Peru	Turkey
Argentina	Costa Rica	Ireland	Philippines	Uganda
Bahamas	Ecuador	Israel	Poland	United Arab Emirates
Bahrain	Egypt	Jamaica	Qatar	United Kingdom
Bangladesh	El Salvador	Kazakhstan	Rwanda	United States
Barbados	Ethiopia	Korea, South	Saudi Arabia	Uzbekistan
Belize	Georgia	Mexico	Singapore	Vietnam
Brazil	Ghana	Moldova	South Africa	
Bulgarie	Greece	Morocco	Spain	
Burma	Honduras	Nepal	Taiwan	
Cambodia	Hungary	Nigeria	Tanzania	
Canada	India	Pakistan	Trinidad and Tobago	

Figure 26 : Résultats à court terme de leur programme pour les étudiantes universitaires (Girls Who Code, 2022, p.7)



Le développement de communautés comme *Girls Who Code* et *Women4Cyber* est très important pour les femmes. Elles leur permettent de prendre confiance (fig. 26). Par ces communautés¹⁰⁹, elles ne se sentent plus seules. De plus, les mentors et les parrains sont essentiels pour aider les jeunes filles et les femmes à s'orienter dans l'ensemble du secteur et développer leurs compétences (Panhans et al., 2022).

¹⁰⁹ Cf. Annexe E : Exemples de communautés de femmes en cybersécurité

3.2.2. La création d'une culture plus inclusive

Les individus sont attirés par les organisations qui reflètent leurs valeurs ou qui correspondent à leurs intérêts. Si le candidat constate qu'une organisation ne correspond pas à ses valeurs, il sera plus enclin à se retirer du processus de recrutement et de trouver une meilleure correspondance (Cha et Edmondson, 2006 ; De Cooman et al., 2009 cités par Dawson et Thomson, 2018).

Pour attirer et retenir les femmes dans le secteur de la cybersécurité, il faut s'intéresser à la rémunération, aux préjugés sexistes, etc. (Tessian, 2019; Poster, 2018 ; Panhans et al., 2022). En 2019, Accenture et Girls Who Code ont mené une étude¹¹⁰ sur l'établissement d'une culture inclusive au sein des entreprises technologiques ainsi que sur les avantages qui en découlent. Ils ont découvert que le développement des opportunités pour les femmes dans la *tech* repose sur une culture inclusive. Les entreprises ne doivent pas montrer seulement une diversité en apparence. Leur culture doit favoriser la prise de parole au sein de leurs bureaux. Accenture et Girls Who Code ont donc exposé les aspects spécifiques de l'environnement qui favorisent la progression et l'épanouissement des femmes dans le secteur technologique. La différence entre les environnements les plus inclusifs et les moins inclusifs est considérable. En outre, ce rapport dévoile également un écart entre l'expérience de terrain des femmes et la perception que les professionnels des ressources humaines ont de leur organisation. Ces derniers surestiment souvent le degré de soutien envers les femmes. Un peu moins de la moitié (45 %¹¹¹) pensent qu'il est "*facile pour les femmes de s'épanouir dans la technologie*"¹¹² contrairement à un cinquième (21%¹¹³) des participantes à l'enquête. Ils ne sont pas non plus convaincus du pouvoir de la culture comme étant un outil d'attraction et de rétention des femmes dans la technologie. Seulement, 38%¹¹⁴ des responsables en ressources humaines considèrent qu'une culture plus inclusive est efficace. Néanmoins, la culture de l'entreprise est un facteur décisif pour une femme. 37%¹¹⁵ des femmes accusent la culture d'entreprise comme principal facteur de leur choix de partir de l'entreprise. Quant à lui, le manque de diversité représente 10%¹¹⁶ des raisons de départ d'employées (Accenture & Girls Who Code, 2019).

Lorsque Accenture et Girls Who Code (2019) ont demandé comment les entreprises pourraient attirer davantage de personnes, 51 %¹¹⁷ des femmes ont évoqué l'importance de la culture et du soutien sur leur lieu de travail.

¹¹⁰ Cette étude s'appuie sur trois enquêtes en ligne menées aux États-Unis entre février et juillet 2019. Accenture et Girls Who Code ont recueilli l'avis de 2.700 étudiants universitaires, 500 cadres RH, 1.990 travailleurs de la technologie.

¹¹¹ Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 20 <https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-134/accenture-a4-gwc-report-final1.pdf#zoom%3D50>

¹¹² [Traduction libre] Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 3

¹¹³ Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 3

¹¹⁴ Ibid

¹¹⁵ Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 16

¹¹⁶ Ibid.

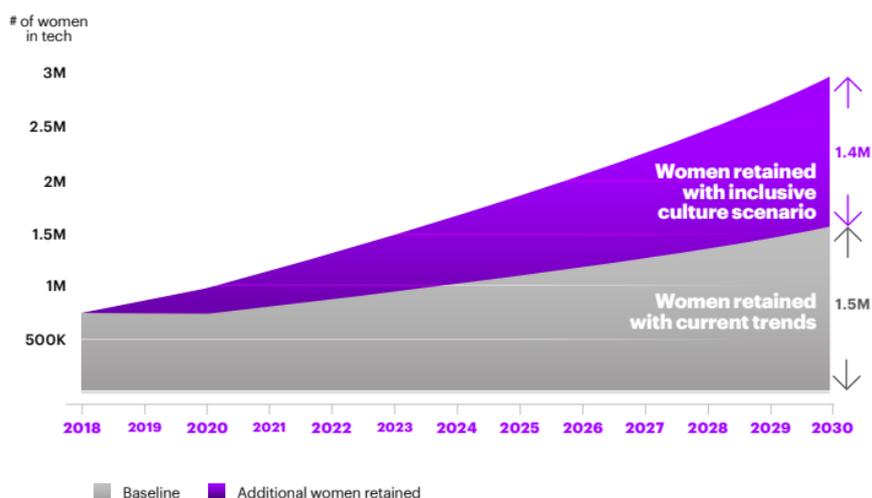
¹¹⁷ Ibid.

Figure 27 : L'expérience des femmes au sein de leur entreprise du domaine de la technologie
(Accenture & Girls Who Code, 2019, p.17)

Women's workplace experiences	In more-inclusive workplace cultures	In less-inclusive workplace cultures
Love their job	85%	28%
Been promoted	66%	42%
Likelihood of advancing to manager	45%	28%
Colleagues assume they are more junior than male peers	33%	63%
Made to feel that the job is not for "people like them"	16%	50%
Have heard or read inappropriate remarks or comments	15%	54%
Likelihood of leaving tech	1%	21%

Si toutes les entreprises possédaient une culture semblable à celle des 20% les plus inclusives, le taux de départ annuel des femmes dans la *tech* pourrait passer de 4,6%¹¹⁸ à 1,3%¹¹⁹, soit une chute de 70%. Ainsi, d'ici 2030, le nombre de femmes employées dans la *tech* pourrait atteindre environ 3 millions soit, près du double des 1,5 millions prévus si les tendances actuelles se maintiennent. Il est donc possible d'augmenter presque de moitié le nombre de femmes travaillant dans le secteur technologique avant 2030 (Accenture & Girls Who Code, 2019).

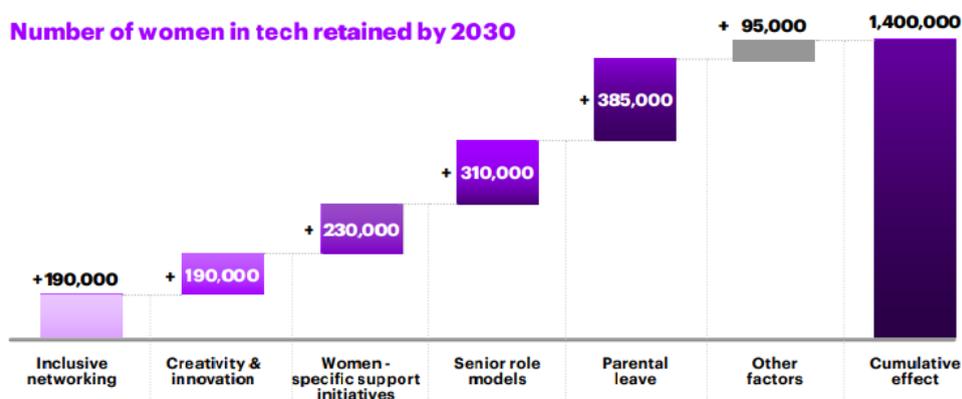
Figure 28 : Doubler le nombre de femmes en tech d'ici 2030 (Accenture & Girls Who Code, 2019, p.22)



¹¹⁸ Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 22

¹¹⁹ Ibid.

Figure 29 : Actions pouvant retenir les femmes dans leur emploi dans la technologie (Accenture & Girls Who Code, 2019, p.26)



Cela pourrait aider à retenir 1,4 million de femmes dans la technologie d'ici 2030 (Accenture & Girls Who Code, 2019).

3.2.3. Le recrutement : ouvrir les portes à différents talents

Le processus de recrutement est composé de plusieurs étapes : les candidatures, les entretiens, la sélection et l'intégration. Dans le domaine de la cybersécurité, le défi du recrutement consiste à assurer les mêmes chances à chaque candidat qui se présente, homme ou femme. Le regard du recruteur sur le/la candidat(e) est biaisé parce qu'à cette étape du recrutement, il recherche le "candidat parfait". Les recruteurs ont tendance à rechercher des profils identiques à ceux qu'ils ont déjà dans leur organisation c'est-à-dire, un individu possédant l'ancienneté, l'éducation et l'expertise technique requises. A cause de la conjoncture actuelle du marché de l'emploi en cybersécurité, ils sont friands de profils qui requièrent peu de formations. Cette approche peut exclure les femmes, en particulier les jeunes femmes qui débudent dans le domaine, et aggrave le manque de main-d'œuvre. Pour améliorer l'accès aux professions en cybersécurité, il serait judicieux d'adopter une perspective plus large et d'envisager des candidats moins traditionnels comme des candidats venant d'études non techniques (sciences sociales, sciences humaines, droit et politique, etc.). En recrutant selon les aptitudes non techniques et en offrant des perspectives de formations spécifiques en cybersécurité, les recruteurs pourront réduire la pénurie de main-d'oeuvre et contribuer au renforcement de l'accès à ce type d'emploi, pour les femmes notamment (Deloitte, 2021 ; Panhans et al., 2022).

En pratique, les recruteurs pourraient aussi rédiger des offres d'emploi de manière inclusive ainsi que faire appel à des comités de sélection diversifiés et procéder à un examen des CV sans distinction de sexe (Poster, 2018). Il existe des organisations qui aident à répondre au besoin de plus de diversité dans les processus d'embauche, telles que : Bluescreen IT's HACKED, Crucial Group's Academy, TechTalent Academy's Women in Cyber Academy et NeuroCyberUK (Deloitte, 2021).

Les biais rencontrés durant le recrutement peuvent aussi se manifester durant les évaluations de performance, les décisions prises concernant les promotions, ainsi que dans les systèmes de récompense basés sur le mérite. Une nouvelle approche plus inclusive du recrutement peut aider à développer de nouvelles perspectives et valeurs dans le secteur de la cybersécurité (Deloitte, 2021).

3.2.4. Le développement de modèles féminins au sein de l'industrie

52 %¹²⁰ ont mentionné la nécessité d'avoir plus de modèles à suivre (Accenture & Girls Who Code, 2019). En effet, les femmes expérimentées en cybersécurité peuvent inspirer celles qui se trouvent au début de leur carrière. Elles sont là aussi pour guider les nouvelles générations en leur expliquant les différents moyens d'évoluer, de se développer en cybersécurité (Panhans et al., 2022).

Betsy Bevilacqua, de Facebook : "*Comparé à d'autres carrières dans la technologie, le parcours d'un ingénieur en sécurité n'est pas clair. Il y a de nombreuses directions possibles. Les femmes dans la cybersécurité ont besoin de plus de soutien pour naviguer dans les différents niveaux de carrière, car nous n'avons pas de manuel de jeu*"¹²¹.

Il est prouvé que plus il y a de femmes qui s'épanouissent dans la cybersécurité, plus elles peuvent attirer d'autres femmes dans le domaine ((ISC)², 2018). 70 % des femmes ayant une certaine expérience en cybersécurité interrogées par le Boston Consulting Group (2022) déclarent qu'un modèle les avait encouragées à développer leurs connaissances ainsi que leurs compétences dans ce domaine (Panhans et al., 2022).

Malgré les bienfaits du soutien de femmes expérimentées en cybersécurité, un rapport de Kaspersky Lab (cité par Bishop, 2020) a révélé que seulement 11 % des jeunes filles en ont rencontrées. L'absence de modèles féminins forts contribue au flou concernant les possibilités de parcours professionnels pour les femmes, notamment en début de carrière. Lorsque les jeunes femmes ont des exemples auxquels elles peuvent s'identifier, cela peut rendre ces rôles plus accessibles, attrayants et inclusifs. L'ensemble de l'industrie pourrait développer ces initiatives au sein des entreprises. En effet, ces dernières devraient envisager le développement de programmes de mentorat bien structurés et encourager les employés à participer à des mouvements tels que Girls Who Code (Bishop, 2020).

3.2.5. La visibilité sur les différentes compétences nécessaires en cybersécurité

Les études et autres formations réalisées en dehors des domaines des STIM sont souvent négligées par les acteurs du monde de la cybersécurité. Cependant, les emplois en cybersécurité nécessitent un panel de compétences, allant de la gestion de personnel à la création de solutions et à la détection des menaces. Ces dernières années, de nombreuses grandes entreprises technologiques modifient leur perspective. Par exemple, en 2011, Bill Gates, le cofondateur de Microsoft, critiquait l'enseignement du droit dans les métiers technologiques. Aujourd'hui, le président de l'entreprise,

¹²⁰ Accenture & Girls Who Code. (2019). Resetting Tech Culture : 5 strategies to keep women in tech. p. 16

¹²¹ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*.

Brad Smith, affirme que cette formation est cruciale pour l'avenir de l'informatique, en particulier pour le domaine de l'intelligence artificielle (Poster, 2018 ; Bishop, 2020). En effet, la créativité et le travail d'équipe sont nécessaires pour s'épanouir pleinement en cybersécurité, au même titre que l'analyse de données, la pensée analytique et les compétences techniques. En sensibilisant le monde de l'emploi à la diversité de compétences requises en cybersécurité, les organisations pourraient aider à résorber l'écart entre les sexes et le déficit de compétences (Bishop, 2020 ; Weingarten et Garcia, 2015 ; Wirth, 2019).

Bianca Wirth, responsable de l'éducation et de la sensibilisation à la sécurité des entreprises chez International Airlines Group déclare que "*Nous assistons à l'émergence de rôles plus variés tels que la gestion des parties prenantes, l'éducation et la sensibilisation, la communication et la gestion de projets spécialisés dans la cybersécurité*"¹²².

Concrètement, afin de sensibiliser le grand public aux différentes compétences requises en cybersécurité, les entreprises pourraient développer une communauté que ce soit au travail ou sur les réseaux sociaux. Les employés en cybersécurité partageront ainsi leurs expériences et les diverses compétences qui ont contribué à leur succès dans leur métier. Il est également essentiel de prêter attention à la manière dont les descriptions de poste sont formulées. L'inclusion de compétences telles que la créativité, le travail d'équipe et la communication dans la liste des compétences requises favoriserait la diversité des candidatures au poste à pourvoir (Bishop, 2020).

3.2.6. L'évolution des établissements d'enseignement supérieur

Il est important d'intéresser les filles aux STIM dès le plus jeune âge. Beaucoup de femmes affirment s'intéresser aux STIM durant les études secondaires (Panhans et al., 2022). Jay Koehler, ancien responsable de la diversité, de l'inclusion et de l'équité chez Cisco Systems, affirme que "*si vous n'intéressez pas les filles avant le lycée, vous les avez déjà perdues*". Les établissements d'enseignement supérieur sont essentiels pour combler la pénurie de femmes dans le domaine, que ce soit en amont ou en aval de l'embauche (Panhans et al., 2022 ; Meier et Roy, 2022).

Les femmes qui étudient à l'université sont plus disposées à rester dans des programmes technologiques si elles se sentent à l'aise et soutenues dans leur expérience en classe (Accenture & Girl Who Code, 2019).

¹²² Wirth B. (2019). Why bringing more women into the cybersecurity workforce is a matter of national security. UNSW BusinessThink.
<https://www.businessthink.unsw.edu.au/articles/Why-bringing-on-more-cyber-women-is-a-matter-of-national-security>

Figure 30 : l'expérience des femmes en STIM à l'université (Accenture & Girls Who Code, 2019, p.13)

Women's college experiences	In more-inclusive college cultures	In less-inclusive college cultures
See a clear pathway from studies to a career	93%	73%
Feel they belong	89%	37%
Plan to look for a tech role after college	85%	64%
Feel comfortable asking questions	83%	46%
Feel like an outsider	5%	25%

Le fait d'avoir une culture plus inclusive au sein des universités a un impact significatif sur la rétention des femmes au sein de ces études ainsi que sur leur envie de travailler dans le domaine après. Cette tendance se vérifie aussi chez les hommes (Accenture & Girls Who Code, 2019).

3.2.7. Le changement de la perception des femmes en ce qui concerne la cybersécurité

Historiquement, les femmes ont joué un rôle pionnier en tant que programmeuses. En réalité, à l'origine, le terme "ordinateur" ne faisait pas référence à la machine elle-même, mais aux femmes qui la programmaient. À cette époque, c'était une profession à prédominance féminine. Au fil des années ainsi qu'avec l'augmentation de la puissance informatique et les salaires attractifs, les hommes sont arrivés dans le secteur. De plus, à partir de 1980 et de l'arrivée de l'ordinateur personnel, la culture *geek* s'est développée. Cette dernière a engendré l'image de l'homme blanc boutonéux qui passe ses journées devant son ordinateur qu'on a aujourd'hui (Poster, 2018 ; Wirth, 2019). Cette image préconçue et inexacte des informaticiens peut rendre l'industrie inintéressante ou inaccessible pour de nombreux candidats (Bishop, 2020). Il est donc essentiel de corriger les préjugés selon lesquels les carrières en cybersécurité sont principalement réservées aux garçons ou à une petite élite. Les potentiels candidats pensent également que la cybersécurité est un domaine difficile qui se résume à une dévotion totale (Deloitte, 2021; Panhans et al., 2022). En effet, il est essentiel d'adopter une représentation médiatique plus exacte et véridique afin d'inciter plus de femmes à envisager des postes dans la cybersécurité. Les entreprises et les établissements scolaires doivent travailler leur image afin de rendre la cybersécurité accessible (Tessian, 2021 ; Bishop, 2020).

"Nous devons recadrer la cybersécurité comme étant bien plus qu'un domaine purement technique"¹²³, affirme Nadya Bartol, directrice générale de Platinion, une entreprise spécialisée du BCG axée sur le numérique. "Les femmes ont beaucoup à offrir dans un domaine qui nécessite une

¹²³ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*.

combinaison de compétences en matière de personnel, de processus et de technologie pour réussir."¹²⁴

Les femmes ayant une compréhension limitée de la cybersécurité ont tendance à percevoir les professionnels de ce domaine comme des individus "hautement intellectuels" ou des "hackers". En revanche, celles qui possèdent une meilleure connaissance de la cybersécurité adoptent une vision plus positive de ces travailleurs, les considérant comme des "codeurs créatifs" ou des "experts en programmation" (Panhans et al., 2022).

4. Investir dans la diversité

Rupal Hollenbeck, président de Check Point Software, a déclaré : *"Il n'y a rien de plus excitant que de rassembler un groupe diversifié de personnes, de faire ressortir le meilleur d'elles-mêmes et de leur permettre de courir pour qu'au final, elles réalisent quelque chose qu'elles n'auraient jamais cru possible... C'est de la pure magie"* [Traduction libre].¹²⁵

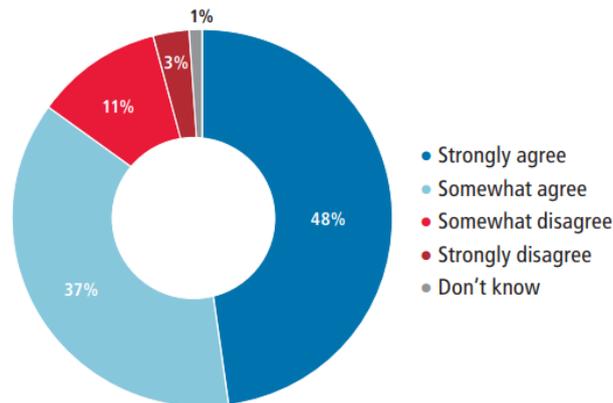
Aujourd'hui, les dirigeants comprennent que leurs entreprises ne peuvent pas réussir à l'échelle mondiale si elles n'ont pas une main-d'œuvre diversifiée. Presque toutes les entreprises de l'enquête de Forbes Insight (2021) (97%¹²⁶) ont développé des stratégies formelles de diversité et d'inclusion. Une main-d'œuvre diversifiée et inclusive est nécessaire pour stimuler l'innovation, favoriser la créativité et orienter les stratégies commerciales (fig...). La diversité de points de vue engendrent de nouvelles idées, de nouveaux services et de nouveaux produits, et encouragent une pensée novatrice. Les entreprises ne considèrent plus la diversité et l'inclusion comme un effort. Ils reconnaissent ces initiatives comme une autre pratique commerciale, celle de les différencier de leurs concurrents et de les aider à attirer de nouveaux clients (Wirth, 2019 ; Forbes Insight, 2021).

Figure... : Une main-d'oeuvre diversifiée est importante pour stimuler la créativité et l'innovation (Forbes Insight, 2021, p.5)

¹²⁴ Ibid.

¹²⁵ Check Point Research Team. (2023). International Women's Day : Achieving gender parity in the C-Suite and advancing equity in the cybersecurity . . . Check Point Blog. <https://blog.checkpoint.com/2023/03/08/international-womens-day-achieving-gender-parity-in-the-c-suite-and-advancing-equity-in-the-cybersecurity-industry/>

¹²⁶ *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce*. (2021). Forbes Insight. p.11



De plus, en développant une main-d'œuvre diversifiée, les entreprises peuvent réduire le risque de maladroites concernant le genre et la culture de leurs clients (Forbes Insight, 2021).

4.1. Investir dans la diversité de genre

Investir dans la diversité de genre est important pour les entreprises. En effet, les femmes ont quelque chose de différent à apporter aux entreprises. Premièrement, une abondante littérature suggère que les femmes ajoutent de la valeur dans le conseil d'administration et dans leurs équipes grâce à leur expérience, leurs connaissances et leurs compétences en interaction sociale (Van Knippenberg et al. 2004 ; Wahid 2019 cités par Radu et Smaili, 2021). "Les femmes ont tendance à penser plus macro aux problèmes au lieu de penser à un problème particulier dans un microcosme", déclare Tiffany Jones, SVP¹²⁷ et CRO¹²⁸ chez iSIGHT Partners¹²⁹. "Les femmes ont tendance à être de bonnes analystes parce qu'elles sont capables de penser à partir de nombreux points de vue différents"¹³⁰ ainsi que de gérer simultanément plusieurs tâches, une compétence qui découle des constructions sociétales. En effet, une femme doit avoir plusieurs casquettes au quotidien (travail, famille, enfants). De plus, les femmes sont un avantage indéniable pour les équipes de cybersécurité, vu qu'elles sont les premières touchées par les menaces informatiques à travers le monde. Leur expérience permettrait de développer des solutions intéressantes aux différentes menaces. Une plus grande représentation favorise l'élaboration de stratégies de défense informatique vu qu'une perspective plus large est prise en compte (Weingarten et Garcia, 2015 ; Deloitte, 2021). L'étude réalisée par l'(ISC)² sur la main-d'œuvre en cybersécurité (2022) confirme cette affirmation par le fait qu'environ deux tiers de leurs participants ont déclaré qu'un environnement inclusif était essentiel à la réussite de leur équipe ((ISC)², 2022).

¹²⁷ Senior Vice President

¹²⁸ Chief Revenue Officer

¹²⁹ Weingarten, E., & Garcia, M. E. (2015). Decrypting the cybersecurity gender gap. New America. p.6 <https://www.newamerica.org/cybersecurity-initiative/policy-papers/decrypting-the-cybersecurity-gender-gap/>

¹³⁰ Ibid.

Figure 31 : Programme actuellement en place dans les entreprises afin de développer une main-d'oeuvre diversifiée (Forbes Insight, 2021, p.9)



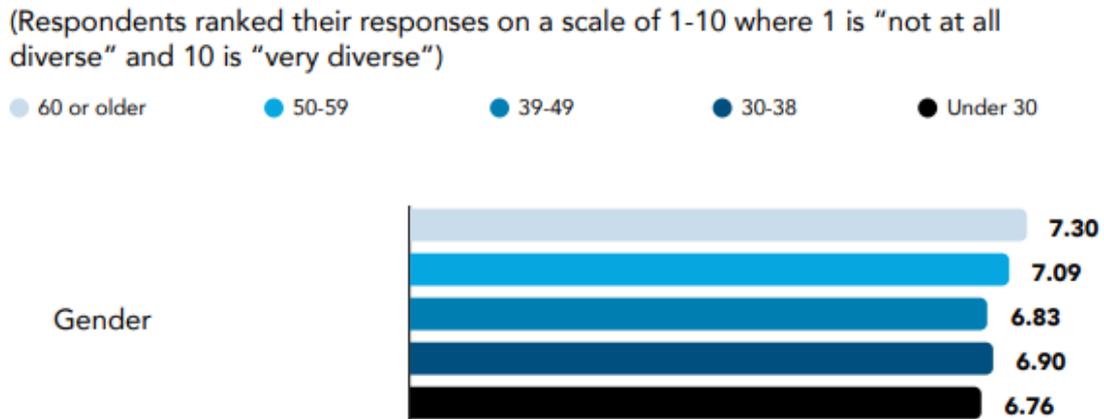
Les femmes membres de conseils d'administration peuvent influencer de diverses manières la cybersécurité des entreprises. Elles apportent des connaissances spécifiques et générales différentes de celles des hommes ce qui permet d'ajouter des perspectives différentes lors des discussions stratégiques. Elles supervisent et gèrent mieux les risques par leur attitude plus conservatrice. Les femmes font plus souvent preuve d'une sensibilité éthique accrue, tiennent compte de toutes les parties prenantes et démontrent un style de leadership particulier (Radu et Smaili, 2021). Dans l'ensemble, "les conseils comptant plus de femmes surpassent les conseils entièrement masculins en ce qui concerne l'attention portée à l'audit et à la surveillance et au contrôle des risques" (Brown et al. 2002, p. 5). C'est pour cette raison qu'il est important de développer différents programmes permettant de faire monter les femmes dans la gouvernance de l'entreprise (fig.31).

4.2. La diversité au service du recrutement et de la rétention

57% des entreprises¹³¹ souhaitent investir dans une politique de diversité, d'équité et d'inclusion afin d'attirer davantage de femmes et de minorités à entrer dans la profession de la cybersécurité et, donc, d'atténuer le manque de personnel en cybersécurité ((ISC)², 2022). Au cours des cinq dernières années, les entreprises de la cybersécurité ont évolué dans leur manière d'appréhender et de s'engager dans leur culture organisationnelle. Actuellement, beaucoup d'employés en cybersécurité, notamment la plus jeune génération, considèrent que la diversité, l'équité et l'inclusion (DEI) est un enjeu que leur entreprise doit prendre au sérieux ((ISC)², 2022). En effet, la plus jeune génération de travailleurs semble plus attentive aux initiatives DEI de leur entreprise (fig. 32).

¹³¹ (ISC)². (2022). CYBERSECURITY WORKFORCE STUDY. p.14. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.aspx>

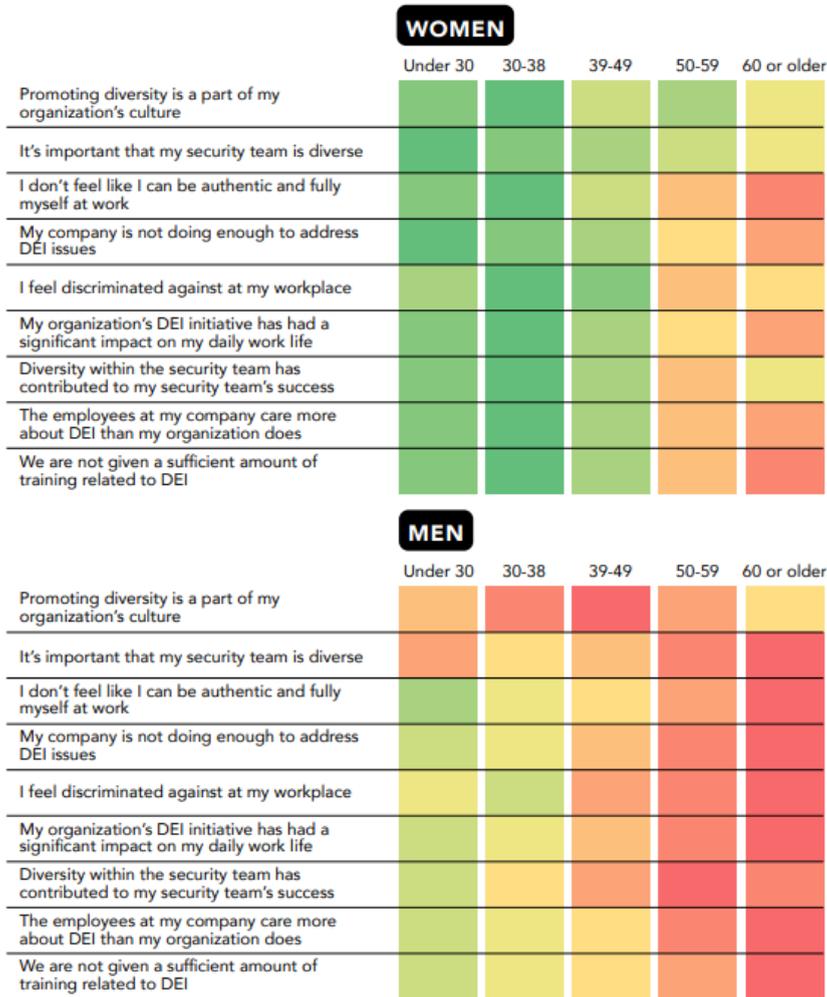
Figure 32 : Evaluation des entreprises par leur employés en termes de diversité de genre ((ISC)², 2022, p.43)



L'organisme (ISC)² a recueilli l'avis de tout leur panel de participants sur différentes affirmations relatives à leur expérience au sein de leur entreprise ainsi que sur le développement d'initiatives en matière de diversité, d'équité et d'inclusion (DEI) dans ces entreprises. Les données révèlent des tendances intéressantes liées aux perceptions et aux priorités des femmes et des hommes dans le contexte professionnel. Les femmes ont tendance à choisir des entreprises où la promotion de la diversité fait partie intégrante de la culture d'entreprise. Cela se retrouve aussi sur l'importance qu'elles accordent à la diversité de leur équipe. Cependant, les jeunes générations, aussi bien chez les femmes que chez les hommes, expriment des préoccupations quant à l'attention insuffisante portée aux questions DEI au sein de leurs entreprises respectives (formations, considération du management). Les femmes font plus attention et sont plus sensibles à la diversité de leur équipe, considérant son impact potentiel sur la réussite de leurs tâches. Néanmoins, les hommes tendent à minimiser l'importance de la diversité au sein de l'équipe. Ils estiment aussi que leurs entreprises s'adressent suffisamment aux divers problèmes DEI, à l'exception des deux groupes d'âge les plus jeunes. Pour les femmes et les hommes âgés de moins de 38 ans, les initiatives DEI mises en place au sein des entreprises ont une répercussion directe sur leur vie professionnelle. Toute la figure 33 démontre un changement direct de mentalité au sein des plus jeunes employés (plus prononcé chez les femmes que chez les hommes). Ces derniers sont plus sensibles aux questions DEI.

Figure 33 : Ressenti des employés en cybersécurité par rapport à la DEI au sein de leur entreprise en fonction du genre et de la tranche d'âge ((ISC)², 2022)

Green — strongest agreement Yellow/orange — medium agreement Red — strongest disagreement



Base: 11,525 global cybersecurity professionals on cybersecurity teams

Chapitre 2 : partie empirique

1. Méthodologie

L'étude a été menée dans le cadre d'un mémoire sur la diversité de genre au sein des études et des entreprises du domaine de la cybersécurité. J'ai choisi d'utiliser une approche qualitative pour comprendre les défis et les opportunités liés à l'intégration des femmes dans le domaine de la cybersécurité ainsi que pour identifier des stratégies visant favoriser une plus grande participation féminine (Aubin-Auger et al, 2008). Cette méthode m'a permis d'explorer les comportements et les expériences personnelles des différents participants. J'ai décidé de réaliser des entretiens directifs. Le but de mon étude était de vérifier les informations apportées par la littérature concernant le problème de la représentation des femmes au sein de la cybersécurité dans son ensemble (Ghiglione et Matalon, 1985). Je n'ai aucunement donner mon avis entre chaque question. Ces entretiens

ressemblaient à un questionnaire avec des questions ouvertes, mais orales. Bien que les entretiens individuels soient plus chronophages, les participants ont pu aborder sans crainte d'être jugés ou surveillés toutes leurs expériences relatives au genre vécues dans le monde professionnel ou scolaire (Aubin-Auger et al, 2008).

En tout, j'ai réalisé quinze entretiens d'une moyenne de trente-cinq minutes. Cinq entretiens avec des femmes travaillant dans la cybersécurité. Ces femmes sont généralement âgées d'une trentaine d'années (30 à 39 ans). Une des femmes a 55 ans. J'ai aussi interrogé cinq hommes travaillant en cybersécurité. Deux ont 47 ans et trois sont âgés entre 25 et 30 ans. Les cinq derniers entretiens étaient avec des professionnels en ressources humaines, un homme pour quatre femmes. Ils sont âgés de 28 à 34 ans. Ces personnes ont toutes été trouvées via les réseaux sociaux et le réseautage. J'ai créé plusieurs postes LinkedIn qui ont été relayés par Women4Cyber Belgium. Je suis aussi rentrée dans le Discord de la communauté BeCyber. Avant de commencer chaque entretien, les participants ont été mis au courant de son caractère anonyme et académique. Les hommes ont été appelés H1 à H5, les femmes F1 à F5 et les professionnels RH, RH1 à RH5. Durant les entretiens, j'ai utilisé deux grilles d'interview, une pour les travailleurs en cybersécurité et une pour les professionnels RH. La grille des travailleurs s'articule autour des thématiques suivantes : leurs études, leur vie professionnelle et la représentation des femmes au sein de leur entreprises. Pour la grille des professionnels RH, je cherchais à découvrir la proportion de femmes au sein de leur entreprise et leur profil ainsi que leurs initiatives concernant la promotion d'une diversité et leur évaluation. Dans les deux grilles, j'ai inclus des questions relatives aux avantages de la diversité de genre, aux clients de l'entreprise. Chaque répondant a pu expliquer les défis que les femmes pouvaient rencontrer ainsi qu'exprimer des conseils pour les relever.

L'analyse des données repose sur la méthodologie qualitative du codage ouvert. Cette approche consiste à fragmenter les récits en éléments distincts d'analyse (citations), lesquels se rapportent aux thèmes principaux abordés par les participants de l'étude (Miles et Huberman, 1994). Premièrement, j'ai relu plusieurs fois les transcriptions. Ensuite, je les ai rapportées dans un tableau afin de comparer les réponses pour chaque catégorie de questions. J'ai également utilisé le logiciel ATLAS.ti, afin d'identifier les grands thèmes abordés lors des entretiens. Dans la partie "Résultats", je vais illustrer chaque thème par des citations des interviews.

2. Présentation des résultats¹³²

2.1. Les études

Que ce soit les hommes ou les femmes, tous affirment que les femmes qui travaillent actuellement en cybersécurité ne réalisent généralement pas leurs études dans le domaine des STIM, ou alors elles sont clairement en minorité.

F1: *"Je viens d'une Business School [...]. En général, les hommes viennent des études concernant l'informatique et l'ingénierie. Il y a aussi des femmes bien sûr mais moins. Les femmes viennent*

¹³² Cf. Annexes F, G et H pour les transcriptions des entretiens

souvent d'autres domaines et font une reconversion professionnelle parce qu'elles voient qu'il y a beaucoup d'opportunités en cyber."

H5 : *"Quand je faisais mes études, c'était il y a plus de dix ans de ça. Pour six cents personnes, il y avait cinq filles. Ça donne vraiment des ratios très prononcés."*

RH4 : *"[...] ces 20 % [de femmes] sont principalement axées dans des domaines tels que la finance, les ressources humaines et tout ce qui concerne le commercial en fait."*

Cette sous-représentation n'est pas dûe un problème de motivation. Quand les femmes décident de faire des études en informatique, elles sont généralement plus motivées que les hommes. Il existe d'autres freins à l'entrée des femmes dans ce type d'études comme le manque de modèles féminins, le sexisme des autres étudiants, le manque d'information sur les métiers de l'informatique et l'image de la cybersécurité. Inversement, les hommes ne ressentent aucune barrière à l'entrée pour ce genre d'études.

H2 : *"Elle était quand même assez motivée et donc on est allé dans cette direction-là [de la cybersécurité]. [...] Les femmes qui vont entrer dans ce métier seront généralement motivées de manière plus pointue, plus précise. [...] Alors qu'un homme qui va aimer l'informatique de manière générale, il va rentrer en cybersécurité parce que ça s'est fait, un peu par hasard. Dans le cadre d'une femme, j'ai plus la sensation que c'est quelque chose qui est vraiment volontaire."*

F2 : *"Pour ce qui est d'entreprendre des études, je pense qu'il y a toujours un frein parce que ça reste quand même un secteur où il y a moins de femmes. C'est plus difficile de se sentir bien, de ne pas pouvoir se rattacher à un modèle."*

F3 : *"Dans mes études, j'ai pu avoir des relations conflictuelles avec d'autres étudiants parce qu'ils me manquaient de respect. Ils n'acceptent pas que je sois meilleure qu'eux donc ils peuvent me rabaisser".*

F4 : *"Je ne pense pas que ça soit un problème de motivation. C'est plutôt un problème d'image de la cybersécurité. Les femmes, elles ne pensent pas que ce genre de métiers/études sont pour elles ou alors, on leur fait savoir."*

H2 : *"Une des raisons principales est le manque d'intérêt des plus jeunes [filles]. On n'apprend pas ou on n'explique pas aux jeunes filles l'informatique."*

2.2. La présence des femmes dans le secteur de la cybersécurité belge

Tous les participants sont d'accord sur le fait que les femmes sont sous-représentées dans le domaine de la cybersécurité en Belgique. Les entreprises "bonnes élèves" sont celles qui ont un ratio d'environ 20 femmes pour 80 hommes, soit 1 femme pour 4 hommes, comme a pu le dire RH1.

F1 : *"[...]il y a 17% de femmes dans l'IT en général. Le pourcentage n'a que faiblement évolué au cours des dernières années."*

H5 : *"[...]sinon dans le temps, depuis dix ans clairement, la gente féminine est vraiment sous-représentée dans tous les services que j'ai pu rencontrer au sein de l'informatique. C'est un gros problème, par exemple, là où je travaille, on est 30 internes dans mon service. Il y a deux femmes dans le lot. Les statistiques sont vraiment très basses [...]"*

H2 : *"C'est un peu compliqué parce que je n'ai pas rencontré beaucoup de femmes dans le domaine de la cybersécurité [...]"*

RH1 : *"Sur 250 travailleurs, il y a environ une quarantaine de femmes. Évidemment, ce n'est pas un nombre élevé, mais cela reste un bon ratio."*

Cependant, il faut nuancer ce propos. Les femmes sont bien plus sous-représentées dans les métiers dits "techniques" de la cybersécurité que dans les métiers "non techniques".

F4 : *"Je dirais que dans le domaine technique, il y en a quand même pas mal qui quittent la sécurité technique pour se tourner vers la sécurité basée sur la documentation, ce que j'ai personnellement fait."*

H3 : *"En somme, pas de femmes venant des études d'ingénierie ou de sciences informatiques ou alors il doit y en avoir une ou deux. Mais du côté GDPR [Règlement général sur la protection des données] et légal, il y a plus de femmes que d'hommes. Les femmes sont beaucoup plus dans des RH attachées au département cyber, ou alors elles sont dans le département légal, rattachées à la sécurité, mais très rarement dans les équipes techniques."*

H1 : *"Dans le pôle technique, nous sommes une quarantaine de personnes. Il y a seulement trois femmes, dont une dans mon équipe qui travaille sur les réseaux et la cybersécurité. Les femmes sont quand même sous-représentées. [...] Évidemment, on retrouve une proportion un peu plus normale de femmes dans les catégories sales, légal, gestion des risques, etc."*

Malgré ce faible ratio, les participants ont trouvé qu'il y avait une évolution positive du nombre de femmes dans les métiers de la cybersécurité. L'entreprise de RH2 a même réussi à avoir la parité dans son équipe de cybersécurité. RH2 a émis l'hypothèse que c'est grâce aux services fournis par son organisation, une ONG.

H5 : *"Oui. On sent qu'il y a vraiment une volonté des entreprises, des écoles et de certains gouvernements de promouvoir les métiers de l'IT chez les femmes."*

RH 2 : *"En faisant le calcul rapidement, on est 15 femmes sur 35 personnes. Par contre, dans le management, c'est 50-50. [...] Après, c'est une ONG, donc c'est différent. L'aspect social aide sûrement à attirer un peu plus de femmes."*

Les femmes participant à l'étude ont trouvé qu'il n'y avait aucune barrière concernant leur promotion. Elles ont toutes déjà été promues ou augmentées au moins une fois, à l'exception de F3 qui est toujours étudiante. Néanmoins, F4 avoue qu'il n'y a aucune femme dans le top management de son entreprise et RH3 trouve que le comportement des managers change en fonction du genre de son subordonné, et cela affecte les possibilités de promotions.

F2 : *"Aucun problème de promotion dans mon entreprise."*

F1 : *"Je n'ai pas ressenti de potentielles barrières quand on m'a promue cheffe d'équipe."*

F3 : *"De plus en plus de femmes ont aussi des hauts postes."*

F4 : *"Je ne vais pas me plaindre, car ça va faire trois ans que je suis là et j'ai déjà eu trois augmentations et une promotion.[...] Le seul problème, c'est le fait qu'il n'y a quasiment que des hommes dans le top management. Il y a quatre personnes au top management, ce sont tous des hommes. Ça a toujours été des hommes. Ensuite, dans le middle top, il y a quand même énormément de femmes. [...] ils ont mis une femme qui était techniquement encore un peu junior en tant que directrice. Ils l'ont soutenue, etc."*

RH 3 : *"On voit aussi dans le comportement des managers et dans la façon dont un homme reçoit une promotion ou est évalué. Ce n'est pas la même chose que chez la femme. Lors d'une promotion, l'entreprise souhaite que le/la promu(e) soit rentable pour elle. Le management et les RH auront donc tendance à choisir un homme parce que, dans leurs pensées, les hommes seront bien plus impliqués dans leur nouveau rôle. Ils pensent que les hommes ont moins de tâches à la maison que les femmes."*

Dans le secteur de la cybersécurité, les compétences sont encore le premier critère de sélection. Il passe avant l'envie de diversité et de parité des participants. Certains collègues masculins et responsables RH ne voient donc pas l'intérêt d'une complète parité dans les équipes.

H2 : *"Non, pas particulièrement, mais, de la même façon que ça me serait égal qu'il y ait 90% de femmes pour 10% d'hommes. Je ne vois pas ce que ça pourrait apporter de plus. La priorité, c'est la connaissance et la compétence. Je ne suis pas très sexiste par rapport à tout ça. Si la personne est compétente, je peux travailler à 100% avec."*

H5 : *"Je marche beaucoup aux compétences. Tant que les personnes sont compétentes, je pense que femme ou homme, on fera du bon travail.[...]Quand je recrute des gens, je m'en fous du sexe. Moi, ce qui m'intéresse c'est de savoir: est-ce que la personne est compétente?"*

RH4 : *"[...]on recherche avant tout les personnes les plus compétentes. Dans la sélection, il n'y a pas de favoritisme sur les hommes ou les femmes."*

RH1 : *"Que ce soit une femme, un homme ou quelqu'un de non binaire, ce n'est pas du tout un critère d'intérêt ou de sélection."*

Les femmes souffrent encore de sexisme dans leur sphère professionnelle. Par exemple, elles doivent sans cesse prouver leur légitimité, qu'elles ne sont pas là pour apporter le café ou prendre des notes. Elles peuvent aussi subir un harcèlement sexuel régulier. Tout cela représente des freins au développement des femmes dans les métiers de la cybersécurité.

RH5 : *“Plus généralement, c'est vrai que les femmes peuvent souffrir de ce manque de légitimité. Les femmes doivent donc montrer qu'elles sont là pour une raison, qu'elles sont compétentes.”*

H5 : *“Cependant, je comprends le point de vue des femmes car, dans des conférences mixtes, elles se sentent comme des bouts de viande.”*

F1 : *“Les quotas n'aident pas dans ce sens [montrer que les femmes sont légitimes]. Je ne veux pas qu'on m'engage parce que je suis une femme. Je comprends que certains hommes puissent douter de nos compétences parfois.”*

F4 : *“[mon manager] était vraiment odieux. Si je posais une question, il me rabrouait. En revanche, l'alternant, qui était un homme, était bien traité. On prenait le temps de lui expliquer les choses. C'était évident que j'étais traitée différemment, comme si j'étais incompetente. Je me souviens même qu'il m'avait dit de chercher sur Google, comme si je ne savais pas comment le faire. [...] Par exemple, lors de réunions, je pouvais donner une bonne idée. Il n'hésitait pas à dire devant toute l'assemblée que je servais enfin à quelque chose. C'était très dégradant. [...] On se heurte donc encore à des vieux réflexes comme "Ah, toi, tu vas prendre des notes pendant la réunion !". [...] Puis les blagues salaces sont encore tellement la norme.”*

F4 : *“Puis, tu as aussi tous les mecs qui veulent avoir un rapport avec toi. Ils ne vont même pas t'écouter.”*

2.3. Les compétences et les traits de caractères requis pour travailler en cybersécurité

On arrive donc à la conclusion qu'il y a bien plus d'hommes techniques que de femmes. Cela est sûrement la raison pour laquelle les femmes sont considérées plus compétentes en technique que les hommes. Vu qu'elles sont peu, elles doivent toujours en faire plus pour prouver qu'elles ont leur place, selon F4.

F4 : *“En technique, non. Si ce n'est qu'en général, elles sont plus compétentes. En tant que femme, tu es obligée de prouver deux fois plus que tu es compétente.”*

F5 : *“J'ai déjà pu constater que les femmes sont en général moins techniques que les hommes. Après, c'est une observation générale. Il y a toujours des exceptions.”*

F1 : *“D'un point de vue technique, je pense que ça dépend juste des études qu'on a faites, des trucs qu'on a creusés. Là, je ne pense pas que ça ait un rapport avec le genre.”*

H3 : *“Comme pour les mecs. Cela dépend du métier spécifique de la cybersécurité.”*

Les *softs skills* semblent différer en fonction du genre, voire même être associées à des stéréotypes. Les femmes sont considérées comme plus sensibles, plus à l’écoute, plus empathiques. Elles sont aussi associées à la communication, au sens du détail, à l’aversion au risque et à la créativité. Contrairement aux hommes, ces derniers sont qualifiés par leur leadership, leur côté direct et moins organisé. Cependant, il reste des *soft skills* qui correspondent au besoin de la profession et que les deux genres doivent posséder pour exceller dans leur tâche.

F1 : *“Je dirais que les femmes apportent une sensibilité, un côté avec plus de rondeurs dans la relation avec les gens, plus de communication. [...] Mais, socialement, je dirais que les femmes sont plus dans le côté empathique. En effet, c'est plutôt dans les soft skills où effectivement j'ai l'impression qu'il y a des choses qui sont plus naturelles en fonction du genre.”*

F4 : *“Moi, je voudrais bien être managée par une femme. [...] Il y a ce côté plus zen, plus calme. Tu peux aborder tes émotions en disant "ce n'est pas un problème, en fait” ”.*

H1 : *“Avoir envie d'apprendre tous les jours, car je crois que c'est peut-être l'un des domaines qui évolue le plus rapidement. Se tenir constamment à jour.”*

H5 : *“Ensuite, il y a toujours une personne alpha dans les équipes qui montre son leadership. Ce ne sont jamais des femmes.”*

RH1 : *“Nous, en tant que femmes, prenons beaucoup moins de risques. Cela fait partie de notre manière d'être. C'est ce que nous avons appris en grandissant, et c'est quelque chose qui est très ancré dans différentes générations.”*

RH3 : *“Elles possèdent un grand sens du détail ainsi qu'une certaine créativité.”*

F4 : *“Comme un homme, enfin comme un être humain normal. [...] Pour la sécurité, c'est très vaste. Si tu fais de la technique, il faut que tu sois un fouille-merde, que tu sois débrouillard. Si tu fais de la sécurité plus papier, il faut que tu sois pragmatique, que tu aies une bonne vision d'ensemble, que tu sois patient, mais comme n'importe qui.”*

H5 : *“Mettre à jour leur connaissance, continuer à apprendre, avoir cette volonté de toujours step up. Et ça, peu importe le genre”*

En ce qui concerne les traits de caractères spécifiques, ils suivent la même tendance que les *hard skills* et *soft skills*. Ils sont relativement les mêmes parce qu'ils sont imposés par le secteur de la cybersécurité. Néanmoins, les femmes doivent avoir presque obligatoirement un caractère bien trempé et du répondant afin de ne pas se laisser faire lorsqu'une injustice, une remarque sexiste ou un comportement inapproprié arrive.

H2 : *“Par contre, il doit y avoir des traits de caractère qui sont très importants. Il faut être opiniâtre. Il faut vouloir continuer à chercher jusqu'à ce qu'on finisse par trouver. [...]. Mais, ce n'est pas propre au fait d'être une femme ou un homme. C'est le caractère qui est exigé par le métier.”*

H5 : *“Aussi, les femmes doivent oser imposer leurs frontières. Elles ne doivent pas se faire marcher dessus. Être passionnées et persévérantes”.*

F3 : *“Quand tu es dans un monde d'hommes, tu es obligé d'avoir du caractère et du répondant pour éviter de te faire marcher dessus.”*

F5 : *“Tout type de traits de caractères car il y a beaucoup de postes différents. Si on veut commencer à monter dans la cybersécurité, il faut être flexible parce qu'on peut nous appeler tout le temps (weekend, nuit, vacances...). Il ne faut pas compter ses heures.”*

H3 : *“Je ne suis pas le mec le plus ordonné, je ne suis pas le mec qui prend le plus de notes, etc. C'est plus carré avec les femmes.”*

Finalement, tant les compétences que la personnalité sont des critères importants pour évoluer correctement dans le domaine de la cybersécurité. Chaque individu a ses propres compétences à apporter à son équipe, en fonction de son genre ou non.

H4 : *“A partir du moment où une personne peut prouver qu'elle possède les compétences nécessaires à la réalisation d'un travail, autant d'un point de vue humain que technique, cela s'arrête là en fait. Dans n'importe quel poste dans l'IT, ce sont les deux éléments les plus déterminants : les compétences et la personnalité.”*

F2 : *“Je pense que chaque individu apporte quelque chose de différent. Ce n'est pas forcément généré.”*

2.4. Les relations au travail

Les relations au travail peuvent prendre différentes formes. Premièrement, il y a les relations avec les collègues. Les femmes et les hommes n'interagissent pas de la même manière entre eux. Les hommes peuvent parfois avoir des comportements misogynes et sexistes envers les femmes. Les femmes peuvent être mises en compétition les unes avec les autres. Cependant, lorsque chaque personne de l'équipe montre du respect à son/sa collègue et reste professionnelle, tout se passe pour le mieux entre les hommes et les femmes. En général, les hommes changent légèrement leur manière de parler quand ils s'adressent à une femme. Ils vont être plus prudents ainsi que limiter les blagues qu'ils pourraient se permettre de faire à d'autres collègues masculins.

H4 : *“J'ai déjà recadrer un collègue qui ne voulait pas écouter la proposition d'une autre collègue à cause de son genre.”*

F5 : *“J’ai toujours eu de bonnes relations avec mes collègues masculins donc je n’ai subi aucun stéréotype durant nos réunions. J’étais toujours écoutée.”*

F3 : *“Dans mes études, j’ai pu avoir des relations conflictuelles avec d’autres étudiants parce qu’ils me manquaient de respect. Ils n’acceptent pas que je sois meilleure qu’eux donc ils rabaissent.”*

F4 : *“[...]notamment quand j’ai commencé ma carrière, il y avait ce côté où on essayait de monter les femmes les unes contre les autres. On te mettait en compétition avec les autres femmes dans le milieu. [...]Quand tu es une femme dans un bureau majoritairement masculin, tu es confrontée à différents rôles que la société t’incite à prendre. Du coup, quand tu ne t’en rends pas compte, tu les acceptes et tu endosses le rôle. Puis, tu as aussi tous les mecs qui veulent avoir un rapport avec toi.”*

F5 : *“Même pied d’égalité. Mais le fait d’être une femme, mes collègues masculins peuvent me parler plus prudemment. Quand on est une femme, les hommes nous parlent différemment. Je préfère même travailler avec un homme plutôt qu’une femme.”*

H1 : *“Nous avons peut-être une tendance à la chouchouter parce que c’est la seule femme dans mon équipe.”*

H2 : *“Il y a toujours des blagues qu’on peut faire ou qu’on ne peut pas faire. Il y a des limites à connaître. Je dirais donc qu’il y a quand même une forme de différence mais qui est de l’ordre de l’interaction sociale. En informatique, les femmes sont souvent sujettes à la plaisanterie. Toutefois, j’ai toujours essayé de limiter ça et de faire en sorte que ça reste dans des limites acceptables.”*

La fait d’être une femme apporte aussi d’autres besoins. Les femmes ne peuvent pas rester au bureau aussi longtemps que leurs collègues masculins. Les femmes endossent encore la responsabilité de tout ce qui se rapporte à la famille. Elles ont donc du mal à faire autant de réseautage que les hommes, celui en dehors des heures de travail.

F5 : *“Le trois-quart des femmes avec lesquelles je travaille sont mamans et vont vouloir partir tôt. Elles doivent s’occuper de toute leur famille.”*

F4 : *“En général, une femme sait qu’elle aura déjà toute cette charge mentale et donc, aura moins tendance à vouloir faire des heures supplémentaires pour essayer d’avoir un équilibre entre vie privée et vie professionnelle.”*

Deuxièmement, il y a les relations avec les clients. Malgré leurs compétences en gestion des relations, les femmes peuvent encore subir des comportements discriminatoires de la part des clients qu’elles doivent servir. Certaines entreprises tiennent beaucoup plus à leurs employées qu’à la relation avec le client donc, quand un comportement inapproprié se déroule, elles préfèrent couper net la relation commerciale. C’est le cas pour les entreprises de H3 et RH2. Par contre, les clientes sont très heureuses de travailler avec des femmes expertes en cybersécurité.

RH2 : *“En fait, dès que j’ai des clientes, il y a un côté plus facilitateur. Elles sont contentes de travailler avec une femme.[...] Je n’ai pas non plus envie de travailler avec ces gens [clients sexistes].”*

F2 : *“Du point de vue des clients, il y a encore une énorme discrimination qui se fait sur le fait d’être vu comme quelqu’un de compétent ou pas selon son genre. [...] J’ai toujours pensé que non parce que la cyber est un secteur où il y a tellement un manque de personnel et un manque de connaissances.”*

H2 : *“Ma collègue la plus proche a très souvent été la cible de problèmes. Alors, à 2/3 exceptions, ce n’était jamais de façon affichée. C’était du sexisme parce que les gens ne voulaient pas lui parler. Le nombre de fois où elle répondait au support technique, les gens lui demandaient “est-ce que je peux avoir un technicien s’il vous plaît?”. Elle avait beau dire : “mais je suis technicienne”. Les clients répondaient “non mais passez-moi Monsieur X”, par exemple. [...] Finalement, je lui ai dit : “Pour ce client-là, signe en mon nom” parce qu’on voulait que le message passe. On visait l’efficacité avant tout et, ça, c’était bien triste. Du point de vue des clients, il y a encore une énorme discrimination qui se fait sur le fait d’être vu comme quelqu’un de compétent ou pas selon son genre.”*

H3 : *“Je sais juste que si ça se passe mal à ce niveau-là, ma boîte de consultants sera derrière car elle est très à cheval là-dessus (différence hommes-femmes, violence verbale). Elle préfère garder un employé plutôt que de travailler avec quelqu’un qui a ce genre de comportement. Elle préfère ne plus traiter avec le client et perdre de l’argent.”*

2.5. Les initiatives pour promouvoir les femmes dans la cybersécurité

F1 : *“[...] il va falloir mener des actions plus fortes pour créer des vocations et un peu casser des images.”*

Le mentorat est l’aide qu’apporte un collègue ou une personne extérieure à une personne peu expérimentée, comme les nouvelles employées en cybersécurité. Le mentor donne à sa mentorée des conseils, des contacts, des voies de carrière ainsi que des certifications utiles. Le mentor joue le rôle de repère et de source d’informations pour la nouvelle génération de femmes en cybersécurité. Grâce à ce programme, les femmes sont capables d’évoluer autant personnellement que professionnellement. C’est donc un moyen de développement et d’apprentissage. Les répondants à l’étude trouvent unanimement que ce genre de programme est intéressant autant pour les femmes que pour les entreprises. Cependant, H3 a soulevé le fait que ce genre de programme ne devrait pas être seulement destiné aux femmes. Il faudrait développer des programmes de mentorat mixtes.

F1 : *“C’est génial. [...] Les mentors peuvent être aussi bien des collègues que des personnes extérieures. Je pense que les femmes sont plus sensibles à ce fonctionnement [le mentorat], parce que socialement, les hommes sont meilleurs en networking. Les femmes le font un peu moins. Mais, savoir s’entourer, c’est hyper important. Si les femmes comprennent qu’elles peuvent se faire entourer et compter sur des personnes de confiance, c’est tout bon. Le mentorat répond à ça.”*

F2 : *“Je pense que c’est toujours bien. Ne serait-ce que pour avoir une sorte de modèle et puis, un peu une idée des carrières qui ont été faites, des bonnes pratiques, des bons conseils, un peu pour avoir une grande sœur comme ça. J’en ai fait personnellement. Puis, juste pour avoir des contacts dans*

l'industrie. L'année passée, j'avais une mentee. Elle cherchait un job. Je l'ai aidée en la mettant en contact avec des gens que je connais. C'est tous des réseaux qui sont toujours utiles à tous les niveaux."

F5 : *"Avoir un mentoring interne à notre société est un gros avantage."*

H5 : *"[...]cela [le mentorat] permettrait aux femmes de se rendre compte de la réalité et de pratiquer des cas concrets."*

H3 : *"Mais à côté de ça, c'est dommage parce que je pense qu'une partie des personnes qui voudraient participer seront des hommes. Si c'est donner des astuces, c'est la même chose, que ce soit pour une femme ou un homme."*

Afin de promouvoir la représentation des femmes au sein de leurs effectifs, les entreprises réalisent des partenariats avec différents organismes comme les établissements scolaires. Elles ont envie de développer la population de femmes en cybersécurité, à la base. En changeant l'image perçue de la cybersécurité ainsi qu'en informant, simplement, plus sur la multitude de métiers disponibles en cybersécurité, plus de femmes pourraient envisager de suivre des études liées à ce domaine. Les organisations développent aussi des partenariats avec des organisations comme *Women4Cyber* afin d'avoir accès à leur communauté et de pouvoir proposer des opportunités de *reskilling* et de stages pour les femmes au sein de leurs bureaux.

H1 : *"On devrait mieux informer les gens. Mais encore une fois, ce serait plutôt au niveau du secondaire qu'il faudrait agir. À l'école secondaire, on devrait mieux informer les jeunes sur les métiers en pénurie, peut-être même leur expliquer ce que c'est. Cela pourrait déjà aider à attirer plus de monde."*

H3 : *"C'est qu'on est sur des clichés du Geek Boutonneux derrière son ordinateur avec ses lunettes. [...] Plus les femmes vont venir faire les études, moins il y aura le cliché que ce sont des études d'homme, et donc plus de femmes viendront. Je pense que c'est là-dessus que ça doit jouer en termes d'environnement."*

RH1 : *"Ce partenariat avec Women4Cyber. [...] Je pense que l'année prochaine, on va avoir un plus gros partenariat avec Women4Cyber afin de participer au job fairs ou peut-être prendre des femmes en stage (reskilling, reconversion, etc.)."*

F2 : *"Je suis dans Women4Cyber. Je me concentre sur ce qui est académique, partnership et puis workforce. Je me concentre particulièrement sur les partenariats avec des organismes de formation. C'est vraiment l'idée d'inciter les femmes à faire des études en cyber, faire de la recherche, donc postuler. On cherche aussi à ce que les universités intègrent la cyber dans des cursus non techniques comme avoir des gens en Sciences Po qui prennent un cours en cybersécurité. Cela permettrait de peut-être les intéresser à intégrer le secteur plus tard ou d'augmenter la compréhension de la cyber."*

RH3 : *"Nous avons également démarré une nouvelle formation avec une société du secteur financier et un établissement d'études supérieures."*

Les établissements scolaires ainsi que les entreprises utilisent différents canaux afin de sensibiliser les femmes à la cybersécurité. Afin d'informer, de motiver et de créer des vocations, ils utilisent les *jobs fairs*, les réseaux sociaux comme *LinkedIn* afin de partager et de mettre en évidence leur culture inclusive et la présence de femmes. Montrer qu'il y a des femmes dans les métiers et les études du secteur de la cybersécurité est très important vu que les potentielles employées et étudiantes pourront s'identifier à elles.

H2 : *“Pour moi, c'est une question d'éducation aux métiers. Il y a des journées qui sont organisées, notamment par l'Helmo, auprès des étudiants. Je pense que le métier d'informaticien - même de cybersécurité - est assez mal connu ou assez mal représenté. On ne sait pas forcément ce que c'est. Il faudrait intéresser plus les jeunes filles à l'informatique déjà en primaire et éviter les cloisonnements.”*

H3 : *“ Ils promeuvent un peu la femme dans le travail, vont à des job fairs. Il font aussi des posts LinkedIn. Ils sont fiers d'avoir des femmes et le mettent en avant. Ce n'est pas juste pour le côté marketing. Cela fait vraiment partie de la boîte.”*

Les responsables en ressources humaines peuvent aussi influencer sur la présence de femmes au sein de leur entreprise. Ces derniers peuvent notamment travailler sur la description de poste afin de la rendre plus inclusive. En effet, cela laissera aux femmes l'idée que le poste n'est pas seulement adressé aux hommes et qu'elles ont le profil pour candidater. Ils peuvent aussi sensibiliser tous les autres acteurs du recrutement sur le fait d'engager plus de femmes. Malgré cela, le marché de l'emploi en cybersécurité reste tendu. Les recruteurs ne peuvent pas tous se permettre comme RH2 de faire attention à la parité de leurs candidatures. RH5, par exemple, ne reçoit pratiquement que des candidatures d'hommes.

F2 : *“Dans tous les secteurs, les femmes ont moins tendance à se mettre en avant et à postuler pour des postes tant qu'elles ne voient pas qu'elles répondent parfaitement aux job description. Il y a donc plus de boulot à faire sur comment le job description est écrit pour ne pas toutes les faire fuir de prime abord.”*

RH2 : *“Je fais attention à recevoir autant de candidats femmes qu'hommes. Je représente l'entreprise dans ce domaine. J'ai donc sensibilisé les cabinets de recrutement qui travaillaient pour l'entreprise, mais aussi des acteurs du recrutement. [...] Du coup, j'ai sensibilisé les gens à cette sous-représentation. En premier lieu, nous avons revu nos descriptions de jobs pour que, du coup, ça puisse parler aux femmes et que ça puisse permettre à chacun de se retrouver. Cela a développé notre pool de candidates.”*

RH4: *“Quand je vais mettre en ligne une offre, j'essaie toujours de faire en sorte qu'elle soit la plus inclusive possible.”*

RH5 : *“Les critères, c'était d'avoir des gens expérimentés dans un premier temps. Ensuite, on demandait qu'ils aient déjà une connaissance en cybersécurité. [...] On n'a pas spécialement eu cette approche d'absolument vouloir une parité homme/femme. Cependant, on n'a pas fermé la porte à*

quelqu'un parce que c'est un homme ou une femme. Mais, c'est vrai qu'au niveau de la parité, il n'y a pas de choses qui ont été mises en place. On n'a pas spécialement recruté une femme parce que c'était une femme."

L'aspect formation n'est pas seulement réservé aux femmes. Les entreprises de la cybersécurité forment tout leur personnel. Cela corrobore le fait que le monde de la cybersécurité est en constante évolution et qu'il y a besoin d'une main-d'œuvre féminine (ou non) compétente et à jour sur les dernières découvertes.

RH1 : *"On ne fait pas de distinction entre les hommes et les femmes. On a un training budget donc tout le monde a un training budget et des jours disponibles pour se former. On a 10.000€ tous les 2 ans et 10 jours que l'on peut poser. L'entreprise nous encourage à utiliser ce training budget. Cela n'a rien à voir avec le fait d'être une femme ou un homme, tout le monde peut le faire. On ne se base pas du tout sur le genre. On a des normes précises au sujet de la formation dont celle qui précise qu'il n'y aucune différence en fonction du genre."*

La création et le soutien de modèles féminins forts sont des éléments importants dans l'attraction et la rétention de femmes dans le domaine de la cybersécurité.

RH 2 : *"On a aussi fait en sorte d'être plus visibles pour les femmes qui étaient déjà dans l'entreprise afin de montrer qu'il y a des femmes dans ce monde masculin. Si on ne montre que des hommes, les femmes n'ont pas la possibilité de se projeter dans leur fonction (en tant que femme) alors que si les employées (ou candidates) rencontrent d'autres femmes, elles ont tout de suite plus envie de rester/d'entrer dans l'entreprise."*

H3 : *"J'ai l'impression que c'est une boucle de rétroaction : plus les femmes vont venir faire les études, moins il y aura le cliché que ce sont des études d'homme, et donc plus de femmes viendront. Je pense que c'est là-dessus que ça doit jouer en termes d'environnement."*

F4 : *"Quand tu es la première, c'est tellement difficile alors que quand tu as des exemples, c'est plus simple. J'ai toujours eu des femmes fortes dans des postes de management au-dessus de moi et ça m'a énormément aidée. Ça m'a montré de ne pas faire de compromis justement, parce que tu vois à quel point elles ont travaillé dur pour en arriver là, etc."*

Beaucoup de participants à l'étude ont déjà pris part à des initiatives encourageant le développement des femmes en cybersécurité. F1, F2, F3 et F5 font partie de *Women4Cyber*. F4 fait partie de la communauté *Blackhoodie*. Quant aux hommes, trois sur les cinq ont déjà participé à des initiatives que ce soit à titre personnel ou dans leur entreprise.

H3: *"Bien sûr, je l'ai déjà fait et je le referai encore une fois. Si tu augmentes la diversité, tu peux augmenter le nombre de personnes intéressées par la cyber. J'aimerais bien qu'il y ait plus de monde qui soit intéressé par la cyber. Donc d'une part, que ce soit à des filles ou des garçons, je suis ouvert pour expliquer ma profession. J'ai un métier passion. Faire découvrir ma passion à des femmes, des hommes ou dédiée aux deux, je le fais volontiers."*

H4 : *“Je n'ai participé qu'une seule fois quand j'en ai eu l'occasion. J'ai trouvé l'initiative très intéressante. L'approche était plus intéressante. Maintenant, il faut quand même davantage développer les choses. Une initiative telle que Women4Cyber, c'est très bien mais il faut davantage d'encadrement c'est-à-dire un peu plus de personnel, un peu plus dévoué, parce qu'il y a énormément de femmes qui aimeraient bien atteindre l'objectif de travailler dans le domaine de la sécurité.”*

2.6. Les recommandations pour un environnement de travail inclusif

Pour un environnement de travail inclusif, le premier critère est le management. En effet, le management doit être capable de créer cet environnement inclusif pour tous ses collaborateurs. Pour ce faire, il doit être à l'écoute, prêt à réagir mais aussi penser à valoriser son (ses) équipe(s). Les managers doivent montrer que tout le monde est traité sur un pied d'égalité. Enfin, les collaborateurs ne doivent pas avoir peur de remonter n'importe quel incident. Les managers doivent ainsi créer un climat de confiance entre eux et leurs équipes. Il faut que ces derniers prennent le temps de penser d'abord à l'humain avant le résultat.

RH2 : *“Ensuite, il y a un accompagnement du manager. Ce dernier doit faire attention à ces sujets et dire justement que, si une femme fait face à ce genre de situation, il faut surtout ne pas se taire et remonter au management.[...] L'objectif est que les gens se sentent à l'aise pour remonter.”*

F4 : *“Il faut de l'écoute et de l'action lorsque des femmes se plaignent de comportements inappropriés. Il devrait y avoir des mesures prises et mises en place de manière efficace pour encourager une culture où les problèmes sont signalés.”*

H1 : *“Je pense qu'hommes ou femmes doivent se sentir valorisés face à leur travail. Les managers peuvent donc essayer de moins rechercher les résultats et de penser un peu plus à l'humain derrière l'ordinateur.”*

H4 : *“C'est avoir un bon manager afin de développer une entente et un esprit d'équipe. Resserrer les liens de l'équipe aura une bonne influence sur la manière dont on voit nos collègues, comment on interagit avec eux. De plus, le manager doit aussi affirmer que tout le monde est au même pied d'égalité, que tout le monde mérite le même respect. Il pourrait aussi valoriser un peu plus ses subordonnés, reconnaître la valeur ajoutée de chaque personne. Je conseillerais aussi au management d'être davantage à l'écoute.”*

F4 : *“Il faut donc essayer de travailler avec les horaires de chacun, de s'adapter aux besoins de tous. Il faut arrêter la vision de “rester tard, c'est bien vu”. Finalement, il faut juste être humain.”*

Afin de créer un environnement où tout le monde est respecté, il faudrait revoir la vision de tous les travailleurs sur les compétences techniques. En effet, ces dernières sont encore trop sous-estimées par rapport aux compétences techniques. Cela a pour effet de discriminer les femmes, dont les profils sont plus souvent non techniques¹³³.

¹³³ cf. 2.1. Les études

F2 : *“Puis, travailler sur la reconnaissance de compétences non techniques. Comment elles peuvent s'appliquer et comment elles peuvent être utiles dans le travail quotidien.”*

F5 : *“il faut faire comprendre aux entreprises qu'il ne faut plus seulement embaucher des candidats avec un background purement IT ou d'ingénieur. Il faut se tourner vers d'autres domaines d'activité. Toutes les personnes venant d'autres domaines peuvent arriver à faire de la cybersécurité. C'est la passion qui va leur permettre de réussir.”*

La sensibilisation de la gente masculine aux différents défis que les femmes peuvent rencontrer en choisissant une carrière en cybersécurité est absolument nécessaire.

H4 : *“Déjà les accepter, leur donner la chance de pouvoir s'exprimer et d'effectuer des tests comme n'importe qui. Instaurer le respect doit être le dénominateur commun de toutes initiatives.”*

F1 : *“Sensibiliser les hommes sur leurs biais. Ce n'est pas parce que je suis une femme, que je n'ai pas fait d'étude en cybersécurité à proprement parlé que je suis incompétente. Je n'ai pas d'enfants donc ils n'ont pas à me proposer de reprendre mon travail pour que je quitte plus tôt. Je n'ai pas besoin d'être chouchoutée.”*

F2 : *“Chez nous, on a un groupe de travail sur la diversité et l'inclusion. [...] Je pense qu'un petit groupe de travail comme ça peut avoir des bénéfices.”*

RH2 : *“Par contre, on n'a pas beaucoup travaillé sur les hommes. En fait, on n'a pas considéré que, pour eux, c'était un changement. Je dirais donc que les femmes doivent avoir de l'empathie pour les hommes. Pour eux, c'est nouveau. Il faut leur expliquer. Il faut aussi avoir de la pédagogie pour dire simplement les choses. Ça passe par la communication non violente en se disant “j'ai l'empathie de me dire que, peut-être, cet homme n'a pas conscience de ses biais”. Il y a beaucoup de maladresses et discuter de ces sujets aident les gens à changer. Je vois que c'est un manque de communication entre les parties qui fait qu'il y a des relations qui se cassent. Avoir cette empathie pour avoir des discussions, pas uniquement avec les femmes pour qu'elles osent mais aussi, pour aider les hommes à accueillir cette diversité. On leur reproche plein de choses, mais on ne leur dit pas concrètement ce qu'on attend non plus. Il faut qu'on leur dise, je pense.”*

2.7. La diversité de genre au sein des équipes

La diversité apporte, selon les participants, divers avantages aux entreprises, notamment le renforcement des liaisons au sein de l'équipe, des perspectives différentes pour la résolution de problèmes ainsi qu'un atout pour la marque employeur des entreprises. La diversité n'est pas seulement importante pour le secteur de la cybersécurité mais pour tous les secteurs d'activités.

H2 : *“Oui, je dirais 2 choses. La première, c'est d'essayer de viser la parité homme-femme, quel que soit le type de métier. Le fait d'avoir des hommes et des femmes dans les équipes, ça renforce les*

liaisons au sein de celle-ci. Des équipes exclusivement constituées d'hommes ou exclusivement de femmes, en général, ne fonctionnent pas aussi bien."

RH1 : *"Je ne suis pas sûre que ce soit vraiment quelque chose qui soit spécifiquement lié à la cybersécurité. Je pense que c'est plutôt applicable au monde en général. La diversité est ce qui apporte le plus d'idées, de mélanges et de résultats. D'ailleurs, il existe une étude qui explique que les décisions sont plus efficaces lorsqu'elles sont prises à parts égales entre hommes et femmes. Pour moi, cela semble logique car nous ne pensons pas de la même manière. [...]. Cela apporte une véritable valeur ajoutée, car lorsqu'il y a des débats, des sessions de brainstorming, les femmes apportent des idées que les hommes n'auraient pas eues. Que ce soit en termes d'idées, de décisions, d'organisation ou dans plein d'autres domaines, les femmes apportent une plus-value."*

RH3 : *"Oui, mais je crois que ce n'est pas seulement dans l'industrie de l'IT ou dans la cybersécurité. On sait que la diversité dans le leadership, mais aussi dans l'entreprise en général, a beaucoup d'impact sur le taux d'innovation, sur la performance financière, sur la façon dont les décisions sont prises, et ainsi de suite. En fait, ça a même davantage d'impact.[...] Forbes a également réalisé des études sur la prise de décisions, montrant que si une décision est prise par un groupe homogène, le taux de qualité des décisions atteint 58 %. Si le groupe est diversifié en termes de genre, d'âge, de culture, etc., la qualité des décisions augmente."*

RH4 : *"Deuxièmement, c'est que cela donnerait, d'un point de vue plus commercial, une meilleure visibilité. En fait, cela permettrait de présenter la société de manière plus favorable.[...] A tous les niveaux, il serait bénéfique d'avoir plus de femmes dans un secteur plus masculin."*

3. Discussion

Dans l'ensemble, les résultats sont conformes à ce que la littérature peut nous enseigner sur le monde de la cybersécurité et sur sa main-d'œuvre.

Le taux de représentation des femmes dans les entreprises des interviewés correspond généralement à la proportion des femmes dans les métiers de la cybersécurité selon l'étude de 2022 d'(ISC)² c'est-à-dire, environ 25%. Selon les données de l'OCDE, les femmes ont tendance à s'orienter dans les études non techniques. Cela s'est confirmé au travers des différentes interviews. Un responsable des ressources humaines de l'enquête a, néanmoins, affirmé avoir la parité dans son équipe de cybersécurité. Il a émis l'hypothèse que c'était grâce au caractère social de son entreprise (ONG). En effet, les femmes travaillant dans la cybersécurité sont susceptibles d'être attirées par ce type d'organisation humanitaire. Accenture et *Girls Who Code* (2019) ont rapporté de leur enquête que *"contribuer à la société"* faisait partie des trois priorités dans leur choix de carrière.

Depuis la phase de recrutement jusqu'à la phase de promotion et de gestion des performances, les femmes font face à des défis. Ce climat peut les mener à quitter le domaine (Wirth, 2019 ; Poster, 2018). Les femmes ont également pointé du doigt des retards inexpliqués en termes de promotion et

de progression dans leur carrière (53%¹³⁴) ainsi que des réactions exagérées à leurs erreurs (29%¹³⁵) (Panhans et al., 2022). Les biais rencontrés durant le recrutement peuvent aussi se manifester durant les évaluations de performance, les décisions prises concernant les promotions, ainsi que dans les systèmes de récompense basés sur le mérite. Les femmes participant à l'étude ont trouvé qu'il n'y avait aucune barrière concernant leur promotion. Elles ont toutes déjà été promues ou augmentées au moins une fois, à l'exception de F3 qui est toujours étudiante. Les femmes souffrent encore de sexisme dans leur sphère professionnelle. Elles subissent également des discriminations à cause de leur genre. Par exemple, elles doivent sans cesse prouver leur légitimité, qu'elles ne sont pas là pour apporter le café ou prendre des notes. Elles peuvent aussi subir un harcèlement sexuel régulier. Tout cela représente des freins au développement des femmes dans les métiers de la cybersécurité. De plus, une des participantes à l'étude a développé le fait que les quotas n'aident pas toujours les femmes. Selon son expérience, la présence de quotas va encore faire diminuer la légitimité des femmes aux yeux des hommes vu qu'elles seront engagées seulement à cause de cette obligation et, non, pour leurs compétences.

Bien que trois femmes sur cinq viennent d'études purement techniques (cybersécurité ou informatique), elles ont toutes affirmé que les femmes venaient généralement d'autres domaines considérés comme non techniques - sciences politiques, management, etc. Les hommes ont aussi confirmé ce résultat. Ensuite, les femmes qui désirent s'engager dans des études en cybersécurité peuvent se sentir marginalisées, par le fait qu'elles n'aient pas le sentiment d'appartenir au groupe des étudiants masculins (Deloitte, 2021 ; Stanford University's Clayman Institute for Gender Research, 2017 ; Panhans et al., 2022 ; Weingarten et Garcia, 2015). Cette idée est confirmée par la totalité des travailleurs en cybersécurité interrogés. Ils ajoutent, cependant, que les femmes, lorsqu'elles sont éveillées au sujet, seront plus motivées et plus sûres de leur choix concernant leurs études en cybersécurité que les hommes. En effet, les résultats montrent que l'image de la cybersécurité est une barrière à l'entrée des femmes dans ce genre d'études. Autant la littérature que les répondants affirment que cette image est erronée. La cybersécurité est bien plus que l'image de "*l'homme blanc boutonneux devant son ordinateur*" que l'on se fait (Poster, 2018 ; Wirth, 2019).

En termes de *hard skills*, elles sont imposées par le métier que les individus exercent, peu importe le genre des travailleurs. Ces compétences varient en fonction du domaine d'études et n'ont aucun lien avec le genre. Selon les données de l'OCDE en 2020, les femmes ont tendance à préférer les études de sciences sociales, de journalisme, d'art, de santé, de management et d'éducation qu'importe le degré alors que les hommes ont plus tendance à se diriger vers des études de management, de droit, d'ingénierie et, dans une moindre mesure, les sciences sociales, le journalisme et la santé. En regardant les données de l'OCDE, on remarque que, finalement, les hommes ne sont pas si intéressés que cela par TICs. Cependant, il reste trois fois plus d'hommes en bachelier et en master dans le domaine des TICs. On arrive donc à la conclusion qu'il y a bien plus d'hommes techniques que de femmes. Cela est sûrement la raison pour laquelle les femmes sont considérées plus compétentes en technique que les hommes. Vu qu'elles sont peu, elles doivent toujours en faire plus pour prouver qu'elles ont leur place, selon F4. Les *softs skills* semblent différer en fonction du genre, voire même

¹³⁴ Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalan, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

¹³⁵ Ibid.

être associées à des constructions sociales. Les femmes sont considérées comme plus sensibles, plus à l'écoute, plus empathiques. Elles sont aussi associées à la communication, au sens du détail, à l'aversion au risque et à la créativité. Contrairement aux hommes, ces derniers sont vus comme des leaders, des personnes directes et moins organisées. Cependant, il reste des *soft skills*, ou traits de caractère, qui correspondent au besoin de la profession et que les deux genres doivent posséder pour exceller dans leur tâche. Potter et Vickers (2015) affirment que chaque catégorie de métiers (consultants, managers, ingénieurs...) a besoin d'un éventail de hard skills et de soft skills, peu importe le genre de l'employé. Néanmoins, les femmes doivent avoir presque obligatoirement un caractère bien trempé et du répondant afin de ne pas se laisser faire lorsqu'une injustice, une remarque sexiste ou un comportement inapproprié arrive.

Les résultats de l'étude ont permis de développer davantage les relations au travail par rapport à la littérature existante. Ces dernières peuvent prendre différentes formes. Premièrement, il y a les relations avec les collègues. Les femmes et les hommes n'interagissent pas de la même manière entre eux. Les hommes peuvent avoir des comportements misogynes et sexistes envers les femmes. Cependant, lorsque chaque personne de l'équipe montre du respect à son/sa collègue et reste professionnelle, les relations sont cordiales et agréables que ça soit pour les hommes ou pour les femmes. En général, les hommes changent légèrement leur comportement quand ils s'adressent à une femme. Le fait d'être une femme apporte aussi d'autres besoins. Les femmes ne peuvent pas rester aussi longtemps que leurs collègues masculins au bureau, ce qui diminue leurs opportunités de *networking* (Accenture et Girls Who Code, 2019). Ce témoignage confirme l'étude de Weingarten et Garcia (2015). Les femmes endossent encore les responsabilités liées aux soins de personnes tiers. Ensuite, il y a les relations avec les clients. Malgré leurs compétences en gestion des relations, les femmes peuvent encore subir des comportements discriminatoires de la part des clients qu'elles doivent servir. Certaines entreprises tiennent beaucoup plus à leurs employées qu'à la relation avec le client donc, quand un comportement inapproprié se déroule, elles préfèrent couper net la relation commerciale. C'est le cas pour deux des entreprises de mon échantillon. Les cyber-travailleuses ont un côté facilitateur quand elles servent des clientes féminines.

Le mentorat est l'aide qu'apporte un collègue ou une personne extérieure à une personne peu expérimentée dans le cas présent, aux nouvelles employées en cybersécurité. Les mentors et les parrains sont essentiels pour aider les jeunes filles et les femmes à s'orienter dans l'ensemble du secteur et développer leurs compétences (Panahans et al., 2022). Le mentor donne à sa mentorée des conseils, des contacts, des voies de carrière ainsi que les certifications utiles à passer. Le mentor joue le rôle de repère et de source d'informations pour la nouvelle génération de femmes en cybersécurité. Les répondants à l'étude trouvent unanimement que ce genre de programme est intéressant autant pour les femmes que pour les entreprises. Cependant, H3 a soulevé le fait que ce genre de programme ne devrait pas être seulement destiné aux femmes. Il faudrait développer des programmes de mentorat mixtes.

Afin de promouvoir la représentation des femmes au sein de leurs effectifs, les entreprises réalisent des partenariats avec des établissements scolaires et des organisations telles que *Women4Cyber*, par exemple. Elles ont envie de développer leur population de femmes en cybersécurité en résolvant le manque d'attrait pour les études STIM des femmes. En changeant l'image perçue de la cybersécurité ainsi qu'en informant, simplement, plus sur la multitude de métiers disponibles en cybersécurité,

plus de femmes pourraient envisager de suivre des études liées à ce domaine. S'associer à *Women4Cyber* permet aux entreprises d'atteindre une communauté de femmes au sein de leur région. Pour augmenter le taux de présence de femmes dans leurs équipes de cybersécurité, ils peuvent proposer des opportunités de reskilling et de stages au sein de leurs bureaux.

Les établissements scolaires ainsi que les entreprises utilisent différents canaux afin de sensibiliser les femmes à la cybersécurité. Dans le but d'informer, de motiver et de créer des vocations, ils utilisent les jobs fairs, les réseaux sociaux comme *LinkedIn* afin de partager et de mettre en évidence leur culture inclusive et la présence de femmes. Montrer qu'il y a des femmes dans les métiers et les études du secteur de la cybersécurité est très important vu que les potentielles employées et étudiantes pourront s'identifier à ces dernières.

Les responsables en ressources humaines peuvent aussi influencer sur la présence des femmes au sein de leur entreprise. En effet, la manière dont le recrutement est abordé - recherche de profils "parfaits", par exemple -, peut biaiser le regard du recruteur sur le candidat. Dans le but d'améliorer l'accès aux professions de la cybersécurité, les entreprises devraient accorder plus d'importance aux compétences non techniques. Cela permettrait de recruter des profils venant d'autres domaines. Cette façon de procéder permettrait de réduire la pénurie de main-d'œuvre et renforcer l'accès aux métiers de la cybersécurité, spécialement pour les femmes dont les profils sont moins techniques que les hommes. Néanmoins, en recrutant de cette manière, les entreprises devront fournir des formations techniques à leurs nouveaux arrivants vu la complexité de la cybersécurité et le besoin de compétences techniques pour réaliser les différentes tâches des fonctions (Deloitte, 2021 ; Panhans et al., 2022). Un autre moyen proposé par les participants de l'enquête pour développer le bassin de candidates de leur entreprise, est le remaniement des descriptions de poste. Les professionnels du recrutement devraient rendre ces descriptions plus inclusives. Cela laisserait aux femmes l'idée que le poste n'est pas seulement ouvert pour les hommes et qu'elles ont le profil pour candidater. Ils peuvent aussi sensibiliser tous les autres acteurs du recrutement avec lesquels ils travaillent sur la nécessité d'engager plus de femmes. Malgré cela, le marché de l'emploi en cybersécurité reste tendu. Les recruteurs ne peuvent pas tous se permettre comme RH2 de faire attention à la parité de ses candidatures. RH5, par exemple, avait besoin de candidats qualifiés directement. Elle ne pouvait pas se permettre d'attendre la candidature d'une femme pour le poste.

L'aspect formation n'est pas seulement réservé aux femmes. Les entreprises de la cybersécurité forment tout leur personnel. Cela corrobore le fait que le monde de la cybersécurité est en constante évolution et qu'il y a besoin constamment d'un effectif compétent et à jour sur les dernières découvertes, féminin ou non.

Beaucoup des participants à l'étude ont déjà pris part à des initiatives encourageant le développement des femmes en cybersécurité. F1, F2, F3 et F5 font partie de *Women4Cyber*. F4 fait partie de la communauté *Blackhoodie*. Quant aux hommes, trois sur les cinq ont déjà participé à des initiatives que ce soit à titre personnel ou dans leur entreprise. Cela affirme que le personnel devient de plus en plus éveillé sur les problématiques de genre et souhaite s'y investir.

Pour un environnement de travail inclusif, le premier critère est le management. En effet, le management doit être capable de créer cet environnement inclusif pour tous ses collaborateurs. Comme expliqué dans la littérature, les entreprises doivent favoriser la prise de parole. Les résultats

de l'enquête ajoutent que les managers sont tenus aussi être à l'écoute, prêts à réagir et à valoriser leurs équipes. Tous les collaborateurs sont sur un même pied d'égalité. Enfin, les employés ne doivent pas craindre de remonter les incidents survenus sur leur lieu de travail. Pour ce faire, les managers sont responsables de la création de climat de confiance entre leurs équipes et eux-mêmes. L'Humain a besoin de passer avant les résultats pour développer une culture inclusive au sein des organisations. Afin de créer un environnement où tout le monde est respecté, la vision de tous les travailleurs sur les compétences non techniques nécessite une révision. En effet, ces dernières sont encore trop sous-estimées par rapport aux compétences techniques. Cela a pour effet de discriminer les femmes, dont les profils sont plus souvent non techniques. Les compétences en gestion de projet et en travail d'équipe pour mener à bien un projet de cybersécurité, les compétences en communication et en leadership pour s'engager avec l'organisation au sens large, ainsi que la créativité et la flexibilité nécessaires pour adapter une solution à une situation spécifique, sont tout aussi appréciées que les compétences techniques (Hall et Rao, 2020 ; Sussman, 2020). Les intervenants ont ajouté, comme dernière recommandation, la sensibilisation de la gente masculine aux différents défis que les femmes peuvent rencontrer en choisissant une carrière en cybersécurité est absolument nécessaire.

La diversité apporte, selon les participants, divers avantages aux entreprises, notamment le renforcement des liaisons au sein de l'équipe, des perspectives différentes pour la résolution de problèmes ainsi qu'un atout pour la marque employeur des entreprises. La diversité n'est pas seulement importante pour le secteur de la cybersécurité mais pour tous les secteurs d'activités.

4. Recommandations

Pour améliorer la représentation et la participation des femmes en cybersécurité, les managers ainsi que les ressources humaines doivent se pencher sur la création d'un environnement inclusif. Pour être inclusif sur le lieu de travail, les responsables RH et le management pourront développer les perspectives d'avancement professionnel des femmes mais aussi favoriser un environnement diversifié et collaboratif. Les critères de décisions pourront être la mesure de nombre de femmes occupant une fonction en cybersécurité, le taux de recrutement des cyber-professionnelles, le taux de rétention, l'évaluation du climat de l'entreprise en rapport avec l'inclusion et l'égalité, le taux de participation des femmes dans les différentes initiatives ainsi que l'évaluation des impacts apportés par une plus grande diversité de genre (performance, créativité, etc.).

Concrètement, les entreprises peuvent mettre en place différentes initiatives concrètes pour promouvoir les femmes dans ces métiers masculins et augmenter l'égalité de genre au sein de leurs bureaux.

- **Développer un service de garderie ainsi que sensibiliser les hommes à la charge mentale.** Les femmes sont les premières concernées par les responsabilités liées à la famille. Les entreprises pourraient attirer et retenir plus de femmes si elles les soutiennent. Les RH pourraient développer des newsletters sur le sujet de la charge mentale afin d'informer au

mieux tous les hommes de l'entreprise. Cette recommandation serait néanmoins coûteuse pour l'entreprise. Il faudrait compter l'aménagement de locaux, l'embauche d'un personnel de garderie ainsi que l'achat de fournitures. En plus de ces coûts, il y a le respect des réglementations (sécurité, santé, etc.).

- **Mettre sur pied un programme de mentoring.** Parmi les différentes initiatives citées dans les entretiens, le mentoring est celui qui a été le plus acclamé par les participants. Les entreprises organiseraient des rencontres entre les mentors et les mentorées. Toute cette initiative se ferait sur une base volontaire. Ce programme pourrait rassurer les femmes qui commencent en cybersécurité car il leur fournirait un point d'ancrage, un modèle et une source d'information. Il a été prouvé, autant par la littérature que par l'étude ci-dessus, que les femmes avaient plus de chance d'entrer et de rester dans une entreprise lorsqu'elles pouvaient avoir un modèle et une communauté à qui se référer. De même que le mentoring, les entreprises pourraient mettre en place une communauté de femmes en cybersécurité. Cela augmenterait leur sentiment d'appartenance à l'entreprise et serait un atout de choix pour une campagne de recrutement sur les réseaux sociaux, tels que *LinkedIn*. Vu que cela serait sur une base volontaire, l'engagement pourrait vraiment être limité, encore plus sur le long terme que le court terme. En outre, il y aurait sûrement une grande différence entre l'offre (nombre de mentors) et la demande (nombre de mentorées). Les responsables RH pourraient mettre en binôme un(e) mentor avec une mentorée alors qu'ils seraient totalement incompatibles, ce qui nuirait à l'efficacité du mentoring. Ce genre de programme demande beaucoup de temps et de ressources (argent, personnel, etc.).
- **Valoriser les compétences non techniques afin de prouver leur importance.** Les managers pourraient récompenser la créativité, l'innovation ainsi que d'autres compétences non techniques que leurs subordonnés peuvent montrer. Les femmes sont représentées comme particulièrement créatives. Cette valorisation de compétences leur permettrait de faire valoir leur légitimité. Ce serait une action concrète vis-à-vis des hommes qui ont tendance à sous-estimer leurs capacités. Cela aura l'avantage d'augmenter le taux de rétention des femmes de l'entreprise. Cependant, c'est très subjectif. Les managers pourraient avoir des préjugés inconscients et donc ne pas percevoir, ni évaluer ces compétences de manière juste. Certains employés, plus anciens, ne pourraient pas comprendre cette nouvelle approche. Ils pourraient ne pas en percevoir la valeur directement. Cela nécessiterait sûrement un effort de sensibilisation de la part des managers et des ressources humaines.

5. Conclusion

Le secteur de la cybersécurité est en pleine expansion, surtout depuis la crise du COVID-19. En 2028, son chiffre d'affaires devrait atteindre 257 milliards de dollars¹³⁶. Cependant, le secteur est en manque significatif de main-d'œuvre. Les entreprises tentent de combler le déficit mondial de 3,4

¹³⁶ Nguyen, P-H. (2023). Cybersecurity - Market data Analysis & Forecasts | Statista. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

millions de travailleurs en cybersécurité¹³⁷ ((ISC)², 2022). Cette pénurie affecte autant les entreprises que la société en général. Les formations et les métiers dans le domaine de la cybersécurité sont divers et variés. Ils répondent à l'aspect multidisciplinaire de ce domaine. Pour travailler en cybersécurité, les candidats ont besoin tant de compétences techniques que de compétences non techniques. Les métiers s'y rapportant requièrent autant de connaissances approfondies en "architecture de sécurité de l'information ; gestion des risques et conformité; et en analyse du renseignement/de la menace" (Caldwell, 2013, p. 6) que de connaissances en sciences sociales, sciences politiques et management. Pour exceller, les employés doivent aussi développer un panel de *soft skills* telles que la curiosité, le sens éthique, la collaboration et la flexibilité.

Pour résorber ce déficit de main-d'œuvre, les entreprises sont encouragées à se tourner vers un bassin de candidats sous-exploités : les femmes. En effet, les femmes ne représentent que 24%¹³⁸ de l'effectif en cybersécurité alors qu'elles représentent 50%¹³⁹ de la population active mondiale. Ce faible ratio est dus à plusieurs barrières mises sur les chemins des femmes tels que la rémunération, l'image perçue du secteur de la cybersécurité, les constructions sociales, le harcèlement et la discrimination. L'avenir de la cybersécurité dépend de sa capacité à attirer, retenir et promouvoir les femmes (Poster, 2018). Pour ce faire, la littérature donne quelques pistes comme les mouvements promouvant les femmes dans la cybersécurité, la création d'une culture plus inclusive dans le monde scolaire et universitaire, une modification du processus de recrutement et une mise-à-jour de l'image de la cybersécurité. De plus, la diversité est devenue un élément essentiel à la réussite des entreprises. 97%¹⁴⁰ des entreprises interrogées par Forbes ont développé des stratégies formelles de diversité et d'inclusion. Des entretiens réalisés auprès de quinze professionnels de la cybersécurité en Belgique permettent d'étayer les particularités du monde de la cybersécurité et de sa main-d'œuvre ainsi que l'importance d'investir dans la diversité et, notamment, dans la représentation des femmes dans la cybersécurité.

Ce mémoire s'établit dans l'optique d'enrichir la littérature concernant la cybersécurité et sa main-d'œuvre. Cette étude cherche à mettre en évidence la situation des femmes dans les métiers de la cybersécurité ainsi que les différents défis auxquels elles sont confrontées durant leurs études et leur carrière. Elle a aussi développé l'importance des femmes et de la diversité au sein des entreprises de cybersécurité afin de réduire les risques et d'améliorer la prise de décision. Cette étude nous aide à mieux comprendre la façon de combler les écarts entre les hommes et les femmes dans le secteur de la cybersécurité à l'aide de différentes initiatives.

Cependant, la validité externe de l'étude est faible. En effet, la généralisation des résultats obtenus lors des entretiens ne peut pas être appliquée à toute la population mondiale. L'étude impliquait seulement des personnes travaillant en Belgique et d'origine belge ou française. De plus, cet échantillon était assez restreint, cinq personnes par catégorie (femmes, hommes et professionnels en ressources humaines). Cet échantillon a été prélevé dans les communautés de *Women4Cyber* et

¹³⁷ Ibid.

¹³⁸ p.4

¹³⁹ Gammarano, R. (2019). 100 statistiques sur l'OIT et le marché du travail pour célébrer le centenaire de l'OIT. ILOSTAT. point 62 <https://ilostat.ilo.org/fr/100-statistics-on-the-ilo-and-the-labour-market/>

¹⁴⁰ *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce*. (2021). Forbes Insight. p.11

de *Be Cyber*, cela laisse sous-entendre que ce sont des personnes qui, pour la majorité, s'intéressaient déjà à la sous-représentation des femmes dans les métiers de la cybersécurité.

Les recherches futures pourraient examiner l'efficacité des initiatives pour promouvoir la représentation des femmes dans les métiers de la cybersécurité. En effet, lors des entretiens, seulement deux responsables en ressources humaines ont été capables de donner un retour sur leurs initiatives. Les autres ont affirmé que le laps de temps entre le lancement de leur politique et leur entretien était trop court pour estimer des retombées positives ou négatives. Les recherches futures pourraient aussi approfondir l'efficacité des initiatives sur une population qui n'a pas d'intérêt particulier pour la diversité de genre dans leurs équipes.

Bibliographie

Accenture et Girls Who Code. (2019). *Resetting Tech Culture : 5 strategies to keep women in tech*. <https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-134/accenture-a4-gwc-report-final1.pdf#zoom%3D50>

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19 : a survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10), 8176-8206. <https://doi.org/10.1016/j.jksuci.2022.08.003>

AustCyber, Australia's Cyber Security Sector Competitiveness Plan, Australian Cybersecurity Growth Network, 2018.

ANSSI. (s.d). *Le Cybermoi/s*. ANSSI.

<https://www.ssi.gouv.fr/agence/cybersecurite/le-cybermois/#:~:text=Le%20cybermoi%2Fs%20est%20la,instant%20de%20votre%20vie%20num%C3%A9rique>

Bishop, E. (2020). Closing cybersecurity's gender gap can aid the skills shortage and the economy. *Forbes*.

<https://www.forbes.com/sites/forbestechcouncil/2020/05/20/closing-cybersecuritys-gender-gap-can-aid-the-skills-shortage-and-the-economy/?sh=285eeb63495a>

Blažič, B.J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. *Educ Inf Technol* 27, 3011–3036 (2022). <https://doi.org/10.1007/s10639-021-10704-y>

Brugman, S. (2022). 2022 Activity Report Women4Cyber Mari Kert – St Aubyn Foundation.

<https://women4cyber.eu/wp-content/uploads/2023/04/W4C-Activity-Report-2022-1.pdf>

Calanca, F., Sayfullina, L., Minkus, L. *et al*. Responsible team players wanted: an analysis of soft skill requirements in job advertisements. *EPJ Data Sci.* 8, 13 (2019). <https://doi.org/10.1140/epjds/s13688-019-0190-z>

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, 2013(7), 5-10. [https://doi.org/10.1016/s1361-3723\(13\)70062-9](https://doi.org/10.1016/s1361-3723(13)70062-9)

Centre canadien pour la Cybersécurité. (2022). *Certifications dans le domaine de la cybersécurité*. <https://www.cyber.gc.ca/fr/orientation/certifications-dans-le-domaine-de-la-cybersecurite>

Centre pour la Cybersécurité Belgique. (2023). *Formations en cybersécurité en Belgique*. <https://ccb.belgium.be/fr/formations-en-cybers%C3%A9curit%C3%A9-en-belgique>

Cercle des Femmes de la Cybersécurité. (2019). *Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité : guide des métiers, formations et opportunités de la cybersécurité*. ISBN: 978-2-7496-0162-5

Check Point Research Team. (2023). International Women's Day : Achieving gender parity in the C-Suite and advancing equity in the cybersecurity. *Check Point Blog*. <https://blog.checkpoint.com/2023/03/08/international-womens-day-achieving-gender-parity-in-the-c-suite-and-advancing-equity-in-the-cybersecurity-industry/>

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). *Defining Cybersecurity*. TIM Review. <https://www.timreview.ca/article/835>

Cyber Seek. (s.d). *Cybersecurity career pathway*. <https://www.cyberseek.org/pathway.html>

Dawson, J. and Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Front. Psychol.* 9:744. doi: 10.3389/fpsyg.2018.00744

Deloitte. (2021). *Women in Cyber : Building Leaders and Improving Cybersecurity with a New Approach*. <https://www.deloitte.com/global/en/services/risk-advisory/blogs/women-in-cyber-building-leaders-and-improving-cybersecurity-with-a-new-approach.html>

Digital Wallonia. (s.d). *Cyberwal by digital wallonia*. Digital Wallonia. <https://www.digitalwallonia.be/cyberwal/>

ECC University. (2023). Top 10 Most In-Demand Leadership Skills for Cybersecurity Professionals. *Accredited Online Cyber Security Degree Programs | EC-Council University*. <https://www.eccu.edu/blog/technology/top-10-most-in-demand-leadership-skills-for-cybersecurity-professionals/>

EDEC. (2022). *Executive Master ou EMBA : quelles différences, comment choisir ?*. EDHEC BUSINESS SCHOOL. <https://www.edhec.edu/fr/news/executive-master-ou-emba-queelles-differences-comment-choisir#:~:text=L'Executive%20Master%20r%C3%A9unit%20des,%2B2%20%C3%A0%20Bac%20%2B4.>

ENISA. (2022). European Cybersecurity Skills Framework (ECSF) - User Manual. <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>

European Union Agency for Cybersecurity, (2022). *European cybersecurity skills framework (ECSF) – User manual*, European Union Agency for Cybersecurity. <https://data.europa.eu/doi/10.2824/95989>

Equipe éditoriale d'Indeed. (2023). Qu'est-ce que sont les hard skills et les soft skills?. Indeed. <https://emplois.be.indeed.com/conseils-carriere/evolution-professionnelle/competences-pratiques>

Fischer, P. J. (2022). A Cybersecurity Skills Framework. *IGI Global EBooks*. <https://doi.org/10.4018/978-1-6684-3554-0.ch010>

Forbes Insight. (2021). *Global Diversity and Inclusion : Fostering Innovation Through a Diverse Workforce*. https://www.forbes.com/forbesinsights/innovation_diversity/

Frost & Sullivan. (2012). *Agent Of Change : Women in the Information Security Profession GISWS Subreport*. <https://fr.scribd.com/document/471283769/Women-in-the-Information-Security-Profession-GISWS-Subreport#>

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*, 102080. <https://doi.org/10.1016/j.cose.2020.102080>

Gammarano, R. (2022, août 23). 100 statistiques sur l'OIT et le marché du travail pour célébrer le centenaire de l'OIT. *ILOSTAT*. <https://ilostat.ilo.org/fr/100-statistics-on-the-ilo-and-the-labour-market/>

Gardia Cybersecurity School. (2023). *Quelles sont les certifications en cybersécurité ?*. <https://guardia.school/boite-a-outils/quelles-sont-les-certifications-en-cybersecurite.html>

Girls Who Code. (2022). *The Next Generation - Annual Report 2022*. <https://girlswhocode.com/2022report/>

Graham C. M. & Lu Y. (2022). Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements, *Journal of Computer Information Systems*, <https://doi.org/10.1080/08874417.2022.2115954>

Hall J. L. and Rao A., "Non-Technical skills needed by cyber security graduates," 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 2020, pp. 354-358, doi: 10.1109/EDUCON45650.2020.9125105.

Indeed. (2023). Expert en cybersécurité : la fiche métier. *Indeed.com France*. <https://fr.indeed.com/conseils-carrieres/trouver-un-emploi/expert-cybersecurite-fiche-metier>

(ISC)². (2022). *Cybersecurity Workforce Study*. (ISC)².
<https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>

(ISC)². (2018). *Women in Cybersecurity : Young, Educated and Ready to Take Charge*. Women in Cybersecurity. (ISC)².
<https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38>

ITU. (s.d). *Women in Cyber Mentorship programme*.
<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/Women-in-Cyber-Mentorship-Programme.aspx>

Kremer S., Mé L., Rémy D., Roca V. (2019). Cybersécurité. *Inria*. <https://hal.inria.fr/hal-02414281>

Kshetri N. and Chhetri M. (2022). Gender Asymmetry in Cybersecurity: Socioeconomic Causes and Consequences, in *Computer*, vol. 55, no. 2, pp. 72-77, doi: 10.1109/MC.2021.3127992.

Le Roy J., 2021, Psyber Sécurité : l'apport de la psychologie dans le management de la cybersécurité, *Revue Internationale de Management et de Stratégie*, <http://www.revue-rms.fr/>.

Libicki, M. et al. *Hackers Wanted: An Examination of the Cybersecurity Labor Market*. RAND Corporation, 2014. *JSTOR*, <http://www.jstor.org/stable/10.7249/j.ctt7zvzmj>.

Lissitsa, S., & Laor, T. (2021). Baby Boomers, Generation X and Generation Y : Identifying generational differences in effects of personality traits in on-demand radio use. *Technology in Society*, 64, 101526. <https://doi.org/10.1016/j.techsoc.2021.101526>

Martin, K. (2019). Europe et cybersécurité : quelle(s) base(s) industrielle(s) ?. *Revue Défense Nationale*, 819, 107-113. <https://doi.org/10.3917/rdna.819.0107>

Meier, O., & Roy, J. L. (2022). Oser réinventer le recrutement pour faire face à la pénurie de compétences en cybersécurité. *Management & data science*. <https://doi.org/10.36863/mds.a.19997>

Nguyen, P-H. (2023). *Cybersecurity - Market data Analysis & Forecasts | Statista*. Statista. <https://www.statista.com/study/124902/cybersecurity-report/>

OECD. (2020). *Enrolment by gender, programme orientation, mode of study and type of institution*. OECD Statistics. https://stats.oecd.org/Index.aspx?DataSetCode=EAG_ENRL_SHARE_CATEGORY

Panhans, D., Hoteit, L., Yousuf, S., Breward, T., Wong, C., AlFaadhel, A. M., & AlShaalán, B. H. (2022). Empowering women to work in cybersecurity is a Win-Win. *BCG Global*. <https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-win>

Parker, A., & Brown, I. (2019). Skills requirements for Cyber security professionals : A content analysis of job descriptions in South Africa. *Communications in computer and information science* (p. 176-192). https://doi.org/10.1007/978-3-030-11407-7_13

Peslak, A. & D. Hunsinger, S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking?. *Issues in Information Systems Volume 20, Issue 2*, pp. 62-72. https://iacis.org/iis/2019/2_iis_2019_62-72.pdf

Pigeyre, F. (2021). 13. Égalité professionnelle ou diversité : Enjeux et débats. Dans : Rachel Beaujolin-Bellet éd., *Les grands courants en gestion des ressources humaines* (pp. 236-251). Caen: EMS Editions. <https://doi.org/10.3917/ems.oiry.2021.01.0236>

Poster, W. R. (2018). Cybersecurity needs women. *Nature*, 555(7698), 577-580. <https://doi.org/10.1038/d41586-018-03327-w>

Potter, L. E., & Vickers, G. (2015). What Skills do you Need to Work in Cyber Security ? *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. <https://doi.org/10.1145/2751957.2751967>

Poupard, G. et Le Ster, N. (2020). *Panorama des métiers de la cybersécurité - Edition 2020*. https://www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk : Evidence from Cybersecurity Related Disclosure. *Journal of Business Ethics*, 177(2), 351-374. <https://doi.org/10.1007/s10551-020-04717-9>

Statista. (s. d.). *Cybersecurity - Worldwide | Statista market forecast*. <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

Schindelheim, R. (2018). IBM' s P-Tech program integrates high school and college coursework. *WorkingNation*. <https://workingnation.com/shaping-future-workforce-ibm-jen-crozier/>

Sussman, L. (2020). Exploring Non-Technical Knowledge, Skills, and Abilities (KSA) that may expand the expectations of the Expectations of the Cyber Workforce. *ResearchGate*. https://www.researchgate.net/publication/348352243_Exploring_Non-Technical_Knowledge_Skills_and_Abilities_KSA_that_May_Expand_the_Expectations_of_the_Cyber_Workforce

Tedongmo Teko H. et Bapes Ba Bapes Y. (2010), Influence sociale et leadership dans la direction des personnes , *SociologieS* [En ligne], <https://doi.org/10.4000/sociologies.3204>

Tessian. (2021). *The Futur is Cyber : Opportunity in Cybersecurity Report 2021*. https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian%20Research/%5BTessian%20Research%5D%20The%20Future%20is%20Cyber%20-%20Opportunity%20in%20Cybersecurity%20Report%202021.pdf?__hstc=&__hssc=&hsCtaTracking=aeff1e33-7b39-4d5a-acbb-1bad896768e8%7C2ab8dd11-0e8e-4d5a-95a9-c0400f15a21f

The Clayman Institute for Gender Research. (2017). Alignment with gender stereotypes predicts success in tech. *Stanford University*.
<https://gender.stanford.edu/news/alignment-gender-stereotypes-predicts-success-tech>

Vicomte, P. & Larroque, E. (2023). Où sont les femmes ?. *Servir*, 519, 65-67.
<https://www.cairn.info/revue--2023-1-page-65.htm>.

W. E. Forum, "The future of jobs report 2018," World Economic Forum, Geneva, Switzerland, 2018.

Weingarten, E., & Garcia, M. E. (2015). Decrypting the cybersecurity gender gap. *New America*.
<https://www.newamerica.org/cybersecurity-initiative/policy-papers/decrypting-the-cybersecurity-gender-gap/>

Wikipédia. (2023). *Fabricant d'équipement d'origine*. fr.wikipedia.org.
https://fr.wikipedia.org/wiki/Fabricant_d%27%C3%A9quipement_d%27origine

Wikipédia. (2021). *Intégrateur*. fr.wikipedia.org.
<https://fr.wikipedia.org/wiki/Int%C3%A9grateur#:~:text=Un%20int%C3%A9grateur%20d'infrastructure%20informatique,collabore%20avec%20l'administrateur%20r%C3%A9seau>.

Wikipédia. (2019). *Systémier*. fr.wikipedia.org.
<https://fr.wikipedia.org/wiki/Syst%C3%A9mier#:~:text=Le%20syst%C3%A9mier%20ou%20assembleur%20est,'automobile%20et%20l'informatique>.

Wirth B. (2019). Why bringing more women into the cybersecurity workforce is a matter of national security. *UNSW BusinessThink*.
<https://www.businessthink.unsw.edu.au/articles/Why-bringing-on-more-cyber-women-is-a-matter-of-national-security>