SOMMAIRE

PRÉFACE

Mariya Gabriel

Commissaire européenne à l'Économie et la Société numériques

Selon une étude réalisée par Arlington Research pour Kapersky Lab auprès de 4 000 jeunes de 16 à 21 ans, un tiers des adolescentes interrogées pensent que les professionnels de la cybersécurité sont des « garçons geeks ». 78% d'entre elles indiquent n'avoir jamais envisagé une carrière dans ce domaine.

Voilà un triste constat de comment les stéréotypes empêchent les jeunes femmes de rejoindre ce secteur dynamique et en plein essor. Donc, comment renverser la tendance ? Comment attirer plus de jeunes femmes ? La réponse doit être trouvée dans un ensemble de mesures, d'initiatives et d'acteurs.

Tout d'abord, il nous faut comprendre que la cybersécurité est l'affaire de tous. Les écoles ont un grand rôle à jouer, mais aussi les parents, les pouvoirs publics et les entreprises. Les enfants, filles et garçons, doivent être sensibilisés à la cybersécurité dès le plus jeune âge, afin de saisir les enjeux passionnants qui l'entourent.

Aujourd'hui, le numérique fait partie intégrante de notre vie. De la même manière dont nous sommes exposés à d'innombrables opportunités d'apprentissage et d'échanges, nous sommes exposés à des risques. Il est primordial que filles et garçons prennent conscience de ces dangers, afin de profiter au mieux du potentiel offert par le numérique.

L'absence des filles et des femmes dans le domaine de la cybersécurité ne peut pas être une fatalité ; il est de notre responsabilité de provoquer le changement.

Tout au long de mon mandat, j'ai activement promu le rôle des femmes dans le numérique et j'ai donné mon soutien personnel pour démystifier l'univers du cyber. Nous avons lancé des initiatives d'envergure euro-

péenne afin de promouvoir les formations dans le domaine du numérique auprès des jeunes et plus particulièrement des filles, depuis le plus jeune âge.

Ces activités visent à accroître la visibilité des modèles de référence féminins. Qu'il s'agisse de femmes « réelles » ou de personnages de fiction, il est essentiel de dresser un portrait équitable du rôle des femmes dans la société et dans le numérique. Il faut également sensibiliser les jeunes filles au fait que les emplois en cybersécurité couvrent des positions diverses, dynamiques et passionnantes.

Ainsi, je tiens à remercier le Cercle des Femmes de la Cybersécurité pour cette publication qui sert de guide et d'allié pour accompagner les jeunes femmes sur le chemin d'une profession fascinante dans le domaine de la cybersécurité.

INTRODUCTION

On dit que « les métiers de la cybersécurité sont très techniques »… que « la cyber est un métier de geek »… On dit aussi que la cybersécurité « n'est pas un métier pour les femmes »… En réponse à ces clichés, le Cercle des Femmes de la Cybersécurité propose un autre éclairage sur les métiers, les formations et les parcours professionnels dans la filière cybersécurité, filière dans laquelle les femmes ont toute leur place.

Une filière d'avenir

La cybersécurité est un domaine transverse, essentiel pour protéger le patrimoine numérique de l'individu, des organisations et de l'État. Son enjeu est stratégique, au carrefour de sujets d'actualité passionnants et indissociables de changement.

Ce livre s'adresse aux lycéen(ne)s et étudiant(e)s, aux parents, aux professionnels de la formation et de l'orientation, aux femmes en situation de reconversion… pour leur permettre de mesurer tout l'intérêt de la filière cybersécurité.
L'ouvrage se veut pragmatique pour démystifier le sujet, susciter l'intérêt et surfer dans l'univers de la cyber.

En moins de 5 ans, la digitalisation a changé la donne : l'Internet des objets, la mobilité, le cloud, l'Intelligence Artificielle, les GAFAM[1]… ont profondément restructuré le paysage technologique et économique. Certes, nous en voyons des bénéfices, mais, dans le même temps, ces bouleversements ont augmenté la vulnérabilité des systèmes, ouvert de nouvelles menaces, intensifié et sophistiqué celles existantes, fra-

[1] Google, Apple, Facebook, Amazon et Microsoft

gilisant ainsi les organisations. La montée exponentielle des cyber-attaques à tous niveaux, individuels ou collectifs, est un fait partagé ; l'actualité est riche à en juger par la cartographie des attaques en temps réel réalisée par Kaspersky[2].

Le besoin de compétences suit la montée en puissance des enjeux qui entourent la cybersécurité. Les créations d'emplois aussi. Mais l'offre est largement insuffisante pour couvrir ce besoin.

Une filière dynamique, mais… méconnue ou mal jugée

Les offres sont largement plus élevées que le nombre de candidats qui répondent. En dépit des formations proposées, des opportunités offertes et de rémunérations – très – attractives, la pénurie de compétences est là : rien qu'en France, les professionnels estimaient l'année dernière à 1000 le nombre de postes pourvus sur les 6 000 ouverts[3].

Méconnaissance des parcours, déficit de notoriété… les raisons du désamour sont multiples et concernent le numérique dans son ensemble. Malgré des millennials aux pratiques hyper connectées, parfois sources de menaces, la cybersécurité est mal connue : l'image du geek et de son éternel sweat à capuche colle à la peau de la cyber !

Il est vrai que certains emplois dans la cybersécurité exigent des compétences en informatique, en programmation ou en ingénierie de réseau. Mais la cyber ne se résume pas à la technique : sa force réside dans des démarches, des processus, des méthodes… Un grand nombre des emplois de la filière demandent plus de compétences humaines et organisationnelles que techniques : la capacité à travailler en équipe, l'aptitude en matière de communication et de leadership, une vision partagée des situations de crise sont des clés de succès des projets cyber.

---

[2] cybermap.kaspersky.com/fr

[3] Michel Van Den Berghe, Directeur Général Orange Cyberdefense. www.lemonde.fr/connaître-et-comprendre-les-metiers-de-demain/article/2018/01/19/expert-en-securite-informatique-ce-heros-qui-protege-les-entreprises_5244162_5240459.html

La cybersécurité est une filière dynamique avec un éventail de métiers techniques, juridiques ou organisationnels passionnants. C'est un domaine inspirant qui incite à la curiosité et induit une profonde satisfaction à servir autrui.

Ce livre est un plaidoyer en faveur des jobs et des parcours de formation possibles dans la cyber, dès la formation initiale et tout au long de la vie professionnelle. Il contient une foule d'informations et de références utiles pour guider les jeunes en phase de choix, les parents soucieux de l'avenir de leurs enfants, ainsi que les professionnels de l'orientation.

Ouvrir les métiers cyber aux femmes

Les femmes représentent à peine plus de 10% de la population du secteur[4]. Ce manque de mixité, conjugué à la pénurie générale de compétences, pose problème : comment faire face à la transformation digitale et à la montée des cybermenaces si plus de la moitié de la population ne s'y intéresse pas, est exclue ou s'auto exclut de la filière ? Les métiers de la cybersécurité doivent-ils rester un no(wo)man's land ? Non.

Peu guidées, pas assez informées, les femmes se détournent de la cyber. Plus globalement, sous le poids culturel des stéréotypes, les talents féminins désertent le numérique. La cybersécurité manque d'organisations en mesure de montrer leur volonté d'ouverture de ces métiers aux femmes.

[4] 11% selon Kaspersky Lab (2017) et l'étude (ISC)[2] de 2018
www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx

L'ouvrage témoigne de la variété des métiers exercés par les femmes de la cyber et présente des visages auxquels s'identifier ; il valorise des entreprises qui recrutent ou qui ouvrent les métiers de la cybersécurité aux femmes.
Il propose une boîte à outils pour alimenter un projet professionnel.

Avec plus de 200 adhérentes, le CEFCYS a pour vocation de promouvoir les métiers de la cybersécurité auprès des femmes et des jeunes filles souhaitant accéder, partager leur expérience ou se reconvertir dans le secteur. Pour ce livre, le CEFCYS a recueilli leurs témoignages et présente des visages féminins de la cybersécurité.

23 cyberwomen évoquent ainsi leur parcours, leurs convictions, leur métier sur des sujets variés comme la gestion de crise cyber, la blockchain et la cybersécurité, la sécurité de l'Internet des objets, le hacking éthique ou la cybersécurité dans l'industrie 4.0, la sensibilisation à la cybersécurité… La cyberwoman est auditrice, chercheuse, responsable sécurité, avocate, hackeuse, communicante, cheffe de projets, commerciale, cryptographe, entrepreneuse ou encore magistrate…

Les profils sont d'horizons, de secteurs et d'expériences divers. Certaines ont choisi les métiers de la sécurité dès leur formation initiale ou aspirent à y entrer ; d'autres les ont découverts au cours de leur vie professionnelle et ont élargi leurs compétences initiales. Les talents féminins de la cyber sont engagés, bien dans leur peau. Nous vous invitons à les découvrir.

Y a-t-il une façon « spécifiquement féminine » d'exercer le métier de la cybersécurité ? Le débat est ouvert, mais nous ne l'engageons pas dans cet ouvrage… Ce qui est certain, ainsi que le souligne le cogniticien Émile Servan-Schreiber dans son ouvrage *Supercollectif. La*

nouvelle puissance de nos intelligences[5], c'est que la mixité et les visions complémentaires concourent au succès des projets. En situation de crise, les équipes mixtes fournissent davantage de créativité et d'innovation. La mixité est un enjeu majeur dans toutes les organisations.

Les métiers de la cyber font partie de ces milliers d'emplois « nouveaux » que les femmes, et de façon plus large les jeunes diplômé.es, doivent investir dès à présent.

Ce livre interpelle aussi les organisations, les instances économiques et sociales : ensemble, faisons bouger les lignes de la mixité !

Nacira Salvan
Fondatrice et Présidente du CEFCYS

[5] Émile Servan-Schreiber est spécialiste de l'intelligence collective et des marchés prédictifs, Docteur en Psychologie Cognitive et auteur de *Supercollectif. La nouvelle puissance de nos intelligences*, Fayard, 2018.

- Chapitre 1 -
Cybersécurité, la filière qui recrute

DES MILLIERS DE PLACES À PRENDRE

La cybersécurité est une filière d'avenir dans le monde entier : il manque déjà près de 3 millions de professionnels dans le monde, dont 142 000 en Europe. Ce déficit devrait atteindre les 350 000 postes en 2022[6]. En France, l'Observatoire Paritaire des métiers de l'Informatique de l'Ingénierie des Études et du Conseil (OPIIEC), les métiers de la cybersécurité représentent actuellement 24 000 emplois. Le chiffre augmente de façon constante, car la filière cybersécurité est directement liée à la transformation numérique de la société.

Une filière en plein essor… et ce n'est qu'un début

La cybersécurité présente la particularité d'être un domaine transverse, comme l'environnement, le droit ou l'Intelligence Artificielle. Santé, banque, finance, commerce, collectivités… tous les secteurs sont concernés. Tous les niveaux de la société française sont impactés : l'individu, les organisations publiques ou privées, l'État et ses institutions.

La transformation numérique se traduit par l'explosion de l'Internet des objets dans un monde connecté accessible en mobilité via smartphones, tablettes…, la dématérialisation massive vers le cloud, ou encore par l'accumulation des données dans le Big Data, en passant par l'Intelligence Artificielle ou le machine learning… Cette révolution digitale a pour contreparties des dérives comme le vol de données, l'interruption de service, les cyber escroqueries ou l'espionnage politique et économique. Les cyberattaques gagnent du terrain et deviennent l'activité criminelle qui connaît la plus forte croissance au monde.

La cybercriminalité est l'un des plus grands défis auquel sont confrontées les entreprises aujourd'hui. Toutes les organisations doivent faire face à des enjeux inédits et déployer de nouvelles protections.

[6] Étude (ISC)[2] de 2018

Face à des cyberpirates organisés, dotés de méthodes sophistiquées et déterminés par l'appât des gains, la cybersécurité est devenue un enjeu stratégique.

À l'horizon de 3 ans, les études anticipent en France une croissance de 6% des effectifs en cybersécurité, qui atteindra les 8% d'ici 5 ans.

- COMPRENDRE -

3 RAISONS POUR LESQUELLES LES EMPLOIS DANS LA CYBER VONT CONTINUER D'AUGMENTER

L'évolution des usages avec la multiplication des plateformes numériques
Internet des objets, blockchain, Intelligence Artificielle, big data, cloud… la digitalisation portée par ces technologies impacte tous les secteurs de la société.

L'augmentation des attaques cybersécurité et leur médiatisation
Phishing, fraude au président, ransomware, chantage, vols de données sensibles, espionnage… Selon des études récentes[7] les cyberattaques deviennent un risque majeur pour les entreprises :
• moins d'une entreprise sur deux se sent capable de gérer une cyberattaque de grande ampleur ;
• 54% des incidents cyber proviennent d'employés actuels ou passés ;
• 80% des entreprises françaises ont constaté au moins une cyberattaque au cours des 12 derniers mois.
En conséquence, leurs dépenses en cybersécurité augmentent.

Les nouvelles réglementations
Les réglementations nationales et européennes se font plus pressantes pour protéger les citoyens, sécuriser les installations, garantir la confidentialité des données personnelles, sécuriser les paiements… Dans les organisations, le renforcement de la sécurité se traduit par des mesures de formation et de sensibilisation des employés (56%), la nomination de nouveaux responsables (35%), une nouvelle politique de gestion des accès (31%) et le chiffrement des données (16%)[8].

[7] Pwc, Cesin, ITSocial, FireEye, Deloitte
[8] Étude Deloitte, « Les 5 tendances dans la cybersécurité identifiées », 2018 www2.deloitte.com/fr/fr/pages/presse/2018/grandes-tendances-cybersecurite.html

Des métiers récents… ou qui n'existent pas encore !

De façon globale, plus de 80% des métiers de demain viendraient du digital. Les besoins dans la filière cyber vont dans ce sens et s'accroîtront en raison de l'émergence des nouvelles technologies, du renforcement des réglementations et de l'augmentation des cybermenaces. La cybersécurité créée de nouveaux métiers et bouleverse ceux existants.

Les emplois sont créés tant dans les entreprises privées que publiques, mais aussi des collectivités territoriales et des institutions ; il s'agit :

– d'emplois déjà identifiés : 18 métiers cyber sont recensés par l'OPIIEC tels que développeur, auditeur, architecte, pentesteur, analyste SOC… Les métiers dits « de gouvernance » correspondent souvent à de nouvelles fonctions telles que délégué à la protection des données ou data security manager ;

– d'emplois associant des compétences cybersécurité à d'autres métiers comme ceux du juridique, du commerce, de la santé, du marketing… Quelle que soit la formation initiale, une spécialisation cybersécurité sera utile dans un parcours professionnel ;

– des emplois « à venir », dont les contours sont encore non identifiés, car liés à des technologies ou à des usages récents (informatique quantique, voitures connectées, Intelligence Artificielle…) ou encore inconnus !

Un(e) étudiant(e) accédera peut-être, au terme de 4 à 5 ans d'études, à un emploi « non identifié » au début de sa formation !

DES IDÉES REÇUES SUR LES JOBS DE LA CYBERSÉCURITÉ

Au cours de ses actions de sensibilisation et d'information dans les écoles, les lycées ou même en entreprise, le CEFCYS relève régu-

lièrement des clichés qui font obstacle aux vocations vers la filière cyber. Voici les 5 idées reçues auxquelles les enseignants, professionnels de l'orientation, parents et étudiants doivent faire face.

Les métiers de la filière cyber sont réservés aux ingénieurs

PARTIELLEMENT FAUX. Les métiers de la filière cyber offrent des possibilités à partir d'un bac+2 et à des salariés qui souhaitent faire évoluer leur parcours professionnel. Beaucoup d'organisations privilégient des compétences déjà acquises telles que la conduite de projet, l'administration de réseaux, le juridique, le commerce… et forment ensuite aux compétences complémentaires nécessaires.

Une formation initiale juridique prouve que vous disposez d'un sens logique et de l'habitude des méthodes. Une expérience dans l'administration des ventes ou dans la hot line clients prouve que vous savez traiter des sujets complexes et souvent dans l'urgence. Évoluer de la Supply Chain vers un poste dans la sécurité informatique : c'est possible car les compétences d'organisation dans l'urgence et de respect des délais sont clés dans la cyber. *(voir le témoignage d'Aline Barthélémy, chapitre 2)*

Les métiers de la filière cyber sont réservés aux jeunes diplômé(e)s

FAUX. Certes, les jeunes diplômés sont sollicités avant même la fin de leurs études… Toutefois, si vous avez déjà entamé votre cursus ou même votre carrière professionnelle, rien n'est perdu ! De nombreuses solutions existent pour permettre à un professionnel de réorienter son parcours dans ce secteur ou d'ajouter une compétence cyber à son métier. Diplôme, titre, certification, MOOC… les formations peuvent varier de quelques jours à plusieurs mois dans le cadre de la formation continue ou à titre personnel.

Diplômé(e) ou autodidacte, la cybersécurité ouvre grandes ses portes aux talents motivés. *(voir les témoignages de Natacha Bakir et d'Odile Huchet, chapitre 2)*

Les entreprises de la filière cyber sont uniquement des grandes entreprises

ENCORE FAUX. La cybersécurité est un enjeu majeur pour toutes les organisations, qu'il s'agisse des entreprises ou des institutions. Les jobs concernent toutes les dimensions d'entreprises, de la start-up à la multinationale.

Les grandes entreprises disposent de ressources leur permettant de déployer des protections.

PME, PMI, TPE prennent actuellement mesure de l'importance de sécuriser leur système d'information. De récentes attaques illustrent une nouvelle tendance des cyberattaquants : passer par les sous-traitants et remonter la Supply Chain pour atteindre les grandes entreprises. Une étude récente[9] affirme que 66% des PME ont été attaquées au cours des 12 derniers mois, augmentant le risque d'infection de l'ensemble de leur Supply Chain.

Les métiers de la filière cyber sont pour les geeks

TOUJOURS FAUX. Le cliché circule partout et détourne de nombreux(euses) candidat(e)s d'une orientation vers cette filière. En fait, les compétences transversales « humaines » jouent un rôle important dans les projets de cybersécurité pour former, anticiper les risques, travailler avec les autres métiers de l'entreprise. Beaucoup d'organisations privilégient des profils de candidats présentant des savoir-faire dans la conduite de projet, l'administration réseau, plus généralement l'IT… et forment ensuite aux compétences complémentaires nécessaires.

De plus de nombreux métiers (juridique, web marketing, commerce…) ajoutent une facette cyber à leur compétence initiale.

[9] Étude Ponemon Institute, octobre 2019