GOUVERNEMENT
Liberté
Égalité
Fraternité

« FORMATION, EMPLOIS ET COMPÉTENCES DE LA FILIÈRE CYBERSÉCURITÉ DU GRAND NANCY »

DIAGNOSTIC PROSPECTIF & PARTICIPATIF

SYNTHESE

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

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

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

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

DIAGNOSTIC DE FORMATION
31 mai 2023

Interne

Préambule

FORE-CY, diagnostic prospectif et participatif « Formation, Emplois et compétences de la filière cybersécurité du Grand Nancy » a été réalisé par un consortium d'acteurs composé de :

- La **Maison de l'Emploi du Grand Nancy**,
- **Numeum**, organisation professionnelle nationale de l'écosystème numérique,
- **CESI** Ecole d'ingénieurs,
- Le cluster **Nancy Numérique**.

L'animation de la démarche a été portée par la Maison de l'Emploi du Grand Nancy, chef de file du projet, en réponse à l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » du programme France 2030. La mise en œuvre opérationnelle de FORE-CY a été confiée à **Randea,** bureau d'étude et cabinet de conseil spécialisé en accompagnement des transitions de filière et prospective territoriale.

Fidèle aux méthodes participatives d'implication des parties prenantes au diagnostic et à la préparation de l'avenir, la mission a mobilisé **un comité de pilotage étendu aux parties prenantes**, lors de trois séminaires de travail en décembre 2022, avril et mai 2023 :

Note : sont présentés ici les partenaires impliqués dans la conduite de la mission ; il ne s'agit pas d'une cartographie de la filière Cybersécurité du Grand Nancy

Les auteurs tiennent à **remercier l'ensemble des membres impliqués** dans le Comité Technique du Consortium, les parties prenantes locales et régionales mobilisées (entretiens, séminaires), **les interlocuteurs nationaux de l'AMI** « Compétences et Métiers d'Avenir » et de Numeum ainsi que les **organismes de formation et entreprises** ayant répondu aux deux enquêtes menées sur le territoire en appui du présent diagnostic.

FORE-CY : les forces du Grand Nancy s'unissent pour anticiper les besoins en cybersécurité et former les professionnels de demain

La cybersécurité, domaine stratégique touchant aux conditions mêmes de notre souveraineté et de notre intégrité tant économique que démocratique, est un levier de résilience territoriale pour ceux qui en relèvent les défis, une vulnérabilité sinon. La cybersécurité constitue l'une des **spécialisations fortes du territoire grand-nancéien** avec trois secteurs économiques exprimant d'importants besoins de compétences en ce domaine (finance, secteur public/services administrés, filière santé et biotechnologies).

Malgré ces atouts indéniables, **la filière cybersécurité connaît une pénurie de candidats disponibles sur le marché du travail.** L'ouverture à des profils plus diversifiés (féminisation, âge, parcours professionnels atypiques) constitue un levier à explorer par les employeurs ; l'identification des leviers de facilitation de ces trajectoires doit encourager ce type de dynamique.

Au travers d'une **méthodologie compréhensive et associant l'ensemble des parties prenantes de l'écosystème** Cyber du territoire, FORE-CY interroge quatre enjeux-clés pour le Grand Nancy :

STRUCTURATION : Qui sont les employeurs de l'écosystème cybersécurité du Grand Nancy ? Comment sont-ils organisés localement ? Quelles sont les interactions entre employeurs de l'écosystème cybersécurité et organismes de formation ?

FORMATION : Quelle offre locale de formation à la fois pour les spécialistes informatiques et les autres profils de la cybersécurité ? Comment pourrait-elle mieux répondre aux besoins territoriaux directs et indirects en cybersécurité, à l'échelle de la Région Grand Est ?

DIVERSITE ET INCLUSION : Comment rendre plus inclusifs les parcours d'accès à l'emploi et à la formation dans la filière (mixité professionnelle, intégration de profils jugés « atypiques ») ? Comment mieux accompagner les projets de reconversion professionnelle dans la filière cybersécurité ?

ANTICIPATION : Quelles perspectives de développement de la filière (marchés à consolider et à conquérir, métiers et technologies en émergence…) ? Quels seront les besoins des employeurs en termes de recrutement (métiers, compétences, spécialités) à l'horizon 2030 ?

Démarche méthodologique générale

Le diagnostic prospectif et participatif repose sur quatre « briques » méthodologiques complémentaires permettant de disposer d'un état des lieux robuste :

1. L'étude des besoins actuels en compétences de l'écosystème cybersécurité
2. Une cartographie et diagnostic de l'offre de formation en cybersécurité
3. Une monographie des parcours de reconversion vers les métiers de la cybersécurité
4. Un diagnostic prospectif territorial

Une démarche de préparation de l'avenir résolument participative

Initié en décembre 2022 et pendant 6 mois, le diagnostic FORE-CY s'appuie sur la mobilisation de l'ensemble de l'écosystème cybersécurité et sur l'implication de nombreux partenaires institutionnels et économiques :

- Les employeurs et leurs représentants ;
- Les organismes de formation ;
- Le monde de la recherche ;
- Les acteurs publics et les prescripteurs.

Le diagnostic débouche sur un macro-plan d'actions, co-construit avec les parties prenantes.

Partie I. Étude des besoins en compétences de la filière cybersécurité du Grand Nancy

Périmètre des métiers et compétences de la cybersécurité : une vision « chaîne de valeur » résolument pluridisciplinaire

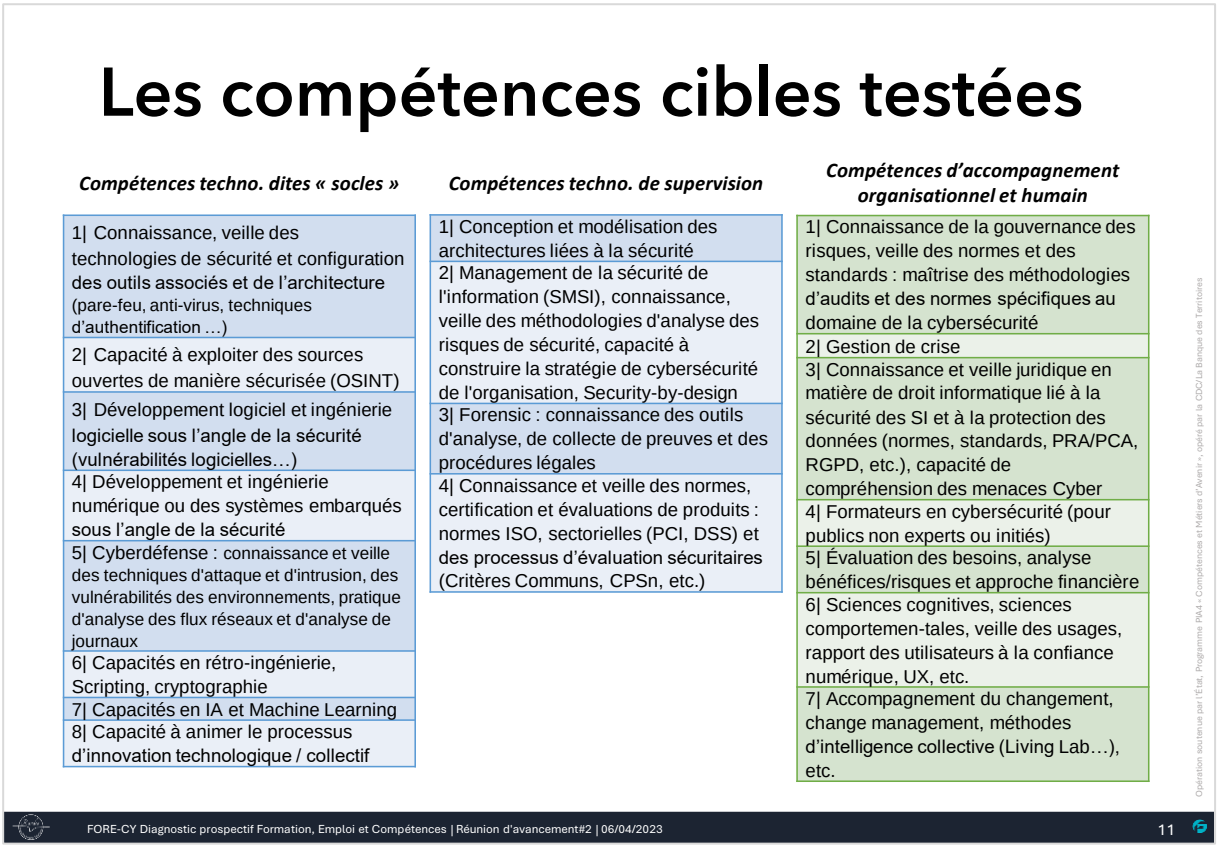
Le projet FORE-CY a retenu une typologie des domaines de compétences liés à la cybersécurité en 5 champs :

- Champ 1 : la maîtrise des **technologies de sécurisation/protection** des systèmes d'information, réseaux, logiciels, applications ou systèmes embarqués ;
- Champ 2 : la maîtrise des **technologies et approches de détection et de gestion des incidents de cybercriminalité et la cyberdéfense** active ;
- Champ 3 : la connaissance des **normes et standards** ; la capacité à évaluer **risques et besoins** ; les enjeux de **conformité** en matière de vie privée et droits en ligne (PRA/PCA, RGPD, etc.) ; la connaissance du **droit appliqué à l'informatique** et à la **réglementation en matière numérique et Cyber** (y compris dans les aspects droit des contrats, recherche en responsabilité juridique, gestion des événements judiciaires) ;
- Champ 4 : **l'accompagnement de l'organisation** (gouvernance, procédure de gestion des risques et de crise…) et des **facteurs humains** (confiance numérique utilisateurs, usages de la Cyber, transformation, changement etc.) ;
- Champ 5 : **la sensibilisation et la formation** (socle ou spécialisée) à la cybersécurité.

Résultat-clé : FORE-CY observe **une triple polarisation des métiers de la filière Cybersécurité :** (i) technologique, (ii) juridique et (iii) d'accompagnement organisationnel et humain.

Au-delà de l'indispensable réflexion sur le périmètre des métiers à considérer, le projet FORE-CY a souhaité approfondir de manière fine les besoins en compétences des entreprises prestataires de service Cyber ou disposant d'un service Cyber interne. **19 compétences recomposées** du référentiel ANSSI ont été retenues comme des compétences cibles :

- 8 **compétences technologiques socles** (cf. première colonne ci-dessous) ;
- 4 compétences dites de **supervision** (cf. deuxième colonne ci-dessous) ;
- 7 compétences davantage liées à l'**accompagnement** organisationnel ou humain (cf. troisième colonne ci-dessous).



Les besoins en compétences des employeurs Cyber : une approche fine novatrice pour la filière

L'enquête a permis d'identifier **les compétences sur lesquelles les entreprises ont d'ores et déjà investi** et pour lesquelles elles disposent de collaborateurs pour répondre à tout ou partie de leurs besoins en ce domaine :

- **Les compétences juridiques :** près de 40% des entreprises de l'écosystème Cyber local en disposent, **signe de leur caractère structurant** ;
- Les capacités d'**évaluation des besoins clients** (analyse bénéfices/risques et évaluation financière) pour un tiers des employeurs, ainsi que les capacités de **gestion des risques** (30% des employeurs) ;
- Les **technologies de sécurité** pour 30% également de l'écosystème.

Ce « palmarès » des compétences les plus disponibles au sein de l'écosystème local traduit d'une part le **positionnement de l'écosystème au sein de la chaîne valeur**, centré pour un grand nombre d'acteurs sur le déploiement d'outils et de technologies de sécurisation développés par d'autres, et confirme d'autre part **l'importance de la problématique de l'accompagnement client** évoquée dans le diagnostic stratégique amont **et surtout l'importance de la maîtrise des enjeux juridiques liés à la cybersécurité.**

A l'inverse, trois compétences tranchent par leur criticité au sein de l'écosystème Cyber et **appellent à être renforcées au vu des besoins exprimés.** Il s'agit en premier lieu de :

- **l'IA et le Machine Learning :** seules 4% des entreprises du territoire disposent de compétences en ce domaine alors que 2/3 des entreprises estiment avoir besoin de ces profils, soit un taux de couverture de 6%, particulièrement faible ;
- **le scripting et la cryptographie :** avec là aussi 4% d'entreprises disposant de compétences en ce domaine pour 1/3 d'entreprises estimant partager ce besoin, soit un taux de couverture de 11% ; l'avènement de l'aire de l'IA pourrait apporter une réponse rapide aux besoins de scripting, déjà assez bien maîtrisés par certaines IA, ce qui renforce encore les besoins en compétences en IA/ML ;

Interne

- **les sciences cognitives et comportementales, les compétences en usages, confiance numérique utilisateurs, UX,** etc. : en ce domaine également, seules 4% d'entreprises Cyber locales estiment disposer de ces compétences alors qu'elles sont 40% à en exprimer le besoin, soit un taux de couverture de 11%.

Résultats-clés : Le diagnostic des compétences met en avant **la centralité des compétences juridiques** comme l'une des trois composantes des besoins en compétence Cyber avec les expertises technologiques et les expertises en gestion des risques. Il pointe **la criticité** des besoins locaux en **IA/ML**, scripting/**cryptographie**, **approches cognitives et comportementales** appliqués à la cybersécurité vis-à-vis desquels un effort doit être réalisé par les organismes de formation et les employeurs afin de s'assurer de disposer des compétences-clés de court et aussi moyen terme.

Après s'être focalisés pour un grand nombre d'entre eux sur le déploiement d'outils et solutions technologiques, les employeurs de l'écosystème local expriment leur intention ou a minima leur compréhension qu'ils gagneraient à **se renforcer également dans les compétences d'avenir** que sont l'IA et le *Machine Learning*, la **cyberprotection** (techniques d'attaque et intrusion, vulnérabilités des environnements, analyse des flux réseaux et de journaux), la maîtrise des **normes et certifications**, la **gouvernance et la gestion des risques**. Les compétences en conception et modélisation des **architectures** liées à la sécurité et en **systèmes de management** de la sécurité des informations sont également essentielles.

Les intentions de recrutement et de formation des employeurs Cyber

Selon l'enquête Employeurs FORE-CY, les compétences dans lesquelles un nombre élevé d'entreprises envisage de recruter sont, par ordre décroissant :

Top 1. **La cyberdéfense & la sécurité et ingénierie logicielle** (28% d'employeurs ayant une intention de recrutement) ;
Top 2. **Les technologies de sécurisation socles** (pare-feu, anti-virus, techniques d'authentification ... 24% d'intentions de recrutement)
Top 3. **La conception et la modélisation des architectures liées à la sécurité, l'IA/ML et les formateurs** (16% à 17% d'intentions de recrutement)
Quant aux projets de formation des employeurs, les domaines visés sont par ordre décroissant :

Top 1. **La cyberdéfense & l'IA/ML** (40% d'employeurs ayant une intention de formation) ;
Top 2. **Les technologies de sécurisation socles** (pare-feu, anti-virus, techniques d'authentification... soit 32% d'intentions de formation)
Top 3. **La gouvernance et la gestion des risques** (audit) (30% d'intentions de formation).

Par ailleurs, deux difficultés RH tranchent par leur intensité : **la féminisation et les difficultés de recrutement invoquées par un employeur sur deux.** Le déficit de candidates touche de façon exacerbée les profils de techniciens ; il s'est accentué depuis la réforme du baccalauréat qui a eu pour incidence indirecte de réduire la proportion de filles poursuivant une spécialité « mathématiques » et s'orientant vers les profils scientifiques techniques.

L'analyse du marché du travail local en cybersécurité

Sur le marché du travail, entre 2018 et 2022, on constate **un phénomène très net de concentration des offres d'emploi publiées sur les profils d'ingénieurs ou cadres** d'étude, de recherche et développement en informatique ou chefs de projets informatiques passés de 19% des offres à 34%, avec un quasi doublement des offres d'emploi durables relatives à ce profil de qualification. La part des offres d'emploi de niveau techniciens informatiques a en revanche fortement baissé en quatre ans, passant de 51% à 36%, là où celle des opérateurs progresse en structure, comme en volume (+4 points, soit +27% en quatre ans).

En zoomant sur les trois métiers les plus en proximité avec les profils Cyber, à savoir l'expertise et le support en systèmes d'information, la production et l'exploitation de systèmes d'information ainsi que les études et le développement informatique, **les tensions relatives aux métiers des SI apparaissent au grand jour.** À l'échelle

du Grand Nancy, comme du Grand Est et de la France entière, les offres d'emploi durables sont supérieures ou d'un ordre de grandeur proche du nombre de demandes d'emploi dans le domaine. Le vivier est ainsi insuffisant pour répondre aux besoins des employeurs.

Résultat-clé : Les cycles de formation doivent prendre en compte une troisième dimension en plus de la maîtrise d'une expertise technique (qu'elle soit technologique, juridique, en gouvernance et gestion des risques, en accompagnement des facteurs humains…) et des savoir-être fondamentaux clés (travail en équipe et en organisation formelle, adaptabilité face aux contraintes et besoins clients…) :

- **les aptitudes et appétences attitudinales** permettant d'établir et d'entretenir son expertise et son apport de valeur que sont dans la Cyber : la **curiosité**, la capacité à faire de la **veille** et la **pédagogie** avec des non experts.

Ces trois domaines complémentaires et distincts constituent autant de forces pour les collaborateurs et la filière cybersécurité toute entière.

Point-clé : les représentations des aptitudes nécessaires aux métiers de la cybersécurité restent en dissonance avec les besoins exprimés par les entreprises quant aux *soft skills* : la curiosité, la créativité, l'appétence pour la veille et la pédagogie envers les non-experts sont des compétences clés et porteuses dans un parcours professionnels en cybersécurité insuffisamment perçues par les candidats au métier, en complément d'une indispensable maîtrise technique (technologique, juridique, en gouvernance et gestion des risques ou facteurs humains).

Partie II. État des lieux de l'offre de formations

Corollaire de l'étude des besoins en emplois et compétences des employeurs de profils Cyber, l'état des lieux de l'offre de formation en cybersécurité est une composante structurante du diagnostic local : les organismes de formation initiale et continue sont en effet, des acteurs essentiels pour la constitution d'un vivier de talents adapté, en nombre et compétences, aux besoins des entreprises.

Le diagnostic FORE-CY s'est intéressé à deux champs complémentaires de formations, en procédant à un recensement cartographique des offres locales et régionales Grand Est, des formations suivantes :

- les **formations permettant d'accéder aux métiers spécialisés en cybersécurité à dominante technologique :** il s'agit de formations initiales du Bac Professionnel au Doctorat, mais aussi de formations professionnelles ou de reconversion ;
- les formations incluant des modules de compétences ou de connaissances de la cybersécurité **intégrés à des parcours ayant une autre dominante de spécialité** qu'il s'agisse de formations initiales ou de modules de formations professionnelles.

L'approche cartographique a été complétée par une enquête dédiée auprès des organismes de formations identifiés. L'objectif était de recueillir des éléments sur l'attractivité des formations et les difficultés rencontrées, les voies et moyens mis en œuvre pour répondre aux besoins des employeurs de profils Cyber, la vision partagée de l'évolution des métiers de la cybersécurité et les défis à relever pour les organismes de formation de ces domaines. La vision des organismes de formation a également été **mise en perspective avec les réponses des employeurs de profils** Cyber quant à leur capillarité avec l'écosystème de formation et leurs attentes.

L'offre de formation en cybersécurité de la Région Grand Est : caractéristiques principales des 211 formations identifiées

La cartographie des formations réalisée recense **au sein de la Région Grand Est, un total de 211 formations** relevant du domaine de la cybersécurité. Un certain nombre de formations non spécialisées correspondent à des

modules de connaissance ou de compétences en cybersécurité et peuvent même être des modules dits d'« hygiène numérique ».

La cartographie recense **96 diplômes de l'Enseignement supérieur ayant un marquant Cyber** de niveaux Bac+2 à Bac+5 :

- 31 **BTS** ;
- 14 **Bachelor,** 10 **Licences** professionnelles, 2 Licences et 2 **DU**, soit 30 formations de niveau 6 ;
- 19 **Master** et 3 Mastères spécialisés ;
- 15 diplômes d'**Ingénieur**.

Parallèlement, **39 formations professionnelles certifiantes** donnent accès à des compétences en cybersécurité sous la forme de :

- 22 **titres professionnels** (8 de niveau 5, 9 de niveau 6 et 3 de niveau 7) ;
- 17 **certificats professionnels** (dont 4 formations longues et 13 formations courtes).

Enfin, **76** formations courtes délivrent une attestation de formation en lien avec la cybersécurité sans être ni diplômantes, ni certifiantes.

Une grande variété de formations en cybersécurité : courtes et longues, à tous niveaux de qualification

Parmi les 211 formations identifiées, **40% sont des formations courtes** (de moins de 200h), près de **60% sont des formations longues de plus de 200h. Sans surprise, les formations sont pour la plupart à dominante informatique.** L'ensemble des organismes ou composantes proposent des formations en lien avec le domaine de l'informatique appliquée à l'administration, à la supervision et à la sécurisation des réseaux informatiques.

La cartographie met en évidence **seulement 6 formations qui ne sont pas positionnées sur des métiers technologiques.** En effet, l'Université de Lorraine, de Strasbourg et Troyes font montre de la volonté de **développer une forme de transversalité dans les enseignements « cybersécurité »** en déployant des modules dans quelques formations des Sciences humaines et sociales et du Droit.

Degré de spécialisation en cybersécurité

En matière de spécialisation, **les termes « Cybersécurité » ou « Sécurité informatique » apparaissent dans l'intitulé de près de 40 % des formations longues, soit 47 diplômes, titres professionnels ou certifications professionnelles** ; 60% des formations sont non spécialisées tout en incluant des modules Cyber.

L'écosystème de formation en cybersécurité du Grand Est

Les 211 formations Cyber sont dispensées par **48 organismes de formation publics ou privés, divers en termes de structure, mobilisant 70 composantes.** Le recensement a ainsi dénombré :

- 23 lycées ou établissements du second degré (LEGT ou LPO) ;
- 11 établissements de l'Enseignement supérieur et de la Recherche mobilisant 30 composantes ;
- 13 organismes spécialisés dans la formation professionnelle ;
- 1 organisme non spécialisé mais porteur d'une offre de formation.

Le retour d'expérience des organismes de formation du domaine

L'exploitation des réponses des organismes de formation à l'enquête semble indiquer que **les formations Cyber jouissent d'un bon niveau d'attractivité, tant dans les parcours Tech que juridiques ou d'accompagnement de**

l'organisation. Ainsi, 42% des établissements ne peuvent satisfaire l'ensemble des candidats sollicitant leur formation technologique en cybersécurité.

La capillarité entre l'écosystème de formation et les employeurs de profils Cyber est satisfaisante. Les employeurs de profils Cyber nourrissent par ailleurs entre eux **de fortes interactions**, notamment dans le domaine technique.

Le volet « Formation » du diagnostic FORE-CY confirme cinq grands défis pour le domaine :

- La féminisation du vivier, gageure aujourd'hui comme à moyen terme ;
- L'attention insuffisante portée aux profils issus de la reconversion ;
- Le défi de la formation des formateurs ;
- L'hybridation des parcours : un virage à réussir ;
- La constitution de parcours pluriannuels favorisant un haut niveau d'acquisition de compétences.

Partie III - Monographie des parcours de reconversion vers la cybersécurité : élargir le vivier et favoriser des parcours plus inclusifs

En proposant un focus sur 12 parcours de reconversion professionnelle, la monographie réalisée dans le cadre du projet FORE-CY s'attache à identifier les compétences d'appui à l'œuvre et les difficultés ressenties, levées ou non, susceptibles de constituer autant de points de blocage à prendre en considération dans ces parcours spécifiques afin de les faciliter.

Résultats-clés : Le choix du domaine de reconversion est un élément structurant du projet de reconversion. Il s'élabore dans le temps à la croisée des mondes personnels, interpersonnels et professionnels. Quatre lignes de forces complémentaires ont pu être mises en évidence que les candidats à la reconversion gagneront à expliciter sous la forme d'une grille d'aide à la décision :

- **l'appérence et les goûts personnels** permettant d'ancrer son projet en soi-même et dans sa biographie ;
- **la capacité à la projection de soi dans un métier donné en s'inspirant des exemples de l'entourage ou en capitalisant sur son parcours professionnel** dans le cas d'une reconversion sans changement de domaine professionnel ;
- **la capacité à dépasser les idées reçues** notamment celle selon laquelle l'informatique est un domaine inaccessible ;
- **l'indispensable pragmatisme vis-à-vis du marché de l'emploi, des facilités ou difficultés d'embauche, ou encore de l'accessibilité de l'offre de formation et de son adéquation au candidat.**

Hormis quelques personnes ayant réalisé leurs recherches en toute autonomie, en contactant directement des organismes de formation, la plupart des candidats à la reconversion se sont rapprochés de structures d'accompagnement (Pôle Emploi, Transition Pro (ex-FONGECIF), la Mission Locale…). Pour les personnes dont l'expérience professionnelle précédente n'a pas de lien avec la cybersécurité, le passage par une formation est un indispensable pour « obtenir des compétences ». Ces compétences très techniques et spécifiques ne pouvant pas, selon eux, être exclusivement obtenues par l'auto-formation. La formation est alors le marqueur du « démarrage » du parcours de reconversion.

Ainsi, qu'il s'agisse d'une démarche de reconversion ou de transition professionnelle, la formation s'ancre comme un passage structurant et pour le moins essentiel dans les parcours de reconversion. L'engagement dans les cursus formatifs des personnes en reconversion diffère pourtant de celui des étudiants en formation initiale : davantage de pression, la peur de l'échec, les sacrifices à consentir.

La technicité attendue, ou supposée, dans les métiers du champ de la cybersécurité est également susceptible de créer des craintes supplémentaires, faisant naître un sentiment d'illégitimité en dépit de profils finalement adaptés aux attentes du métier et à l'aise dans le processus d'apprentissage.

Partie IV. Prospective territoriale

Le diagnostic prospectif territorial constitue le quatrième volet de l'étude. Il prolonge le tableau statistique et l'analyse des besoins en compétences des employeurs de profils Cyber par un cadrage des perspectives en emplois du secteur, à l'horizon 2030. Ce cadrage repose sur quatre scénarios prospectifs :

Scénario A. 2030 | Vers un territoire de confiance et de résilience numériques
La Métropole du Grand Nancy s'est mobilisée de façon prioritaire sur le sujet de la résilience numérique : agissant par plans d'action de filière animés et suivis par un référent Cyber, orientant les budgets disponibles pour soutenir le renforcement Cyber des services et établissements publics du territoire et procédant par allègement de la fiscalité locale pour motiver les entreprises à solliciter les prestataires locaux. Dans ce scénario de mobilisation générale, les ESN connaissent un pic de demande et la terre fertile nancéienne voit s'implanter et se développer sur son territoire des acteurs nombreux et en forte croissance de leurs effectifs. Les acteurs de la formation du domaine se mobilisent eux aussi et parviennent à fournir en nombre et qualité les talents dont les entreprises ont besoin.

Scénario B. Scénario fil de l'eau : « Pourvu que l'orage tombe plus loin… »
Les entreprises et administrations du Grand Nancy sont nombreuses à remettre à demain le « dossier cybersécurité ». Seules les plus structurées, soucieuses de l'efficacité de leur plan de continuité d'activité en cas de crise, effectuent un diagnostic de risques Cyber et prennent les premières actions de renforcement qui s'imposent, sollicitant les entreprises prestataires du territoire, très mobilisées. Dans ce scénario, les acteurs locaux poursuivent une croissance relativement modérée de leurs effectifs. L'entrepreneuriat progresse à la marge. Le marché est structurellement orienté à la hausse.

Scénario C. L'IA, une révolution, de nouveaux risques à accompagner
Les ETI et les services publics renforcent leurs services de Cybersécurité internes, afin de pour répondre de manière appropriée à l'explosion des menaces induites par l'IA et le Machine Learning. Les équipes sont mises sous forte pression, malgré les mesures d'aguerrissement et l'adaptation des postes, les démissions se multiplient. L'outil de formation est fortement sollicité pour fournir en nombre et en qualité les talents dont les entreprises ont besoin : la situation est sous haute tension. Les acteurs de pointe s'implantent et se développent sur le territoire métropolitain avec une stratégie mixte de croissance modérée de leurs effectifs et de recours à la cotraitance.

Scénario D. L'IA, révolution et rupture pour la Cyber, « l'effet pointe de diamant »
La révolution de l'IA bat son plein… si les menaces numériques explosent, l'IA est mobilisée au sein même des solutions de cybersécurité et impacte fortement le domaine lui-même. Les emplois de premier niveau se font rares, le niveau de qualification moyen continue de se concentrer sur les pointes de diamant des Bac +6 et docteurs. Certains start-uppeurs continuent de tirer leur épingle du jeu avec un parcours atypique, sans lien aucun avec l'informatique ou la gouvernance des risques, mais rares sont les élus.

Sous ces hypothèses, à l'horizon 2030, les effectifs de profils Cyber du Grand Nancy pourraient connaître une croissance de 40% à 175%, soit une croissance annuelle moyenne de +5% dans le cas du scénario D simulant une chute des emplois de techniciens dans la Cyber sous le coup de l'IA, à +15% dans le scénario A de mobilisation générale.

Attentes et perspectives d'avenir pour les organismes de formation

Interrogés sur l'école de la cybersécurité de demain, les organismes de formation convergent fortement. Pour aller plus loin aujourd'hui et pour répondre aux défis de demain, ils mettent en avant les apports de « la mise en situation réelle », « l'accès à des plateformes de simulation », « des travaux sur plateforme de démonstration cybersécurité industrielle ou tertiaire seraient un plus ».

Certains soulignent les apports qui pourraient être obtenus de la « mise en place d'un laboratoire de tests », de la possibilité de « participer à une plateforme d'open innovation en cyber ». Ainsi, l'école de la cybersécurité de demain est décrite comme « un croisement entre un living lab et un fab lab tout en laissant du temps à l'approche théorique » ou encore « comme ayant une part importante en immersion via une plateforme cyber-range, l'alternance en entreprises… », « Une école où tous les étudiants pourraient s'entraider et où il y aurait des formations sur la cybersécurité interactives et ultra réalistes ».

Le besoin de mise en situation opérationnelle faciliterait aussi l'hybridation des profils non-issus de la technologie : « l'accès à des logiciels du marché pour permettre à des juristes ou des professions de santé d'approcher concrètement les sujets » est différenciant.

Le développement de « coopérations avec des formations à l'international » et le renforcement « des partenariats avec différents experts dans différents domaines » sont mis plus ponctuellement en avant comme leviers d'innovation et de renforcement de l'offre de formation. Les outils de e-formation sont également cités pour faciliter l'apprentissage des notions plus théoriques : disposer d'un « campus digital avec une plate-forme d'apprentissage personnalisée avec des parcours individualisés » ou « de vidéos et de modules e-learning à réaliser à distance et en autonomie pour maîtriser les concepts théoriques » sont envisagés comme des plus.

Capitaliser sur les atouts du territoire

L'écosystème du Grand Nancy est riche d'acteurs proactifs et volontaires dans la mise en place d'initiatives partenariales, notamment dans deux domaines d'intérêt susceptibles de répondre à certaines problématiques soulevées par le diagnostic Cyber réalisé :

- la sensibilisation aux métiers en tension et l'accompagnement de parcours professionnels atypiques vers le secteur numérique ; les dispositifs innovants tels que « l'OPEN du Numérique » ou « Place des Compétences Numériques » pourraient être transposés à la cybersécurité ;
- la mobilisation d'outils de simulation (CESI NumériLab et cyber ranges interopérables) et surtout l'expérience unique de simulation de cyberguerre en vraie grandeur, « *Cyber Humanum Est* », développée sur le territoire grand-nancéien en coopération avec le Ministère des Armées.

Au-delà des capacités de formation, **le diagnostic local emploi/compétences souligne l'importance des besoins d'entraînement et de simulation en vraie grandeur**. Ces besoins s'expriment non seulement en cours de formation pour éprouver ses compétences techniques et comportementales indispensables en gestion de crise, mais aussi pour les entreprises. Plus que dans d'autres domaines, **les capacités d'entraînement et de simulation Cyber permettent un aguerrissement individuel et le développement d'un bon niveau de performance et de résilience collective.**

Les expériences du territoire du Grand Nancy pourront être mobilisées pour imaginer les conditions et dispositifs à mettre en place pour permettre un « passage à l'échelle » sur ces problématiques structurantes pour tout écosystème cybersécurité.

Partie V. Macro-plan d'action

Les différentes approches mobilisées dans le cadre de FORE-CY et leur croisement ont permis d'élaborer un macro-plan de 16 actions opérationnalisables :

Axe 1. Améliorer les dispositifs d'orientation professionnelle

Proposition #1. Sensibiliser les acteurs en charge de l'orientation scolaire et post-bac afin qu'ils tiennent mieux compte de la pluralité des métiers de la chaîne de valeur Cyber, en embrassant l'ensemble des sous-filières métier.
Proposition #2. Développer des outils de détection des profils « compatibles Cyber », basés sur les compétences transversales et l'appétence à l'informatique, à la gouvernance des risques ou à la gestion de crise.
Proposition #3. Valoriser l'offre de BTS en informatique appliquée à la cybersécurité ou des champs connexes qui constitue le maillage de proximité locale du domaine, en veillant au mieux à la féminisation de ces parcours d'entrée.

Axe 2. Mieux accompagner les parcours de reconversion professionnelle

Proposition #4. Sensibiliser les acteurs en charge de l'accompagnement socioprofessionnel et de la reconversion aux différents univers professionnels de la cybersécurité.
Proposition #5. Mieux accompagner les personnes qui engagent un parcours de reconversion en cybersécurité ou dans un domaine connexe avec module Cyber.

Axe 3. Anticiper les expertises technologiques clés de demain

Proposition #6. Intégrer dans les maquettes pédagogiques des enseignements renforcés en IA.
Proposition #7. Renforcer les liens entre cryptographie et cybersécurité.
Proposition #8. Apprécier les besoins et renforcer le cas échéant, l'offre de formation en conception et modélisation des architectures et en cyberdéfense/cyberattaque**.**

Axe 4. Améliorer la formation des profils Cyber

Proposition #9. Consolider et renforcer la formation en instaurant plus de pluridisciplinarité au sein des parcours technologiques (approche hybride juridique, sciences humaines et sociales, UX, design, méthodes agiles)**.**
Proposition #10. Développer les parcours hybrides pour répondre aux besoins en compétences de l'ensemble de la chaîne de valeur Cyber, au sein des établissements d'expertise non-technologique.
Proposition #11. Renforcer l'acquisition et l'entretien des *soft skills* (gestion du stress, travail en transverse…) afin de limiter l'attrition des professionnels des métiers technologiques de la Cyber.

Axe 5. Faire du Grand Nancy une place forte de formation Cyber d'envergure nationale

Proposition #12. Promouvoir une offre de formation Cyber de haut niveau, cohérente, forte et attractive du Bac +2 au Bac +8 à l'échelle du bassin nancéien, en favorisant les continuums de parcours d'excellence, les mentions de spécialisation en santé ou en finance, et en développant des réponses innovantes aux besoins de la filière Cyber.
Proposition #13. Mettre en œuvre une sensibilisation systématique à l'hygiène numérique des jeunes publics du bassin nancéien.
Proposition #14. Doter le territoire du Grand Nancy d'une infrastructure hybride de simulation d'attaque Cyber et de gestion de crise à destination de tous les publics**.**

Axe 6. Concourir à un territoire de résilience et confiance

numériques en étant à l'écoute des besoins de l'écosystème

Proposition #15. Concrétiser sur le territoire nancéien le projet de Campus Régional Cyber (lieu totem ou antenne), afin de favoriser les coopérations au sein de l'écosystème et de mettre en place un Observatoire prospectif local et régional des emplois, métiers et compétences Cyber.

Proposition #16. Renforcer la sensibilisation de tous les acteurs du bassin nancéien à la cybersécurité et mieux faire valoir les services offerts par le CSIRT et les ESN de la métropole auprès des entreprises, des administrations, des élèves/étudiants et du grand public**.**

GOUVERNEMENT

Liberté
Égalité
Fraternité

FRANCE 2030

Contact

Ekaterina MINTCHEVA
Coordinatrice Emploi et Compétences
de la Maison de l'Emploi du Grand Nancy
Tél. 03.83.22.24.00
88 Avenue du XX^{e} Corps BP 90657 – 54063 NANCY CEDEX