

PÔLE D'EXCELLENCE CYBER

PENSER AUJOURD'HUI LA CYBER DE DEMAIN

Regards croisés sur les transformations des métiers, des formations et des compétences.

Une étude prospective fondée sur 17 entretiens avec des acteurs de l'écosystème cyber.

Novembre 2026

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

Cet ouvrage a bénéficié d'une aide de l'État gérée par **l'Agence Nationale de la Recherche** au titre de **France 2030** portant la référence « ANR-23-CMAS-0026 ».

Rédacteurs :

Le Pôle d'excellence cyber tient à remercier Louise Dachelet, Iris Hourcade et Solène Chevreau qui ont contribué à la préparation et à l'élaboration de cet ouvrage, en tant que rédactrices.

Le Pôle d'Excellence Cyber souhaite également remercier chaleureusement tous les professionnels qui ont accepté les interviews proposées qui ont servie de base de travail pour cet ouvrage.



IRIS HOURCADE

Chargée de l'Observatoire Emplois et compétence, coordinatrice des GT du Pôle d'excellence cyber.



LOUISE DACHELET

Étudiante Sciences Po et IMT Atlantique, stagiaire du Pôle d'excellence cyber et cadette de la cyber.



SOLÈNE CHEVREAU

Coordinatrice Cyberskills4All, responsable des projets de formation Pôle excellence cyber

PRÉFACE

par l'Amiral Coustillière

La cybersécurité n'est plus un sujet technique parmi d'autres. Elle touche désormais directement à notre souveraineté et tous les pans de nos sociétés modernes.

Intelligence artificielle, cloud public et souverain, cryptographie post-quantique, attaques informationnelles et fake-news : ces technologies redessinent les rapports de force, mais comportent aussi des dimensions sociétales, économiques et géopolitiques. Notre capacité à protéger nos infrastructures et nos données dépend largement de notre maîtrise des compétences qui les rendent possibles, compétences qu'il faut aussi savoir et pouvoir conserver en Europe, sans se fermer aux échanges et coopérations.

Au-delà de ces technologies en évolution extrêmement rapide, la question de la souveraineté en matière de compétences et de formation reste trop souvent le parent pauvre de l'autonomie stratégique. Et pourtant il constitue un point de départ essentiel : former les esprits aux référentiels, aux réglementations, aux méthodologies, et aux outils propres à l'Europe devrait être une priorité.

Après un premier volet centré sur l'analyse des enquêtes existantes, ce nouveau livrable prend le parti d'une approche qualitative et prospective. Il s'appuie sur des entretiens menés auprès d'un panel volontairement large : experts techniques, responsables RH, dirigeants d'entreprises, enseignants-chercheurs, représentants d'institutions régaliennes. Les échanges ont parfois été contrastés, mais toujours instructifs, et ils nous ont permis d'aller au-delà des constats habituels pour cerner les tendances qui structureront le marché de demain.

Ce document n'a pas la prétention de clore le débat, plutôt de l'ouvrir. La feuille de route rassemble, sans chercher à les hiérarchiser, les pistes qui sont ressorties des entretiens : révision des maquettes pédagogiques, doubles compétences à développer, nouvelles formes de gouvernance, actions de sensibilisation au plus près du terrain. Libre à chacun de vous, que vous travailliez dans la formation, le recrutement ou la stratégie d'entreprise, de vous saisir de ces propositions, de les discuter, de les faire évoluer et, surtout, de les traduire en actions.

La souveraineté numérique se construit dans la durée par des actions concrètes, notamment par l'investissement dans les compétences et le dialogue entre les acteurs. Ce travail y contribue grâce au temps et à l'expertise des professionnels qui ont accepté de partager leur expérience. Je les en remercie sincèrement, ainsi que toutes celles et ceux qui s'engageront dans la réflexion et donneront une suite concrète à ces pistes.



SOMMAIRE

PRÉFACE PAR L'AMIRAL COUSTILLIÈRE 5

INTRODUCTION 9

PARTIE 1 : ANALYSE DES INTERVIEWS 11

I. ÉCOSYSTÈME DE FORMATION : ADAPTER LES PARCOURS AUX RÉALITÉS DU MARCHÉ 12

A. La formation initiale face à l'évolution des métiers 12

1. Les ajustements nécessaires au sein des parcours de formation 12

2. Maintenir l'adaptabilité des diplômes face aux mutations rapides 13

3. Développer la culture générale, compétences transversales et intégration de l'IA 13

B. Enjeux d'alternance et renforcement des liens avec le monde professionnel 14

1. L'alternance : un modèle à faire évoluer 14

2. Structurer un dialogue entre les acteurs de la formation et les employeurs 14

3. L'intégration des compétences comportementales et de la culture d'entreprise 15

II. LE MONDE PROFESSIONNEL : TRANSFORMER LES PRATIQUES DE RECRUTEMENT ET RESPONSABILISER LA GOUVERNANCE 17

A. L'évolution des enjeux de recrutement 17

1. Surmonter les blocages d'insertion des profils juniors face à l'automatisation et aux tensions d'encadrement. 17

2. Moderniser les référentiels : passer d'une approche métier à une approche compétence fine et dynamique. 18

3. Répondre aux exigences du recrutement en valorisant la posture, les compétences relationnelles et la communication 19

B. Une nécessaire prise de conscience des dirigeants et des entreprises 20

1. Réveiller la gouvernance pour sortir de la passivité, de l'illusion de sécurité, et prendre conscience des risques 20

2. Sécuriser le terrain industriel et l'ensemble de la chaîne de valeur 20

3. Inculquer une culture de souveraineté et réorienter les politiques d'achat 21

III. PROSPECTIVE : ANTICIPER LES RUPTURES ET ACCOMPAGNER LES MUTATIONS 23

A. Réglementation et dynamiques territoriales 23

1. Accompagner la poussée réglementaire européenne pour transformer l'obligation de conformité en un levier d'action 23

2. Renforcer le maillage des compétences et l'accompagnement des territoires 24

B. L'impact des technologies émergentes sur les métiers de demain 24

1. L'intelligence artificielle : un domaine à structurer 24

2. Engager le virage du post-quantique et anticiper les risques 25
3. Garantir la souveraineté des infrastructures cloud : freins géopolitiques, disparités territoriales et réalités de recrutement 26
CONCLUSION 27
PARTIE 2 : FEUILLE DE ROUTE OBSERVATOIRE 29
Thème formation initiale 30
Thème Soft Skills 31
Thème formation continue / tout au long de la vie 31
Thème RH / GPEC 32
Thème Faire rayonner la cyber 32
Thème Management des entreprises 32
Thème Dirigeants d'entreprises 33
Thème Sensibilisation 33
Thème Relation écoles /universités avec les entreprises 33
PARTIE 3 : SYNTHÈSE DES INTERVIEWS RÉALISÉES 35
AMIAD (Agence Ministérielle pour l'Intelligence Artificielle de Défense) 36
ANSSI – Agence Nationale de la Sécurité des Systèmes d'Information 38
BCI - Bretagne Commerce Internationa 42
Capgemini 45
CEA - Commissariat à l'énergie atomique et aux énergies alternatives 50
CLUSIF 53
COMCYBER 56
Cyber'Occ 60
DINUM-Direction interministérielle du numérique 64
Territoire Grand Nancy 68
Grand groupe international de services numériques 70
OVALT Group 74
Sciences PO Rennes 77
S3NS (Thalès) 80
SOPRASTERIA 84
Université Côte d'Azur 87
Université Côte d'Azur 90

INTRODUCTION

Après une première étude qui a permis de faire un tour d'horizon des enquêtes existantes dans le domaine des besoins en emploi et compétences en cybersécurité, cette seconde étude est une approche qualitative des grandes tendances de la cybersécurité et des thématiques émergentes (à titre d'exemple : l'intelligence artificielle, le cloud souverain et la menace quantique).

Ce document regroupe ainsi l'analyse de 17 interviews effectuées entre avril et juin 2026 auprès de professionnels. Ces personnes ont volontairement un profil très divers (experts cyber dans différents domaines d'activités, professionnels RH, responsable d'équipes, mais aussi enseignants, responsables de cursus de formations ou directeur/directrice de structure publique ou privée). Le panel est composé de 11 femmes et 8 hommes répartis sur tout le territoire français (avec une attention toute particulière portée à la représentativité des différents territoires : Nord, Est, Ouest, Sud et Île de France). Certaines interviews se sont faites en duo.

Au cours de ces interviews, chacun nous a livré sa vision du monde cyber d'aujourd'hui et des besoins pressentis pour demain. Ces interviews extrêmement riches présentent donc différentes visions / points de vues et des positions très différentes. En matière d'anticipation et de prévisions des besoins de demain, personne n'a forcément la réponse, néanmoins en croisant tous ces regards, nous sommes convaincus que nous approchons un peu plus de ce dont sera fait l'avenir et ainsi d'être en capacité de percevoir les grandes tendances. Ainsi dès les premiers entretiens, nous avons très vite constaté des points communs, des tendances de fond qui se dessinent mais aussi des divergences dans ces visions. Cette étude s'applique donc à vous retranscrire ces visions communes et divergentes sur les grandes tendances de la cyber.

Après une première partie d'analyse globale de ces interviews, vous trouverez en annexe deux éléments complémentaires :

- Une feuille de route qui recense toutes les propositions et idées qui ont émergées au cours de ces interviews. Aucun tri n'a été fait dans ces itérations, ces idées ont vocations à être débattues et chacun pourra décider de la voie à suivre ou non pour sa formation, son entreprise. L'objectif de cette feuille de route est de nourrir la réflexion stratégique du projet Cyberskills4all mais également de tout l'écosystème cyber.
- Les synthèses de ces 17 entretiens, cela vous permettra de rentrer plus dans le détail et d'explorer la richesse de ces entretiens.

Enfin, je tiens à remercier tout particulièrement les professionnels qui se sont prêtés au jeu des interviews : cet exercice de projection est loin d'être évident et nos questions parfois ardues. Mille mercis pour le temps passé à ces interviews et à la validation des compte rendus qui reflètent toute la diversité et la richesse de l'écosystème actuel.


01

ANALYSE DES INTERWIEWS

- **I. ÉCOSYSTÈME DE FORMATION :**
  ADAPTER LES PARCOURS AUX RÉALITÉS DU MARCHÉ

- **II. LE MONDE PROFESSIONNEL :**
  TRANSFORMER LES PRATIQUES DE RECRUTEMENT ET RESPONSABILISER LA GOUVERNANCE

- **III. PROSPECTIVE :**
  ANTICIPER LES RUPTURES ET ACCOMPAGNER LES MUTATIONS

I. ÉCOSYSTÈME DE FORMATION : ADAPTER LES PARCOURS AUX RÉALITÉS DU MARCHÉ

L'analyse des interviews réalisées met en lumière l'importance de renforcer les liens entre le monde de la formation initiale (écoles, universités…) et le monde professionnel. Les technologies, les outils et les menaces évoluent très vite, en cyber. Face à cette accélération, les métiers se transforment, les besoins en compétences changent ; et la formation initiale doit s'adapter à ces bouleversements et accompagner ses apprenants dans leur insertion professionnelle plus difficile actuellement.

A. La formation initiale face à l'évolution des métiers

1. Les ajustements nécessaires au sein des parcours de formation

Les entretiens menés auprès des acteurs de l'écosystème de cybersécurité révèlent certains défis structurels dans l'orientation et l'attractivité des formations. L'offre se caractérise par un paysage très foisonnant, près de 900 cursus[1], ce qui peut rendre la lisibilité complexe et l'adéquation continue avec les besoins du marché délicate. Ce phénomène engendre des déséquilibres ciblés sur certains métiers ou une incompréhension de certaines contraintes liées aux métiers de la part des apprenants. Comme l'illustre David Dutertre (Bretagne Commerce International BCI), *«Le côté romantique du hacker […] de nombreux candidats à l'embauche voulaient être en tests de pénétration […] c'était beaucoup moins fun de faire de la surveillance en 3/8 et de passer du temps à faire du triage d'alertes et de faux positifs »*. Cette préférence des candidats a créé une pénurie ciblée, plus qu'une pénurie généralisée : *« il manquait du monde certes, mais surtout dans certains secteurs comme le monitoring 24/7»*. Cette préférence peut occasionner des tensions de recrutement dans des domaines essentiels comme les centres de sécurité opérationnelle (SOC).

Par ailleurs, les établissements restent encadrés par des contraintes réglementaires et académiques (habilitation à délivrer des licences ou masters, CTI, RNCP,…) qui limitent parfois leur agilité pédagogique et l'adaptation des contenus de formation face aux évolutions rapides des métiers.

Cette situation s'accompagne d'une pluralité d'approches selon les établissements. D'un côté, certains cursus universitaires (comme Toulouse ou Montpellier) se concentrent fortement sur l'open source et Linux, offrant une base solide mais pouvant nécessiter un complément d'acculturation sur les environnements propriétaires. *« Une entreprise a pointé du doigt les diplômés de l'Université de Toulouse : excellents sur Linux, mais peut-être un peu moins sur Windows »*, souligne Karine Béguin (Cyber'Occ). De leur côté, les écoles privées (YNOV, EPITA, EPITECH) cherchent à intégrer rapidement les retours du marché : *« Elles ont réussi à couvrir différents systèmes d'exploitation dès qu'un besoin était identifié »*.

Cette réactivité pédagogique s'explique par des processus décisionnels plus souples. À l'inverse, les universités publiques, confrontées à des contraintes budgétaires et administratives plus strictes, composent avec des rythmes de révision de maquettes plus longs. *« Les universités doivent absolument se transformer. Le modèle*

1 whttps://www.opiiec.fr/etudes/141341

économique préexistant est en train de disparaître », observe le Général Franck Nicol (Sciences Po Rennes). Ce constat est corroboré par Christian Tafani (Université Côte d'Azur) qui rappelle les évolutions culturelles en cours pour renforcer le dialogue avec le privé. Enfin, cet écart classique entre temps institutionnel et technologique s'illustre par la création récente de la mention nationale de Master « Cybersécurité »[2], marquant une étape clé mais progressive dans l'institutionnalisation de la discipline.

2. Maintenir l'adaptabilité des diplômes face aux mutations rapides

Malgré une préparation technique solide, l'accélération des menaces et l'émergence de technologies disruptives (IA, quantique…) obligent à faire évoluer en continu les cursus afin d'anticiper les compétences de demain, car comme l'explique le Général Franck Nicol (Sciences Po Rennes), si les cursus actuels préparent efficacement aux compétences techniques (sécurisation du SI, détection et de réponse aux incidents), la rapidité des évolutions technologiques (IA, quantique) invite à enrichir ces parcours. Au-delà des approches d'auto-formation par les défis techniques (type CTF), l'enjeu est d'apporter aux futurs ingénieurs une culture managériale, stratégique, juridique et géopolitique globale. En effet *« il faut des ingénieurs agiles, qui apprennent à apprendre, à défendre, mais aussi à attaquer. Car quand on apprend à attaquer, quand on se met à la place de l'autre, on se protège mieux »*.

Ainsi, au cours d'un cursus, certaines compétences et outils enseignés en début de parcours peuvent rapidement nécessiter des mises à jour. Les programmes ont donc intérêt à ne pas se focaliser uniquement sur des technologies spécifiques pour privilégier l'adaptabilité. *« Dans nos métiers, qui évoluent à une vitesse considérable, nous avons avant tout besoin de personnes qui possèdent les bons réflexes, du discernement et une véritable capacité d'apprentissage. Nous recherchons des profils qui savent se poser les bonnes questions et apprendre en permanence, plutôt que des experts ultra-spécialisés dans une technologie ou un langage précis. Car nous savons qu'en l'espace de trois ans, la technologie sur laquelle ils ont été formés peut ne plus répondre aux besoins du marché. »*, résume Édouard Jeanson (Capgemini).

Cette vision n'exclut pas le besoin d'ancrage métier, selon David Dutertre *« Par exemple, un pentester ou quelqu'un du CSIRT issu d'un parcours de formation générale, c'est à minima 7 ans, pour qu'il devienne quelqu'un de suffisamment expérimenté. Or, aujourd'hui, on a des outils d'automatisation et l'IA qui posent la question de la rentabilité de l'embauche de profils juniors »*. Il en résulte un besoin de spécialisation plus tôt dans les cursus, non pas sur une technique donnée, mais sur un métier ou un segment de la posture cyber (défense, gouvernance, réponse à incident, rétro-ingénierie), chacun nécessitant un temps d'apprentissage propre minimum de plusieurs années.

3. Développer la culture générale, compétences transversales et intégration de l'IA

Face à l'accélération technologique, les acteurs de la cybersécurité s'accordent sur un constat : les formations gagnent à renforcer l'apprentissage par compétences transversales. Cette mutation passe par un renforcement de la culture générale et de la réflexion critique, comme le souligne Christian Tafani (Université Côte d'Azur) : *« Dans cette perspective, la philosophie, la géopolitique, l'histoire et les sciences humaines occupent une place fondamentale. Elles permettent de développer l'ouverture d'esprit, l'empathie, la capacité à comprendre des logiques culturelles différentes ainsi que le recul indispensable face à des situations souvent complexes »*. L'idée est de former des esprits agiles, capables de contextualiser leurs connaissances.

Cette transversalité s'incarne dans l'émergence d'un profil de « techno-stratège », tel que le défend le Général Franck Nicol (Sciences Po Rennes): *« On a besoin de personnes qui font le lien entre la technique et la décision politique ou économique »*, insistant sur la création de passerelles avec des institutions comme Sciences Po. Pour autant, imposer une double spécialisation obligatoire ne fait pas consensus. Christian Tafani (Université Côte d'Azur) nuance : *« Pour autant, cette évolution ne me paraît pas devoir être imposée de manière uniforme*

2 https://www.francecompetences.fr/recherche/RNCP/39495

à l'ensemble des cursus. Une obligation réglementaire risquerait de produire un effet inverse à celui recherché, en conduisant certains établissements à créer des enseignements répondant davantage à une exigence administrative qu'à une véritable ambition pédagogique ». Il semble préférable d'encourager les initiatives, de valoriser les parcours atypiques et de favoriser les passerelles entre disciplines. La qualité d'une double compétence repose avant tout sur la cohérence du projet de formation et sur la motivation de l'étudiant, davantage que sur le respect d'une obligation formelle.

Ainsi, pour contrer l'obsolescence rapide des connaissances techniques, le modèle de formation ne peut plus reposer uniquement sur l'apprentissage d'outils figés. L'accent doit être mis sur des qualités comportementales et intellectuelles. *« Pour la compétence principale recherchée, je dirais la curiosité, c'est un domaine qui évolue constamment donc il faut se remettre en cause, avoir des bases solides. Je pense qu'il y a un socle de connaissances à avoir, et après savoir faire preuve de curiosité et d'agilité »* explique le Colonel (COMCYBER)

Enfin, les formats pédagogiques évoluent pour renouveler le cours magistral au profit de mises en situation pratiques. Cette transition s'accompagne d'une transformation nécessaire des modes d'évaluation à l'ère de l'IA générative. Comme l'illustre Marina Teller (Université Côte d'Azur), l'utilisation de négociations fictives ou de simulations d'attaque permet de stimuler directement l'agilité, la réflexion stratégique et l'éthique des étudiants.

B. Enjeux d'alternance et renforcement des liens avec le monde professionnel

1. L'alternance : un modèle à faire évoluer.

Le contexte socio-économique, marqué par l'évolution des mécanismes d'aide à l'alternance, invite à réinterroger les parcours d'insertion des jeunes diplômés. Alors que l'offre de formation a fortement progressé, un décalage persiste entre les candidatures et la nature des besoins exprimés. Comme le souligne Florence Puybareau (Clusif) : *« L'offre de formation a explosé en quelques années, il y en a aujourd'hui quasiment dans toute la France. C'est une bonne nouvelle mais j'ai été plusieurs fois contactée par des directeurs d'établissements me disant qu'ils n'arrivaient pas "à caser" leurs alternants . Et parallèlement, les entreprises me disent qu'elles n'arrivent pas à trouver les bons profils ». « C'est surtout vrai dans les moyennes structures qui ont besoin d'experts cyber mais ne souhaitent pas prendre des alternants car elles n'ont pas les moyens (humains et financiers) et le temps de les former . Il y a un vrai problème d'adéquation entre l'offre et la demande ».* Face aux contraintes d'encadrement, certaines structures opérationnelles hésitent à s'engager auprès de profils juniors sans accompagnement dédié. Ce constat met en lumière une polarisation des recrutements. Tandis que les diplômés de Master accèdent plus rapidement aux dispositifs en entreprise, les apprenants issus de parcours intermédiaires (BTS CIEL, BTS SIO, BUT) rencontrent davantage de difficultés. Karine Béguin (Cyber'Occ) observe ainsi qu'*« au niveau Master, il y a très peu de soucis pour trouver une alternance ou un stage, par contre pour les niveaux Bac+2 ou Bac+3, c'est plus complexe ».*

Cette situation affecte particulièrement le tissu des TPE et PME, pourtant directement exposées aux risques numériques mais souvent privées de compétences internes pour tutorer des étudiants. *« Des entreprises qui auraient besoin de compétences cyber ne peuvent pas prendre d'étudiants, puisqu'elles n'ont pas de maître d'apprentissage »*, rappelle Karine Béguin (Cyber'Occ). Développer des solutions d'accompagnement pour ces structures constitue ainsi un levier d'insertion stratégique pour le territoire.

2. Structurer un dialogue entre les acteurs de la formation et les employeurs

L'alternance, levier clé de la montée en compétences, nécessite un alignement continu entre programmes académiques et besoins opérationnels. Une partie des écarts constatés provient d'une imprécision initiale dans la caractérisation des métiers. Comme le relève Nicolas Turquet (DINUM), de nombreuses offres restent trop génériques : *« Tant que le répertoire décrit chaque métier dans le détail, il reste difficile d'identifier ce qui, d'un*

métier à l'autre, relève de compétences réellement transférables » ; en raisonnant par métiers macros, le RMFP+[3] doit pouvoir rendre au contraire visibles les compétences invariantes qui traversent plusieurs métiers proches : un data steward, un data scientist et un data analyst partagent, par exemple, une même culture de la chaîne de valeur de la donnée, quand bien même leurs compétences techniques restent distinctes.

Pour surmonter ces imprécisions, des synergies prometteuses s'organisent. Des acteurs comme S3NS co-construisent des parcours adaptés avec des établissements ciblés : *« certains sont pris en considération, d'autres sont un peu plus compliqués à développer [...] on travaille notamment avec l'EFREI [...] S3NS a été notamment le sponsor de la création d'une majeure »*. Néanmoins, l'accélération technologique, notamment autour de l'intelligence artificielle, exige une mise à jour constante des référentiels pour que l'école et l'entreprise s'enrichissent mutuellement.

De leur côté, les grandes institutions publiques et sécuritaires cherchent également à fluidifier leurs canaux d'échanges. Stéphanie Beheydt (CEA) et le Colonel (COMCYBER) soulignent l'intérêt d'instaurer des cadres de concertation plus réguliers avec les organismes de formation. Comme le reconnaît le Colonel, ce décalage se traduit concrètement par un long délai de montée en autonomie des jeunes recrues sur le terrain, qu'illustre l'exemple du CALID : *« un jeune qui arrive au CALID, il a besoin d'un an et demi voire 2 ans pour pouvoir être autonome »*. Le Colonel y voit un axe de travail à explorer avec les écoles pour réduire ce temps d'adaptation, en s'appuyant sur des dispositifs de liaison existants : *« je pense que le Pôle d'Excellence Cyber peut être une bonne courroie de transmission entre nos deux mondes »*. De son coté, l'AMIAD récemment créée (2024) commence à entamer ce dialogue *« Il y a plusieurs écoles qui ont été identifiées, la feuille de route école a été validée il y a peu de temps [...] il n'y a encore rien de formalisé à ce jour, les premières actions sont prévues à l'automne 2026 »*.

3. L'intégration des compétences comportementales et de la culture d'entreprise

Au-delà de la maîtrise technique, l'insertion professionnelle des diplômés repose de plus en plus sur leurs compétences comportementales (soft skills) et leur compréhension de l'écosystème économique. Florence Puybareau (Clusif) note à ce titre qu'il convient de renforcer l'acculturation des étudiants au fonctionnement des organisations : *« Ils ont un bon bagage technologique mais dès que l'on parle de la cyber sécurité en tant que secteur industriel, [...] ils n'en ont aucune idée. Ils connaissent quelques grands acteurs du marché mais rien sur son organisation, son mode de fonctionnement, les forces en présence, les enjeux économiques... Idem sur la façon dont fonctionne une entreprise, le processus des appels d'offres, la réalisation d'un cahier des charges, la conception d'un budget que l'on va aller défendre devant sa direction. C'est ce que j'essaye de leur apporter pendant nos cours »*. Dans un marché du travail plus exigeant, la capacité à dialoguer avec des instances dirigeantes devient déterminante.

Cette attention portée au savoir-être est aujourd'hui partagée par l'ensemble des recruteurs. Delphine Chadozeau et Romain Brechet (S3NS) expliquent *« Nous recherchons des personnes qui disposent des compétences techniques attendues, mais qui savent également travailler en groupe et répondre à des problématiques complexes avec le savoir-être approprié. Cette composante n'est pas encore suffisamment intégrée dans les parcours scolaires. »*, un aspect désormais mieux pris en compte par les équipes pédagogiques.

Dans un environnement en mutation rapide où l'IA transforme les pratiques, la posture prime sur la simple maîtrise d'un outil éphémère. Stéphanie Beheydt et Estel Chiron (CEA) soulignent ainsi que *« Au-delà des softskills, [...] la capacité à apprendre [...] permettra de s'adapter à la fréquence à laquelle les nouveaux outils arrivent, probablement supérieure à ce que les générations précédentes ont vécu à l'arrivée du téléphone portable, d'Internet etc. Donc celui qui sera en difficulté, c'est celui qui n'arrivera pas à apprendre et à s'adapter en permanence tout en préservant le collectif. »*. Cette agilité intellectuelle s'accompagne d'un savoir-être fondamental sur le terrain, comme le résume Madame C. (Sopra Steria) : *« Ça va être vraiment sa posture. Est-ce*

3 Le répertoire du référentiel des métiers de la fonction publique sert de guide exhaustif et structuré, énumérant une diversité de professions réparties sur trois versants distincts : l'État, la Territoriale et l'Hospitalière. Chaque métier est soigneusement détaillé, permettant une compréhension claire et précise de l'activité et des compétences requises pour exceller dans le domaine. https://www.data.gouv.fr/datasets/repertoire-du-referentiel-des-metiers-de-fonction-publique-rmfp

qu'il est capable d'écouter un client ? C'est sa capacité à dire qu'il ne le sait pas. Ne pas savoir, ce n'est pas grave. On prend l'information, on pose la question, et on va rechercher la réponse ». Enfin, Christian Tafani (Université côte d'Azur) rappelle que cet accompagnement gagne à inclure des méthodes pratiques d'autonomie et de gestion de projet afin d'assurer une transition fluide vers le monde du travail.

II. LE MONDE PROFESSIONNEL : TRANSFORMER LES PRATIQUES DE RECRUTEMENT ET RESPONSABILISER LA GOUVERNANCE

L'analyse des interviews porte notre attention sur les enjeux de recrutement aujourd'hui : quelle place pour les juniors ? Comment adapter les référentiels d'emplois ? Quels sont les soft skills particulièrement recherchés ?

L'enjeu, selon les témoignages des experts, porte également sur la prise de conscience des dirigeants d'entreprises et la place de la gouvernance dans les entreprises, dans l'approche des risques cyber. Qu'en est il également des questions de souveraineté, de politique d'achat ; quelles réalités pour les petites industries ?

A. L'évolution des enjeux de recrutement

1. Surmonter les blocages d'insertion des profils juniors face à l'automatisation et aux tensions d'encadrement.

L'accès au marché du travail pour les jeunes diplômés en cybersécurité se heurte au croisement d'incertitudes économiques, d'automatisation technologique et d'un manque d'encadrement. Face aux tensions géopolitiques, les recrutements se recentrent sur une exigence de maturité opérationnelle immédiate comme l'exprime l'AMIAD : « *Actuellement, nous avons beaucoup de candidats juniors ou peu expérimentés qui postulent sur nos offres, avec l'évolution de nos projets et de nos besoins, notre cœur de cible ça va plutôt être des seniors voire des experts* ». Ce repositionnement fait suite à un premier cycle de recrutements plus orientés juniors, qui a mis en évidence un besoin complémentaire d'expertise technique plus affirmée et plus polyvalente : *« on a recruté l'année dernière en grande majorité des juniors, et on se rend compte qu'on a aussi besoin d'un certain niveau d'expertise, et peut-être pas seulement sur une seule technologie »* . Comme l'alerte Édouard Jeanson (Capgemini), *« Nous privilégions aujourd'hui des profils expérimentés, capables d'exercer leur jugement, de prendre du recul et de s'appuyer sur des situations déjà vécues. Mais cela soulève une question essentielle : si nous voulons préparer l'avenir, comment continuer à intégrer et à former les jeunes générations afin qu'elles puissent, à leur tour, acquérir cette expérience ? »*.

Cette réticence est accentuée par l'arrivée de l'IA générative dans les opérations courantes. En automatisant les tâches répétitives d'entrée de gamme, notamment au SOC ou dans l'analyse juridique, l'IA supprime la porte d'entrée traditionnelle des juniors. Florence Puybareau (Clusif) observe : *« En effet l'IA est en train de changer la donne pour beaucoup de métiers. Avant, il fallait des humains pour faire des travaux "d'entrée de gamme". Aujourd'hui, avec l'automatisation et l'IA il faut d'autres compétences […] Les premiers niveaux d'analyse sont remplacés par l'IA, et il y a besoin de gens qui analysent l'analyse »*. Ce passage direct à des tâches d'analyse prive les débutants de leur tremplin. *« Pendant longtemps, les postes d'opérateur de SOC constituaient une porte d'entrée naturelle vers les métiers de la cybersécurité. C'est à partir de cette première expérience que les professionnels pouvaient ensuite évoluer vers des fonctions plus expertes, notamment en architecture.*

Aujourd'hui, ces postes de premier niveau tendent à disparaître sous l'effet de l'automatisation. Cela soulève un véritable enjeu : comment offrir aux jeunes diplômés les premières expériences indispensables à leur montée en compétences ? Par où commenceront-ils leur parcours professionnel demain ? », s'interroge Édouard Jeanson (Capgemini), ce qu'étaye Madame C. (Sopra Steria) : *« On continue à recruter des profils juniors mais on n'augmente pas ce volume, on le stabilise». Romain Bréchet (S3NS) nuance toutefois « L'IA ne doit pas être considérée comme un moyen de remplacer les collaborateurs. En revanche, elle devient indispensable pour améliorer l'efficacité de certaines activités. »*

L'intégration de ces juniors se heurte aussi à d'autres problématiques des entreprises : le manque d'encadrement par des seniors et l'augmentation des responsabilités confiées aux juniors, faute de trouver des seniors. Au CEA, Stéphanie Beheydt et Estel Chiron indiquent limiter le recrutement des jeunes aux capacités d'encadrement de la structure. Ce déficit de seniors produit des anomalies : Aurélie Bauer et Claudia Miranda Pires (ANSSI) s'étonnent de voir *« beaucoup de jeunes qui sortent d'études qui se retrouvent RSSI »*, occupant prématurément des postes à hautes responsabilités.

En parallèle, la surenchère s'intensifie sur les expertises de niche en cybersécurité – cryptographie post-quantique (PQC), reverse engineering, forensic et Active Directory (AD) –, des compétences devenues stratégiques pour la sécurité des infrastructures nationales. Cette tension se traduit par des écarts de rémunération croissants entre secteurs public et privé, rendant le recrutement et la fidélisation de profils expérimentés particulièrement difficiles pour les institutions publiques.

Comme le soulignent Aurélie Bauer et Claudia Miranda Pires (ANSSI), *« Si vous souhaitez recruter un expert en cyber aujourd'hui, cela ne va pas être chose aisée, car ils sont extrêmement recherchés, donc rares et, dès lors, coûteux »*, tandis qu'Estel Chiron (CEA) et le Colonel (COMCYBER) constatent que les pentesters et spécialistes en forensic sont systématiquement ciblés par des offres privées plus attractives. Cette dynamique de turnover structurelle spécifique à certains domaines du public comme le Ministère des Armées, avec des durées moyennes de service de l'ordre de trois années, affaiblit les capacités d'encadrement et de transmission des savoirs. *« On a des temps de service faibles, de l'ordre de 3 ans […], on a des facilités à recruter des juniors, mais des profils expérimentés, c'est un défi »*, résume le Colonel, soulignant le cercle vicieux qui prive le secteur d'une stabilité opérationnelle nécessaire à l'émergence d'une expertise souveraine durable.

Si la fidélisation des talents reste un défi pour le secteur public, celui-ci mise sur la notoriété de ses entités et la dimension stratégique de ses missions pour attirer les compétences. Stéphanie Beheydt (CEA) en témoigne : *« L'attractivité de l'organisme fonctionne globalement bien, notamment du fait du caractère particulier du CEA, organisme public de recherche porteur de grands projets dont la vocation est d'agir pour la souveraineté scientifique, technologique et industrielle de la France et de l'Europe. »* Cette attractivité se heurte cependant à une concurrence marquée sur les profils les plus recherchés.

2. Moderniser les référentiels : passer d'une approche métier à une approche compétence fine et dynamique.

Le décalage entre la formalisation des métiers et la réalité du marché constitue un obstacle majeur au recrutement. Cette difficulté provient d'abord d'une mauvaise définition des besoins au sein même des organisations. Aurélie Bauer et Claudia Miranda Pires (ANSSI) dressent un constat sévère sur la rédaction des offres d'emploi : *« On s'est rendu compte que les offres d'emploi étaient très mal rédigées, et surtout que les employeurs n'arrivaient pas vraiment à identifier les compétences dont ils avaient besoin : c'est ça, la grosse difficulté. […] Sur 16 000 fiches de postes en cybersécurité, 30 % avaient un intitulé « ingénieur cyber » en 2021, sauf que « ingénieur cyber », ce n'est pas un métier, c'est juste un niveau de qualification : on cherche quelqu'un qui a un bac+5 en cyber. Mais le problème, c'est que cela ne dit pas quelles compétences on recherche. »*. Cette confusion conduit à utiliser des intitulés imprécis et à mélanger des rôles aux logiques très différentes. Comme le rappelle David Dutertre (BCI), l'enjeu consiste à sortir d'une logique purement technologique pour cibler les métiers dans toute leur composante : *« On ne peut pas se baser sur la seule spécialisation technique. Une spécialisation dans les*

différents segments de la posture cyber, ça c'est important. Ce n'est pas du tout le même métier de faire du rétro-ingénierie de malwares ou de la réponse à incident que de faire de la surveillance 24/7 par exemple ».

Face à cette méconnaissance, les outils traditionnels de gestion des RH montrent leurs limites. Les référentiels de postes et les feuilles de route deviennent obsolètes à mesure que les technologies évoluent. Madame M (Grand groupe international de services numériques) observe la fin des planifications à long terme : *« Si on prévoit des parcours de montée en compétence, le temps qu'on les construise, il y aura des technologies, des choses qui auront évolué. Avant, on pouvait se dire : on fait un plan sur trois ans, même avant cinq ans, et on était sûr que c'était OK. Ce n'est plus le cas »* pour autant elle ajoute que cela ne revient pas à renoncer à l'anticipation *« On essaye d'anticiper, mais on devient parfois plus en réactivité par rapport aux nouvelles technologies »*. Pour sortir de cette rigidité, Nicolas Turquet (DINUM) plaide pour un basculement vers une approche axée sur la planification stratégique par scénario plutôt que sur des fiches de postes figées : *« elle consiste à construire plusieurs futurs possibles, contrastés, et à identifier pour chacun les compétences qu'il faudrait pouvoir mobiliser »*. Appliquée à la fonction publique, cette méthode change la question posée à la gestion des ressources humaines : il ne s'agit plus seulement de recruter pour couvrir des besoins déjà identifiés, mais de se donner, en amont, la capacité de réagir vite quel que soit le scénario qui se réalise. Pour la filière numérique en particulier - où un choc technologique, une crise cyber ou une rupture réglementaire peuvent redéfinir en quelques mois les compétences critiques, l'intérêt d'une telle démarche est direct : *« elle offre un cadre pour anticiper l'incertitude elle-même, plutôt que de chercher, en vain, à la réduire »*.

Enfin, ce manque de lisibilité se double de blocages organisationnels dans la formation continue et la coopération entre grands acteurs. Si certaines entités internalisent leurs parcours de montée en compétences, les échanges transversaux restent rares. Dans le secteur public, la formation continue se heurte au refus de libérer du temps pour les agents. Aurélie Bauer et Claudia Miranda Pires (ANSSI) illustrent cette difficulté avec leur cursus d'experts : *« Nous le voyons très bien au sein de notre centre de formation, où nous proposons une formation d'expert en cybersécurité de niveau bac+5. Malgré la gratuité de cette formation pour tous les agents publics, nous peinons à la remplir, car elle dure un an. »*. Cette réticence est accentuée par un morcellement administratif et un manque de coordination. Le Colonel (COMCYBER) reconnaît ainsi qu'*« il n'y a pas de dialogue vraiment structuré pour partager l'état de nos besoins en termes de compétences fines »*, il formule également à ce sujet une forme d'autocritique : *« nous devons aussi, côté état-major, gagner en précision dans notre approche des compétences, des travaux sont par ailleurs en cours au sein du ministère »*

3. Répondre aux exigences du recrutement en valorisant la posture, les compétences relationnelles et la communication

Au-delà de la validation des compétences techniques, le marché exige désormais des qualités humaines et relationnelles indispensables sur le terrain. L'écosystème cyber restant un secteur restreint, le recrutement des profils pointus s'appuie fortement sur la cooptation et la reconnaissance entre pairs. Au CEA comme chez S3NS, on souligne ainsi l'importance des réseaux internes, des hackathons et des conférences spécialisées pour interagir avec d'autres experts et faire la preuve de ses compétences terrain. Pour autant, cette maîtrise technique ne suffit plus. Comme le rappelle le Colonel (COMCYBER), l'agilité et la curiosité constituent le premier socle recherché, une analyse partagée par Madame C. (Sopra Steria) qui place la posture et l'écoute au cœur des attentes.

Aurélie Bauer et Claudia Miranda Pires (ANSSI) constatent également une forte demande des ministères et des entreprises pour des formations axées sur la conduite de crise et le management, des rôles qui reposent avant tout sur des aptitudes humaines et d'accompagnement.

Enfin, la capacité à dialoguer avec la gouvernance et à adopter une vision stratégique devient un critère de sélection majeur. Les entreprises privilégient des profils capables d'articuler technique et décision politique ou économique. Comme le résume Florence Puybareau (Clusif), *« L'un des points importants, ce sont les softskills. Aujourd'hui, les entreprises recrutent moins [...] elles sont davantage en recherche de personnes qui ont un peu*

d'expérience technique, ou alors des profils transverses, qui vont pouvoir se former à la cyber mais possèdent les softskills pour s'adapter et parler à un comité exécutif ». Cette communication passe par un effort de simplification indispensable : Karine Béguin (Cyber'Occ) rappelle que *« si le technicien s'adresse au dirigeant avec un vocabulaire trop spécialisé, celui-ci décrochera rapidement »*. Face à l'obsolescence rapide des outils et à l'arrivée massive de l'IA, cette prise de hauteur s'appuie sur la capacité à apprendre en permanence.

B. Une nécessaire prise de conscience des dirigeants et des entreprises

1. Réveiller la gouvernance pour sortir de la passivité, de l'illusion de sécurité, et prendre conscience des risques

La prise de conscience du risque cyber par les dirigeants demeure freinée par un sentiment d'invulnérabilité et une perception purement comptable de la sécurité. Pourtant, cette prise de conscience des dirigeants faciliterait le déblocage de budgets et lorsque nécessaire, la montée en compétences des équipes. En effet, bien que les attaques fassent régulièrement la une des médias, les dirigeants de PME continuent d'y voir une menace distante. Comme l'observe Édouard Jeanson (Capgemini), *« Les écoles forment encore trop peu à ces enjeux, alors même qu'il ne se passe pratiquement pas une semaine sans qu'une cyberattaque fasse l'actualité. Malgré cette visibilité croissante, beaucoup continuent à penser que ces incidents n'arrivent qu'aux autres. »*. Les petites structures peinent à mesurer leur exposition réelle, estimant ne pas présenter d'intérêt pour les cybercriminels. Karine Béguin (Cyber'Occ) souligne cette fausse représentation : *« vous ouvrez les journaux, on ne parle que des gros groupes. Les petites structures se disent que ça ne peut pas leur arriver »*. Christian Tafani (Université Côte d'Azur) rappelle pourtant la vulnérabilité de ces acteurs face aux conséquences opérationnelles et financières d'un incident. La prévention reste ainsi perçue comme un coût facultatif, conduisant à l'absence d'outils de base : *« la cartographie des risques doit être la première chose à faire, mais ce n'est absolument pas le cas »*, déplore Florence Puybareau (Clusif).

Cette passivité contraint le secteur à s'en remettre à deux leviers réactifs : le choc d'une attaque ou la contrainte réglementaire. Édouard Jeanson (Capgemini) résume ce constat en expliquant que depuis vingt ans, le consensus est que l'évolution des entreprises est principalement stimulée par deux facteurs : une crise externe ou une obligation réglementaire.
Ce constat est partagé par Jérôme Champenois (Ovalt), qui note que la collaboration entre DSI et directions techniques ne s'amorce souvent qu'après un incident marquant ou lors d'une restructuration. De son côté, Marina Teller (Université Côte d'Azur) insiste sur la portée des cadres juridiques : *« Si l'on n'avait pas ces textes qui, à un moment donné, peuvent devenir punitifs et donner lieu à des sanctions, l'inertie serait bien plus lourde. L'alternative serait de laisser des acteurs privés développer leurs propres outils de régulation, ce qui ne me convient pas »*.

Enfin, cette acculturation est inégale sur le plan territorial et organisationnel. Le Général Franck Nicol (Sciences Po Rennes) rappelle que les dirigeants doivent appréhender le monde virtuel comme *« superposé au monde physique »*. Or, la sensibilisation souffre de déserts régionaux. Le secteur de la cybersécurité est directement touché par la diagonale du vide qui traverse la France, où la faible présence d'entreprises du numérique s'accompagne d'un déficit d'offre de formation. Comme en témoigne Madame E (Territoire Grand Nancy), cette fracture territoriale prive le tissu économique local des structures nécessaires à la sensibilisation et à la montée en maturité des dirigeants.

2. Sécuriser le terrain industriel et l'ensemble de la chaîne de valeur

La sécurisation de l'outil de production et de l'écosystème commercial constitue l'un des chantiers prioritaires de l'écosystème cyber. Le secteur industriel demeure un domaine très à la marge en raison de la technicité de ses besoins et de la rareté des compétences hybrides, exigeant à la fois des maîtrises informatiques et la compréhension des procédés opérationnels. Ce milieu est régi par des contraintes de production et des

temporalités particulières. Comme l'explique Jérôme Champenois (Ovalt), *« Les cycles de vie sont très longs. Généralement quand ils construisent une usine, les industriels achètent « les murs, les machines, l'informatique qui vient avec, et ils vont amortir cet investissement sur 20 ans […] contrairement à l'informatique de gestion où l'on a plus de facilité à faire évoluer les versions de nos logiciels, à les patcher et où les cycles d'amortissement sont plus court […]. Cette compréhension des cycles de vie industriels et des contraintes de production est essentielle »*. Il rappelle que *« l'on ne protège bien que ce qu'on connaît bien »*, plaidant pour des profils maîtrisant les architectures, interfaces et protocoles industriels (tels que la norme IEC 62443, bien moins enseignée que l'ISO 27001). Alors que la frontière entre informatique et automatisme s'estompe, les automaticiens n'ont pas été formés initialement à intégrer la sécurité, retardant la prise de conscience au sein des usines.

Ce virage sécuritaire est d'autant plus urgent qu'il conditionne la compétitivité des filières industrielles stratégiques à forte valeur d'exportation. Comme le souligne David Dutertre (Bretagne Commerce International BCI), les secteurs qui progressent le plus à l'export ne relèvent pas du numérique classique, mais d'équipements de haute technologie : *« Il serait judicieux de faire un parallèle entre les grands secteurs technologiques à l'export (spatial, composants électroniques et radio fréquences) avec les besoins de compétences en cybersécurité à venir. »* Sécuriser ces technologies de pointe face aux ingérences et à l'espionnage économique devient un impératif pour préserver leur positionnement international.

Enfin, cette démarche d'assainissement doit impérativement couvrir l'intégralité de la chaîne de valeur, sous peine de laisser des portes d'entrée béantes chez les sous-traitants et partenaires. Madame M. (Grand groupe international de services numériques) souligne la nécessité de faire de l'organisation un espace d'apprentissage collectif afin de pallier aux écarts de maturité entre acteurs d'un même écosystème : *« Il faut savoir parler à son public. Soit les personnes viennent du terrain, soit elles le côtoient au quotidien, et garantissent que ce qui va être réalisé et proposé ne tombe pas à côté. »*. La cybersécurisation de l'industrie implique ainsi d'élever simultanément le niveau d'exigence de l'ensemble des réseaux de partenaires et fournisseurs.

3. Inculquer une culture de souveraineté et réorienter les politiques d'achat

L'action stratégique des gouvernances doit intégrer les dimensions politiques, souveraines et comportementales de la sécurité numérique. Face au risque de dépendance envers les géants technologiques étrangers, l'autonomie stratégique s'impose comme un impératif pour l'écosystème. Le Colonel (COMCYBER) souligne que la posture des alliés historiques oblige à repenser le soutien technologique sur le long terme et incite à bâtir une souveraineté autonome. Cette démarche implique notamment d'affranchir les parcours d'excellence des cadres de certification internationaux : *« le COMCYBER pense aussi qu'il serait très judicieux de gagner en autonomie pour les compétences pointues »*. Pour devenir une puissance numérique, la souveraineté nationale doit s'appuyer sur un réseau élargi, capable de produire ses propres cadres de pensée et ses propres formations.

Cette volonté de souveraineté se heurte toutefois à des réalités économiques chez les acteurs privés et les collectivités. Florence Puybareau (Clusif) rappelle le coût d'opportunité d'une démarche souveraine pour le tissu économique : *« La dépendance aux solutions extra-européennes, notamment sur le cloud, est forte puisque 80 % de nos entreprises fonctionnent avec du cloud américain. Est il possible de tout basculer vers le cloud européen ? Non, d'abord parce que cela a un coût. Choisir une solution SecNumCloud, peut faire augmenter l'addition de 20 à 30% par rapport à certaines solutions extra-européennes. Et puis, il y a peut être un déficit de visibilité pour les solutions européennes moins connues que leurs concurrentes américaines. Quand vous êtes une PME, une ETI, ça vous fait réfléchir »*.

Cette prise de conscience pousse néanmoins les institutions à réinterroger leur doctrine d'équipement et d'achat. La dépendance envers les outils et cadres de pensée américains incite à développer des compétences propres, particulièrement dans les secteurs régaliens. Au sein du COMCYBER, le Colonel pointe la nécessité d'anticiper les évolutions géopolitiques : *« L'incertitude concernant le soutien américain à moyen et long terme nous amène à réévaluer notre dépendance. En réponse, des initiatives visant à renforcer notre souveraineté sont désormais menées au-delà du seul périmètre du ministère des Armées »*.

Pour sortir de cette dépendance, les décideurs politiques et économiques doivent privilégier le développement et le soutien à un écosystème souverain, même si cela implique des arbitrages financiers plus lourds ou des processus plus complexes. Comme le résume le Général Franck Nicol (Sciences Po Rennes), cela revient aussi à savoir parfois faire preuve de pragmatisme : plutôt que d'accepter une offre trop généreuse venue de l'étranger, il peut être préférable de privilégier des solutions locales, même si elles impliquent un léger surcoût et des normes de qualité différentes.

III. PROSPECTIVE : ANTICIPER LES RUPTURES ET ACCOMPAGNER LES MUTATIONS

Dans un contexte en évolution constante, les mutations technologiques et les cadres réglementaires ré-interrogent les conditions d'une transition maîtrisée. Cette partie s'attache à décrypter les dynamiques locales et les évolutions normatives qui façonnent les territoires, tout en évaluant comment les technologies émergentes transforment les métiers de demain. L'enjeu ? Identifier des leviers d'action pour transformer ces bouleversements en opportunités.

A. Réglementation et dynamiques territoriales

1. Accompagner la poussée réglementaire européenne pour transformer l'obligation de conformité en un levier d'action

Les nouvelles directives européennes transforment la cybersécurité en une obligation légale, restructurant le marché et créant d'importants besoins en gestion des risques et conformité. Comme le soulignent Aurélie Bauer et Claudia Miranda Pires (ANSSI), *« Dans la directive NIS2, les obligations réglementaires passent, dans sa première version, de quelques centaines d'entités à plusieurs dizaines de milliers dans la seconde version. […] » Il y a donc une prise de conscience de ces entités, qui comprennent désormais la nécessité d'intégrer la cybersécurité et, donc, de former des gens en interne pour répondre aux exigences réglementaires ».*

L'arrivée de NIS 2 va permettre aux entreprises industrielles de repenser leur respect et leur conformité à ces nouvelles réglementations. Cela représente l'opportunité de faire de la pédagogie sur les normes spécifiques à l'industrie et de mettre en lumière le manque de compétences dans ce domaine. Comme le rappelle Jérôme Champenois (Ovalt), *« tout le monde connaît ISO 27001, par contre on parle très peu des normes de sécurité des SI industriels ».* Il y a ainsi un vrai enjeu d'appropriation de ces nouvelles réglementations par les entreprises pour les obliger à s'améliorer dans leur maturité cyber.

Toutefois, ce virage réglementaire se heurte à une lourdeur bureaucratique et à un manque de clarté opérationnelle *« La bureaucratie qu'on peut avoir en France sur d'autres sujets nous a rattrapé dans la cyber »* déclare Edouard Jeanson. Cette complexité perturbe les petites structures qui peinent déjà à assimiler les cadres existants. Karine Béguin (Cyber'Occ) constate cette saturation : *« quand on parle de NIS2, il y en a beaucoup qui me regardent en disant c'est quoi NIS2 ? […] Les entreprises, des petites et moyennes, sont déjà noyées par les normes européennes. Le RGPD, ça fait plusieurs années qu'il est en place, et il y a encore à ce jour des entreprises qui disent mais c'est quoi le RGPD ? ».*

Face à ces blocages, l'imposition de normes avec une sanction financière en cas de non respect montre ses limites en l'absence d'accompagnement et de pédagogie. *« le déploiement de normes structurantes, telles que la directive NIS2, est perçu comme un ensemble de contraintes formelles et d'objectifs chiffrés dont le sens profond n'est pas toujours explicite. Ce formalisme risque de limiter l'appropriation active du sujet par les acteurs, incitant les entreprises à s'en tenir à une logique de conformité administrative vis-à-vis de l'ANSSI,*

plutôt qu'à appréhender le cyberespace comme un environnement dynamique en constante évolution. », déclare le Général Franck Nicol. Ce manque de préparation et de compréhension ralentit la concrétisation des projets sur le terrain. Madame C. (Sopra Steria) observe ainsi que si la montée en puissance de ces sujets exige une double compétence technique et juridique, l'impact réel sur le marché reste plus lent que prévu : *« on commence à avoir des demandes qui émergent, mais un petit peu moins vite qu'on le pensait. Je pense plutôt que c'est en 2027 qu'on aura un gros boom »*.

2. Renforcer le maillage des compétences et l'accompagnement des territoires

L'analyse du maillage territorial fait apparaître de fortes inégalités dans l'accès aux formations et aux expertises cyber, directement calquées sur la répartition des acteurs économiques du numérique. Le secteur est touché par une fracture géographique où des pans entiers du territoire restent hors des réseaux d'acculturation. Comme l'explique Madame E (Territoire Grand Nancy), *« Notre marché compte relativement peu de grands acteurs spécialisés dans les services numériques et très peu d'entreprises dont l'activité est exclusivement consacrée à la cybersécurité. La majorité des recrutements provient plutôt de DSI des secteurs utilisateurs, qui doivent avant tout sécuriser leurs propres systèmes et activités. »*. Cette configuration a une incidence directe sur la nature des formations et emplois proposés à échelle territoriale. Les postes entièrement consacrés à la cybersécurité restent relativement rares. Dans de nombreuses organisations, notamment les structures de petite ou moyenne taille, les missions de cybersécurité sont intégrées à des fonctions informatiques plus larges, cette dynamique se retrouve également dans le secteur de la formation.

Loin des grandes métropoles qui concentrent les pure players et les ESN, les territoires ruraux ou les villes de taille intermédiaire reposent quasi exclusivement sur des « secteurs utilisateurs » (collectivités, hôpitaux, PME). Dans ces zones, le marché ne recherche pas des spécialistes pointus, mais des profils polyvalents capables d'assurer des fonctions IT classiques et des missions de sécurité. *« Les offres d'emploi correspondant à des postes exclusivement consacrés à la cybersécurité restent peu nombreuses. Dans beaucoup d'organisations, les missions de cybersécurité sont associées à d'autres responsabilités, avec une recherche importante de profils polyvalents. »*, précise Madame E (Territoire Grand Nancy).

Face à cette situation et à l'éloignement des agences nationales comme l'ANSSI, perçues comme distantes par les petites structures, la sensibilisation repose sur des initiatives de proximité. Pour Karine Béguin (Cyber'Occ), l'action de terrain d'acteurs comme la gendarmerie s'avère décisive : *« vous parlez à une TPE/PME […], vous leur parlez de l'ANSSI, ils vont vous dire : c'est quoi l'ANSSI ? […] Je pense que ce contact de la gendarmerie, au niveau rural, ça peut permettre aux entreprises de comprendre et de s'approprier les dispositifs qu'ils ne connaîtraient pas sans ce contact physique »*.

B. L'impact des technologies émergentes sur les métiers de demain

La transition vers les technologies de rupture redéfinit en profondeur le secteur de la cybersécurité. Comme le souligne le Général Franck Nicol, *« la matière évolue tellement vite, elle est immatérielle (quantique, IA…), on est dans des champs assez incroyables, on est dans une révolution dans les métiers avec des conséquences qu'on ne mesure pas »*. Cette accélération modifie autant les vecteurs d'attaque que les moyens de défense et les compétences requises sur le terrain.

1. L'intelligence artificielle : un domaine à structurer

L'intelligence artificielle s'impose comme un sujet prioritaire mais marqué par des niveaux de maturité très hétéroclites et une absence de cadre stabilisé. Nicolas Turquet (DINUM) observe que *« Deux domaines cristallisent aujourd'hui l'essentiel des tensions : la cybersécurité, dont l'acuité s'est trouvée renforcée par les incidents récents, et l'intelligence artificielle, devenue en peu de temps un sujet politique de premier plan, porté*

directement par les cabinets ministériels ». Cependant, l'intégration concrète reste inégale. Madame E (Territoire Grand Nancy) note que « *Nous n'arrivons pas encore à mesurer avec précision les besoins liés à l'intelligence artificielle. Le sujet est très présent dans les discours et les réflexions prospectives, mais il ne se traduit pas encore partout par des usages concrets.* ». Dans le secteur industriel, cette adoption précoce sans recul pose d'ailleurs des défis de compétences et de contrôle : Jérôme Champenois (Ovalt) rapporte avoir eu « *un problème en production sur une ligne, sur un bout de code qui avait été généré par IA et qui n'avait pas été bien compris par le développeur* », s'interrogeant sur la capacité des futurs experts à challenger ces outils s'ils s'y reposent dès leur sortie d'école. Pour Romain Bréchet (S3NS), l'enjeu réside dans une adaptation pragmatique : « *Tous les métiers que nous connaissons aujourd'hui vont devoir s'adapter et intégrer l'IA. […] Celle-ci répondra à un besoin d'efficacité, mais n'a pas vocation, dans notre vision, à remplacer les compétences humaines* » ; il ajoute que « *Nous sommes encore au début de la courbe d'apprentissage. […] Nous devons apprendre à travailler avec ces nouveaux outils et à en maîtriser les usages* »

Cette mutation accélère l'automatisation des opérations et la réorganisation des équipes cyber pour faire face à la sophistication des attaques informatiques. Comme le résume le Colonel (COMCYBER), « *Aujourd'hui avec le domaine de l'IA on se rend compte qu'on va devoir accélérer, pour intégrer ces nouvelles capacités dans la cyber* ». Pour opérationnaliser cette vision, la stratégie consiste à diffuser cette expertise au plus près des équipes opérationnelles du ministère : « il y a ce besoin de mettre des « *sachants* » au plus proche des métiers ». Florence Puybareau (Clusif) anticipe également cette redistribution des cartes. Pour elle, l'intégration généralisée de l'intelligence artificielle dans les outils de supervision transforme radicalement les centres opérationnels de sécurité (SOC). Les tâches d'entrée de gamme, autrefois dévolues aux profils juniors pour l'analyse humaine des alertes de premier niveau, sont désormais automatisées. Le besoin se déplace vers des compétences d'analyse plus complexes.

Cette dynamique impose une hybridation rapide des compétences et un rapprochement étroit avec les métiers de la donnée. Aurélie Bauer et Claudia Miranda Pires (ANSSI) identifient trois piliers majeurs : comprendre si l'IA aide les attaquants, l'utiliser pour mieux défendre, et apprendre à sécuriser l'IA elle-même. Pour soutenir cette ambition, le Colonel (COMCYBER) mise sur l'acculturation de profils de data scientists : « *Face à la généralisation des compétences data, le COMCYBER devra recruter des profils polyvalents qu'il conviendra de spécialiser a posteriori. Cette évolution, qui s'annonce croissante, constituera un défi majeur en raison de la concurrence accrue pour ces talents.* ». Le Général Franck Nicol (Sciences Po Rennes) insiste sur cette synergie stratégique d'allier l'IA à la cyber.

Enfin, l'IA doit être appréhendée et protégée comme une infrastructure critique à part entière. Romain Bréchet (S3NS) rappelle que « *L'IA est un outil, mais c'est aussi une infrastructure […] Nous protégeons nos applications ; nous devons appliquer le même niveau d'exigence aux systèmes d'IA, qui introduisent eux aussi de nouveaux risques* ». Cette sécurisation exige une vigilance accrue sur la fuite et la souveraineté des données traitées. Comme le met en garde le Général Franck Nicol (Sciences Po Rennes), la question des données utilisées dans l'IA doit être prise en compte, ce n'est pas parce que c'est invisible que les données restent au même endroit et ne sont pas exploitées par d'autres ensuite.

2. Engager le virage du post-quantique et anticiper les risques

La transition vers la cryptographie post-quantique (PQC) représente un enjeu technologique majeur, marqué par un contraste saisissant entre l'urgence identifiée par les autorités et la réalité opérationnelle des entreprises. Face à la menace future de l'ordinateur quantique sur les algorithmes de chiffrement actuels, les instances nationales demandent[4] d'anticiper la migration. Comme le rappellent Aurélie Bauer et Claudia Miranda Pires (ANSSI), « *Les entreprises aujourd'hui doivent toutes passer, ou a minima réfléchir, à la transition post-quantique. L'ANSSI demande que les gens utilisent de l'hybridation, c'est-à-dire un mélange de cryptographie classique et de cryptographie post-quantique.* ». Pourtant, hors du premier cercle institutionnel, la maturité globale reste très

4 https://messervices.cyber.gouv.fr/guides/en-anssi-views-post-quantum-cryptography-transition

faible et la démarche concrète est encore largement différée. Madame E (Territoire Grand Nancy) illustre cette mise à distance par le tissu économique local : « *La cryptographie post-quantique est aujourd'hui principalement portée par les acteurs de la recherche et de l'expertise technologique. Ce n'est pas un sujet qui remonte jusqu'à nous depuis les entreprises.* ».

Cette situation crée un fossé entre une poignée de pionniers ultra-spécialisés et un déficit généralisé de formations dédiées sur ce domaine très précis. Quelques acteurs de pointe et organismes de recherche ont déjà pleinement intégré ce virage dans leurs environnements. C'est le cas au CEA (Stéphanie Beheydt et Estel Chiron), « *complètement impliqué* » sur ces sujets, ou chez S3NS ou la cryptographie post-quantique fait déjà l'objet de travaux concrets, en s'appuyant notamment sur les avancées technologiques disponibles dans l'écosystème Google Cloud. Cependant, ces initiatives privées ou de recherche de pointe ne s'accompagnent pas encore de cursus académiques structurés à grande échelle pour former les futurs ingénieurs à ces nouvelles normes cryptographiques. Romain Bréchet rappelle en ce sens que « *Une part importante des incidents de sécurité dans le cloud est liée à des erreurs de configuration plutôt qu'à l'exploitation de vulnérabilités inédites. La formation sur ce volet doit encore progresser.* »

Face à ce constat, l'urgence impose d'initier des travaux de prospective, notamment sur le plan juridique et financier. Marina Teller (Université Côte d'Azur) souligne la nécessité de devancer les ruptures d'infrastructures stratégiques : « *on a commencé à essayer de se projeter, de faire un exercice de prospection juridique, pour imaginer ce qui peut se passer pour le secteur financier mondial, si l'ordinateur quantique permettait par exemple de hacker une blockchain telle que Bitcoin* ». Elle précise toutefois la portée encore isolée de ces travaux : « *ça tient beaucoup à ma démarche à moi en tant qu'enseignante-chercheuse* ». Sans un effort d'acculturation et une véritable structuration des formations, le passage à la cryptographie post-quantique risque de devenir un goulot d'étranglement majeur lors des prochaines échéances de sécurité.

3. Garantir la souveraineté des infrastructures cloud : freins géopolitiques, disparités territoriales et réalités de recrutement

Le Cloud est un sujet important des entreprises actuellement. Il y a une vraie prise de conscience des risques d'ingérence. Cette réalité s'observe directement sur le terrain local ; pour Madame E (Territoire Grand Nancy), les entreprises locales n'ont pour l'instant pas engagé de réflexion structurée sur le sujet. Ce décalage illustre un temps d'appropriation encore nécessaire entre les capacités de recherche académique et leur diffusion vers les entreprises utilisatrices, notamment les structures les plus petites, moins directement connectées aux centres de recherche que les grands comptes. En effet les compétences et l'intérêt pour ces infrastructures souveraines souffrent d'un partage géospatial inégal, directement calqué sur la faible densité des acteurs du numérique hors des grandes métropoles.

Cette faible adoption du Cloud souverain est encore plus marquée dans le secteur industriel, qui privilégie la souveraineté physique de ses machines. Comme l'analyse Jérôme Champenois (Ovalt), « *Les industriels aiment bien avoir leurs solutions informatiques proches de leurs machines pour se prémunir de problématique de connexion externe et garantir un fonctionnement autonome de leur installation. L'externalisation n'est pas encore un sujet* ». Dès lors, plutôt que de viser une souveraineté technologique intégrale souvent inatteignable, la stratégie des organisations s'oriente vers la protection granulaire de leurs actifs critiques chez les hébergeurs majeurs. Édouard Jeanson (Capgemini) explicite cette posture pragmatique ; pour lui, il n'y a pas de difficulté à effectuer son hébergement sur Microsoft Cloud pour ses données. L'enjeu porte sur le type de données à y stocker et les mesures de protection à mettre en œuvre. En effet, avec un chiffrement des données et la maîtrise de sa clé, les technologies actuelles permettent de sécuriser l'ensemble des flux, même lorsque l'infrastructure est externalisée chez Microsoft.

Pour répondre aux besoins de l'hybridation et à l'ouverture croissante des environnements de travail, les architectures de sécurité évoluent vers une adoption massive du modèle Zero Trust. Comme l'indique Edouard Jeanson (Capgemini) cette approche implique que les collaborateurs, qu'ils travaillent depuis leur domicile, les

locaux de l'entreprise ou ailleurs, doivent systématiquement se connecter dans un cadre sécurisé.

Cette transformation des infrastructures redistribue les exigences du marché de l'emploi : les grandes structures ne font pas tant face à une pénurie sèche de compétences qu'à un allongement des délais de recrutement pour dénicher des architectes capables de concevoir ces environnements distribués et sécurisés de bout en bout.

CONCLUSION

La première étude de l'Observatoire nous a permis de mettre en lumière et d'analyser les différentes enquêtes existantes. Nous avons notamment constaté que le marché de l'emploi en cybersécurité commence à se tendre outre-Atlantique, mais cette tension commence également à se faire sentir sur le territoire français. Cela se manifeste notamment par la difficulté croissante des jeunes à trouver des lieux de stage ou d'alternance, mais aussi par la désaffection des profils juniors au profit des profils plus expérimentés.

Cette seconde étude s'est appuyée sur les regards croisés de 17 professionnels du secteur, aux profils variés tant en termes d'expérience que d'environnements, répartis sur l'ensemble du territoire. Cette diversité nous a permis de confronter les perceptions, les pratiques et les préoccupations de professionnels qui ne vivent pas nécessairement les mêmes réalités, mais qui sont tous directement confrontés aux transformations du secteur. Notre postulat de départ était qu'il est impossible de prédire avec certitude à quoi ressemblera l'avenir de la cybersécurité. Pour autant, les similitudes qui émergent de l'analyse de ces 17 entretiens sont suffisamment nombreuses pour révéler des tendances communes. Sans prétendre prédire les compétences de demain, elles permettent d'identifier des signaux forts, des tensions et des enjeux structurants, qui pourraient annoncer les besoins à venir.

Au-delà de cette complexité croissante à anticiper ou à planifier les montées en compétences, de vraies questions se posent : comment intégrer les juniors, à l'ère de l'IA, pour qu'ils deviennent un jour les seniors dont on a tant besoin aujourd'hui ? Comment s'adapter collectivement aux nouvelles technologies, qui accélèrent encore le rythme des adaptations nécessaires et l'intensité du travail ? Comment les écoles et universités adaptent-elles leurs programmes de formation ? Enfin, une question traverse l'ensemble de ces enjeux : comment faire évoluer collectivement l'écosystème de la cybersécurité pour que l'offre de compétences suive le rythme des transformations des besoins ?

Cette étude qualitative constitue une première cartographie des transformations à l'œuvre et des signaux qu'il nous semble important d'approfondir. La prochaine étape consistera donc à passer de ces perceptions et signaux qualitatifs à une mesure plus objective des besoins. Quelle est l'ampleur de ces transformations ? Quels métiers sont réellement concernés ? Quelles compétences évoluent, émergent ou gagnent en importance ? À quel rythme ? Et comment ces besoins se répartissent-ils selon les territoires, les secteurs et les niveaux d'expérience ?

C'est la raison pour laquelle notre prochaine étude sera cette fois quantitative. Elle permettra de mesurer et d'objectiver les tendances identifiées lors de cette première phase, afin de mieux comprendre l'évolution des besoins en compétences et en emplois dans la cybersécurité, et surtout de contribuer à éclairer les décisions qui devront être prises pour y répondre.



02

FEUILLE DE ROUTE OBSERVATOIRE

- THÈME FORMATION INITIALE
- THÈME SOFT SKILLS
- THÈME FORMATION CONTINUE / TOUT AU LONG DE LA VIE
- THÈME RH / GPEC
- THÈME FAIRE RAYONNER LA CYBER
- THÈME MANAGEMENT DES ENTREPRISES
- THÈME DIRIGEANTS D'ENTREPRISES
- THÈME SENSIBILISATION
- THÈME RELATION ÉCOLES /UNIVERSITÉS AVEC LES ENTREPRISES

L'objectif est d'ici de faire une synthèse de toutes les propositions qui ont pu émerger à un moment ou à un autre au cours des entretiens menés, et ceci de manière anonyme. Il n'est pas question de faire un tri entres celles qui nous semblent intéressantes et les autres, mais plutôt d'alimenter un débat et une réflexion collective sur les actions qui ont du sens et qui semblent pertinentes.

Toutes ces idées ont donc vocation à être débattues à divers niveaux. Les propositions liées à une refonte des programme de formation initiale intéressent en premier lieu les écoles et universités : charge à eux de les trier et d'en garder certaines. Quant à celles qui concernent la vie des entreprises, c'est à elles de décider les choix à effectuer.
L'AMI CMA Cyberskills4all, à travers cet observatoire, fonctionne comme un incubateur à idées, mais toutes ne sont pas forcément bonnes à prendre. Il est de la responsabilité de chacun de faire sa part du chemin.
Pour une meilleure lecture de ces idées, nous allons tout de même les présenter par thématiques.

Thème formation initiale :

- **Créer des possibilités de doubles diplômes** : techno stratège, ingénieur commercial, ingénieur juriste, technique et géopolitique… Qui sauront plus aisément comprendre la cybersécurité dans toute sa complexité.
- **Repenser les contenus de formations** en les orientant vers les métiers, plutôt que de les focaliser sur les technologies à la mode qui peuvent s'avérer très vite obsolètes. Un besoin de spécialisation plus tôt dans les cursus, non pas sur une technique donnée, mais sur un métier ou un segment de la posture cyber (défense, gouvernance, réponse à incident, rétro-ingénierie).
- **Créer des passerelles** avec des instituts de sciences politiques, intelligences économiques, géopolitique, stratégie pour développer les doubles compétences.
- **Créer des parcours à la croisée entre cyber et automatisme** pour répondre aux enjeux de la cybersécurité industrielle.
- **Refondre les programmes techniques :**
  - Passer de l'approche défensive à une approche hybride offensive/défensive (comprendre l'attaque pour anticiper la défense)
  - Intégrer l'IA en tête de gondole (modules obligatoires IA + cyber, prompt engineering cyber, défense contre les agents IA)
  - Ouvrir les disciplines aux sciences humaines (éthique, philosophie de la donnée, anthropologie du numérique)
  - Réintroduire les compétences réseau fondamentales (basses couches, protocoles Internet) et l'utilisation des commandes Unix.
  - Privilégier l'enseignement des concepts d'architecture globale (IAM, organisation d'un SOC) plutôt que l'apprentissage des outils spécifiques soumis à l'obsolescence.
  - Penser un parcours avec une spécialité Architecte logiciel et réseau.

- **Financer et imposer des fablabs et des incubateurs** au sein des écoles pour que les étudiants et chercheurs puissent tester des attaques/défenses en temps réel sur des jumeaux numériques en code open source.
- **Intégrer une connaissance approfondie** des principes fondamentaux, de l'histoire des technologies et des mécanismes qui ont conduit aux architectures actuelles. Comprendre les origines d'une discipline pour mieux appréhender les évolutions futures.
- **Réintégrer de la culture générale** et de la culture de l'environnement cyber comme moyen de mieux appréhender ensuite la complexité. Réintroduire la culture de l'interdisciplinarité.
- **Développer le sens critique des étudiants** : leur apprendre à construire un raisonnement, à confronter des points de vue, à distinguer les faits des opinions et à exercer leur libre arbitre. La philosophie, la géopolitique, l'histoire et les sciences humaines permettent de développer l'ouverture d'esprit, l'empathie, la capacité à comprendre des logiques culturelles différentes ainsi que le recul indispensable face à la complexité.
- **Donner aux étudiants les outils** qui leur permettront de valoriser leurs compétences et de construire

progressivement leur projet professionnel (CV recherche de stages…)

- **Réintroduire la culture de l'entreprise** et la culture managériale dans les formations, ainsi que l'écosystème cyber.
- **Corréler refonte des programmes** au même rythme que l'accélération des technologies.
- **Sensibiliser tous les masters de droit** aux risques cyber pour pouvoir ensuite irriguer tous les secteurs d'activités.
- **Inscrire un module cyber** dans chaque référentiel de formation (fiches RNCP), quel que soit le métier visé, plutôt que de réserver ce sujet aux seules filières numériques.
- **Repenser l'approche pédagogique** : diminuer les cours magistraux et théoriques, au profit de mise en situations pratiques concrètes.
- **Arrêter de chercher une employabilité immédiate** et spécialisée au profit d'une approche académique plus durable et donc avec des profils plus adaptables aux évolutions technologiques.
- **Imaginer un cursus de formation spécifique à la L2I** (Lutte informatique d'influence) en ouvrant à des compétences hybrides alliant les sciences comportementales, la psychologie et le marketing social capables d'analyser l'impact des outils numériques à la fois sur la psychologie individuelle et sur les dynamiques de groupe.
- **Intégrer les compétences liées à l'IA agentique** appliquée à la détection de menaces.
- **Créer des doubles diplômes cyber et IA :** profils encore très rares et donc très recherchés.
- **Former des étudiants** dotés d'une compréhension globale de l'infrastructure et de la chaîne de détection : il faut des profils polyvalents capables de dialoguer avec des équipes projets, de travailler sur l'architecture, de créer des règles de corrélation et, si besoin, de faire du forensic… Des personnes avec une vision et une connaissance globale pour mettre du liant entre experts et faire en sorte qu'ils se comprennent.

Thème Soft Skills :

- **Réintroduire des connaissances de français** : une meilleure maîtrise de la langue.
- **Développer les qualités rédactionnelles**, l'esprit de synthèse et la culture générale, qui constituent désormais des compétences professionnelles à part entière.
- **Développer les compétences en communication** : parler à un client, à un Comité Exécutif, dialoguer avec un non expert…
- **Développer les compétences d'Empathie** : être capable de se mettre à la place de l'autre et de comprendre ses réactions : utile pour mieux sensibiliser aux risques cyber.
- **Développer l'adaptabilité et l'aptitude à apprendre** en continu qui est décisive pour la suite des carrières, notamment face à l'arrivée de l'IA.

Thème formation continue / tout au long de la vie :

- **Sélectionner des profils ingénieurs** à fort potentiel et une appétence pour la stratégie après quelques années ou en fin de cursus, et les former à la stratégie cyber.
- **Développer les contenus de formations** permettant des passerelles entre automatisme et cybersécurité : le monde de l'industrie a besoin de ces doubles compétences. Intégrer des modules sur les normes de la sécurité industrielle.
- **Revoir la stratégie de formation** des experts en cyber pour aller vers plus d'autonomie stratégique en matière de formation mais également de référentiel d'emploi, de compétences ou des outils utilisés mais également des référentiels des menaces. Aujourd'hui, l'enjeu est de construire un savoir faire européen en la matière, y compris pour nos forces armées.
- **Les besoins de recrutement évoluent** : La difficulté porte actuellement sur les profils seniors capables de conjuguer expertise technique et compétences managériales, un double profil nécessaire à l'accompagnement des équipes plus juniors et jugé rare sur le marché. Il serait ainsi intéressant de créer des parcours de type MBA pour former ces experts techniques qui ont quelques années d'expérience vers le management, pour combler ce besoin.

Thème RH / GPEC :

- **Passer d'une logique de métiers détaillés à une logique de montée en macro-compétence**, changer le paradigme de la Gestion Prévisionnelle des Emplois et des Compétences. Simplifier l'ensemble des familles de métiers pour faciliter les passerelles professionnelles et l'upskilling des professionnels en poste.
- **Réactualiser régulièrement les référentiels de compétences** pour parler le même langage.
- **Changer la GPEC traditionnelle** pour mettre en place un projet de planification stratégique par scénarios à la manière de l'OCDE : c'est une manière de se préparer à l'incertitude.
- **Repenser la pyramide des ages** au sein des organisations pour intégrer les juniors de manière plus efficace (avec un senior en rôle de mentorat par exemple).
- **Penser la souveraineté des données de nos apprenants** : il faut parfois ré-internaliser certaines compétences clefs pour éviter d'envoyer nos experts se former dans des organismes de formations non souverains, au risque qu'ils soient débauchés.
- **Mieux sensibiliser les RH**, notamment des structures plus petites, sur les métiers cyber pour avoir des fiches de postes plus détaillées et mieux ciblées : ce qui incitera les professionnels à postuler à des offres mieux détaillées.
- **Promouvoir les dispositifs de formation** continue existants et appuyer auprès du management pour faire en sorte que les experts ou les interlocuteurs cyber soient libérés pour se former plus régulièrement : en particulier sur la partie fonction publique / étatique où il est parfois difficile de libérer les professionnels pour qu'ils se forment.
- **Repenser les cycles d'évaluations des compétences**. Si on le fait sur un an, les compétences, notamment en IA, sont déjà obsolètes. Penser un modèle plus dynamique avec des cycles plus courts.
- **Constituer des équipes de formateurs** au sein des entreprises qui viennent du terrain et qui ont encore un pied dedans pour s'assurer que les contenus de formations soient en adéquations avec les besoins et avec les évolutions technologiques. Ou alors il faut mobiliser les collaborateurs déjà experts sur un sujet comme ambassadeurs internes pour un échange entre pairs favorisant la montée en compétences.

Thème Faire rayonner la cyber :

- **Cibler 10 à 15 % des dirigeants** (PME/ETI) ayant déjà une appétence pour le numérique ou utilisant des technologies avancées (IA, jumeaux numériques), travailler avec eux pour co-construire des cas d'usage réels, sécuriser leurs flux, modéliser leurs risques, puis utiliser ces 10 à 15 % comme des ambassadeurs qui incarnent la réussite. Leur retour d'expérience servira à convaincre le reste des dirigeants par capillarité.

Thème Management des entreprises :

- **Reformer la structure managériale** pour l'intégration les juniors :
  - Abandonner les modèles d'encadrement reposant sur des profils purement autonomes à plein temps.
  - Déployer un modèle d'équipe pyramidale partagé : un profil senior (directeur de mission) supervise à temps partiel des chefs de projet intermédiaires, qui encadrent directement des juniors sur des missions d'investigation.

- **Palier l'absence de maître de stages** dans les petites structures :
  - Création d'un système de tutorat externe triangulaire : étudier la faisabilité d'associer un étudiant, une PME et un expert externe (RSSI à la retraite sous accord de non-divulgation par exemple) assurant la fonction de tuteur académique et opérationnel

- **Diffuser le savoir** (notamment en matière d'IA ou de bases de données) au plus près des métiers opérationnels, en particulier pour les Ministères pour pouvoir accélérer l'intégration de ces nouvelles capacités en cyber.

Thème Dirigeants d'entreprises :

- **Déployer des exercices de crise obligatoires** : transposer le modèle des exercices incendie aux risques cyber pour les dirigeants de PME, afin de leur enseigner de manière pratique les réflexes de base et la gestion de crise, tout en leur démontrant le retour sur investissement de cette démarche
- **Vulgariser les outils étatiques gratuits** (ex mon aide cyber) en allant à la rencontre des TPE/PME : Renforcement du maillage territorial et du contact physique : réactiver ou s'inspirer des initiatives de contact direct (comme les anciens référents cyber régionaux de la gendarmerie ou les CCI), en s'appuyant sur les brigades locales pour aller à la rencontre physique des patrons de TPE-PME.
- **Développer la culture du risque cyber** chez les dirigeants d'entreprise.
- **Intégrer l'approche par les risques** dans sa gestion de la cyber : commencer par faire une cartographie de son SI.
- **Réévaluer sa dépendance** vis-à-vis des technologies étrangères pour gagner en autonomie stratégique et réduire cette dépendance dans la mesure du possible. Cela concerne les entreprises mais également les institutions publiques quelles qu'elles soient.

Thème Sensibilisation :

- **Sensibiliser les jeunes générations** de manière systématique.
- **Évolution des outils scolaires de certification** : intégrer un vrai module cybersécurité au sein de la plateforme PIX afin de sensibiliser et d'ancrer les bons réflexes dès le collège et le lycée. Réfléchir à un permis de naviguer sur internet, comme il existe un permis de conduire.
- **Sensibiliser tous les agents publics** aux risques cyber ou à la cyber d'une manière générale (pas uniquement les équipes techniques).

Thème Relation écoles /universités avec les entreprises :

- **Créer un dialogue régulier** entre les organismes de formations et les acteurs économiques afin de mieux identifier les compétences émergentes et les besoins des organisations.
- **Mieux partager les besoins** entre écoles/universités et organisme étatiques pour avoir des jeunes opérationnels plus vite. Utiliser les intermédiaires, comme le Pôle d'Excellence Cyber, pour faciliter cette mise en relation et remontée de besoins : une sorte de courroie de transmission entre deux mondes.


03

SYNTHÈSE DES INTERVIEWS RÉALISÉES

- AMIAD (AGENCE MINISTÉRIELLE POUR L'INTELLIGENCE ARTIFICIELLE DE DÉFENSE)
- ANSSI – AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
- BCI - BRETAGNE COMMERCE INTERNATIONAL
- CAPGEMINI
- CEA – COMMISSARIAT À L'ÉNERGIE ATOMIQUE ET AUX ÉNERGIES ALTERNATIVES
- CLUSIF
- COMCYBER
- CYBER'OCC
- DINUM–DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE
- TERRITOIRE GRAND NANCY
- GRAND GROUPE INTERNATIONAL DE SERVICES NUMÉRIQUES
- OVALT GROUP
- SCIENCES PO RENNES
- S3NS (THALÈS)
- SOPRASTERIA
- UNIVERSITÉ CÔTE D'AZUR

AMIAD (AGENCE MINISTÉRIELLE POUR L'INTELLIGENCE ARTIFICIELLE DE DÉFENSE)

1. Un recentrage vers les profils seniors et expérimenté

1.1 Alignement des profils des candidats avec les besoins réels

L'AMIAD reçoit majoritairement des candidatures de profils juniors ou avec peu d'expérience, sachant que ses besoins se portent aujourd'hui sur des profils plus expérimentés, y compris via la reconversion professionnelle.

« Actuellement, nous avons beaucoup de candidats juniors ou peu expérimentés qui postulent sur nos offres, avec l'évolution de nos projets et de nos besoins, nous notre cœur de cible ça va plutôt être des seniors voire des experts ».

Ce repositionnement fait suite à un premier cycle de recrutements plus orientés juniors, qui a mis en évidence un besoin complémentaire d'expertise technique plus affirmée et plus polyvalente : *« on a recruté l'année dernière en grande majorité des juniors, et on se rend compte qu'on a aussi besoin d'un certain niveau d'expertise, et peut-être pas seulement sur une seule technologie ».*

1.2 Un lien avec les écoles en développement

La structuration d'un réseau d'écoles partenaires est en cours afin de promouvoir la filière de l'intelligence artificielle de défense, le recrutement effectif passant davantage par la publication d'offres et la chasse directe de profils. Cela s'explique notamment par la création récente de l'AMIAD (2024).

« Il y a plusieurs écoles qui ont été identifiées, la feuille de route école a été validée il y a peu de temps [...] il n'y a encore rien de formalisé à ce jour, les premières actions sont prévues à l'automne 2026 ».

Concernant les canaux de recrutement effectifs : *« c'est plutôt en publiant sur nos différentes plateformes, et en faisant de la chasse ».*

2. Les compétences ciblées : la cybersécurité et le développement de modèles IA alliées à un parcours d'intégration externe.

2.1 Deux axes de compétences techniques prioritaires

Les compétences critiques recherchées se concentrent sur la cybersécurité et le développement de modèles d'intelligence artificielle, avec quelques éléments de granularité apportés côté développement : bonnes pratiques de développement sécurisé, analyse de vulnérabilités, et mise en œuvre de chaînes CI/CD sécurisées[5].

5 La sécurité CI/CD désigne l'ensemble des pratiques, outils et politiques visant à protéger le pipeline d'intégration et de livraison continues (CI/CD) contre les menaces tout au long du cycle de développement logiciel. Elle garantit l'intégrité, la sécurité et la fiabilité des modifications de code, du développement initial au déploiement en production.

2.2 La complémentarité des parcours d'intégration internes et des dispositifs de formation

Les nouvelles recrues bénéficient d'un cycle d'acculturation d'environ un mois à l'arrivée, complété si besoin par des formations internes ou externes. Les agents ont également la possibilité de consacrer 20% de leur temps de travail pour explorer de nouveaux sujets, s'ouvrir à d'autres thématiques, une opportunité pour se tenir à jour au fil du temps.

Le plan de formation 2026 couvre un périmètre technique large, allant de l'IA (deep learning, fine-tuning de LLMs, prompt engineering) aux systèmes embarqués et à la conduite de projets informatiques.

ANSSI – AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



AURÉLIE BAUER
Cheffe du CFSSI
Division CFSSI
Sous-direction SDE



CLAUDIA MIRANDA PIRES
Responsable de labellisation des formations continues
ANSSI/CFSSI

1. Évolution du marché du recrutement et difficultés d'identification des compétences

1.1 Une méconnaissance des métiers cyber qui complexifie la compréhension du besoin.

L'analyse des offres d'emploi met en lumière une méconnaissance des recruteurs non spécialisés face aux besoins en cybersécurité. Beaucoup d'entre eux recherchent un *« ingénieur cyber »*, or ce terme désigne un niveau académique (bac+5) plutôt qu'un ensemble de compétences ciblées. Cela crée de la confusion sur le marché de l'emploi.

« On s'est rendu compte que les offres d'emploi étaient très mal rédigées, et surtout que les employeurs n'arrivaient pas vraiment à identifier les compétences dont ils avaient besoin : c'est ça, la grosse difficulté. […] Sur 16 000 fiches de postes en cybersécurité, 30 % avaient un intitulé « ingénieur cyber » en 2021, sauf que « ingénieur cyber », ce n'est pas un métier, c'est juste un niveau de qualification : on cherche quelqu'un qui a un bac+5 en cyber. Mais le problème, c'est que cela ne dit pas quelles compétences on recherche. »

Cette incompréhension pousse les employeurs à demander des profils trop polyvalents et à attendre d'eux qu'ils couvrent tout le spectre de la cybersécurité. Ce manque de clarté décourage les candidats qualifiés. Bien qu'une baisse de ces intitulés génériques (passant de 30 % à 15 % en cinq ans) montre une lente amélioration, la définition des besoins reste un problème majeur.

« Les gens ne connaissant pas bien la cyber, ils demandent une personne qui va tout savoir faire. En demandant un ingénieur cyber, ils se disent que c'est quelqu'un qui a suffisamment de connaissances en cybersécurité pour couvrir tous les aspects de la cybersécurité : il va pouvoir sécuriser leur entité. Cette approche est loin d'être idéale. »

1.2 L'accès précoce des profils juniors aux postes de RSSI

Cette méconnaissance des métiers cyber provoque des anomalies dans les trajectoires professionnelles, notamment l'accès précoce de profils juniors à des postes de Responsables de la Sécurité des Systèmes d'Information (RSSI). Historiquement considéré comme l'aboutissement d'une carrière nécessitant un recul macroscopique et une solide expérience de terrain, le rôle de RSSI est aujourd'hui attribué par défaut à de jeunes diplômés pour répondre à l'urgence managériale des structures de taille intermédiaire.

« On s'est aperçu qu'il y avait beaucoup de RSSI très jeunes, notamment des RSSI qui étaient dans la cyber

depuis environ cinq ans ou moins. Et cela est très déconcertant, car normalement, le poste de RSSI est un poste à haute responsabilité qu'on est censé atteindre au fur et à mesure des années, avec une connaissance de plus en plus importante en cyber et de plus en plus large. Or, ce dont on se rend compte, c'est qu'il y a beaucoup de jeunes qui sortent d'études et qui sont engagés directement en tant que RSSI. »

Ce parachutage de profils inexpérimentés à la tête des politiques de sécurité limite la garantie d'une protection effective des organisations. Il traduit la difficulté des départements RH à nommer correctement les fonctions intermédiaires, tels que les postes de chef de projet cyber, et à comprendre le périmètre de responsabilité associé à chaque dénomination.

« Les gens ne savent pas comment on appelle un chef de projet en cyber. Les gens ne connaissent pas les métiers de la cyber, ni les dénominations. Ils ne savent pas ce qu'un RSSI est censé savoir faire, ou un DSI, ou un consultant en cyber. Le RSSI ne se limite pas à cela, ce n'est pas son métier. Ils mettent donc des noms au hasard. »

1.3 La normalisation des fonctions par les référentiels

Pour clarifier le marché, les institutions s'efforcent de standardiser les métiers. Le panorama des métiers de la cybersécurité, porté par l'ANSSI, a permis d'accorder les acteurs civils et militaires sur une même nomenclature. Ce travail se poursuit avec le Campus Cyber pour créer une matrice de compétences et l'actualiser régulièrement. L'objectif est de définir le niveau requis pour chaque compétence et pour chaque métier afin d'aider les RH à recruter, de guider les reconversions professionnelles et de permettre aux écoles d'adapter leurs programmes.
« On a travaillé avec le Campus Cyber et un grand nombre d'acteurs sur une matrice de compétences qui permet d'identifier, pour chaque métier de ce panorama, les compétences associées à ces métiers. »

2. Évolution des besoins en formation

2.1 La distinction entre l'expertise technique et le référent cyber

Pour mieux comprendre les besoins, on peut faire un parallèle avec la médecine. D'un côté, il existe un besoin précis pour des experts de très haut niveau (comparables à des chirurgiens spécialisés). Ces profils, souvent chercheurs ou docteurs, sont indispensables pour les structures étatiques ou nécessitant une haute technicité, et sont très difficiles à recruter.

En revanche, la majorité des structures (TPE, PME, collectivités) n'a pas besoin de ces experts de niche. Leurs besoins relèvent d'une sécurité de proximité et de l'application des règles d'hygiène informatique de base.
« La majorité des mairies, collectivités, TPE et PME n'ont pas besoin d'experts de haut niveau pour sécuriser leur entité, dont le parc informatique se limite parfois à une dizaine d'ordinateurs. Ces entités ont en revanche un besoin massif en cybersécurité, auquel peuvent aisément répondre des référents en cybersécurité avec un niveau technique moindre. »

2.2 Structuration des formations courtes et adaptation aux besoins opérationnels

L'offre académique commence à s'adapter en s'éloignant du modèle unique de l'ingénieur généraliste de niveau bac+5. La tendance s'oriente vers le développement de cursus plus courts (bac+2 et bac+3) et de formations ciblées sur des blocs de compétences métiers spécifiques, rompant avec la logique d'un enseignement globalisant.

« Jusqu'à récemment, toutes les formations se ressemblaient : elles formaient toutes des ingénieurs cyber, bac+5 en cyber, où l'on apprend à tout faire. On constate désormais une autre tendance qui consiste à former des personnes sur des métiers précis, avec un programme de formation visant à offrir les compétences spécifiques à ces fonctions. »

Cette évolution répond à l'émergence de nouveaux besoins opérationnels, comme les profils spécialisés en administration sécurisée. Pour les petites structures, un administrateur systèmes et réseaux doté de connaissances cyber robustes mais basiques s'avère plus adapté et plus accessible qu'un expert de haut niveau.

2.3 Les obstacles au développement de l'alternance et de la formation continue

Bien que l'alternance soit considérée comme une excellente solution, les étudiants en région peinent à trouver des entreprises d'accueil. Ce blocage s'explique par la fin des aides de l'État à l'apprentissage et par un retournement économique du marché. Mais il faut aussi s'interroger sur d'autres causes plus profondes, telles que l'inadéquation des compétences des étudiants par rapport aux compétences actuellement recherchées sur le marché de l'emploi.

Face à la pénurie et aux coûts élevés des experts externes, la requalification des collaborateurs actuels du numérique représente une bonne alternative. Pourtant, cette démarche de formation continue se heurte à d'importants blocages logistiques au sein des administrations publiques. Hormis le ministère des Armées, qui possède une culture historique de la formation tout au long de la vie, les ministères civils peinent à libérer leurs agents pour des cursus longs d'un an, faute de moyens pour compenser leur absence sur le terrain.

« Si vous souhaitez recruter un expert en cyber aujourd'hui, cela ne va pas être chose aisée, car ils sont extrêmement recherchés, donc rares et, dès lors, coûteux. Former vos agents en interne peut s'avérer un choix plus judicieux. Nous le voyons très bien au sein de notre centre de formation, où nous proposons une formation d'expert en cybersécurité de niveau bac+5. Malgré la gratuité de cette formation pour tous les agents publics, nous peinons à la remplir, car elle dure un an »

3. Anticiper les mutations technologiques et intégrer des compétences humaines

3.1 L'impact réglementaire de NIS2 et le recentrage sur la gestion de crise

L'entrée en vigueur de la directive européenne NIS2 agit comme un accélérateur de conformité. En faisant basculer le nombre d'entités régulées de quelques centaines à plusieurs dizaines de milliers, cette réglementation contraint un volume massif de nouvelles structures à s'engager dans la sécurisation de leurs infrastructures et la déclaration de leurs incidents.

« Dans la directive NIS2, les obligations réglementaires passent, dans sa première version, de quelques centaines d'entités à plusieurs dizaines de milliers dans la seconde version. […] » Il y a donc une prise de conscience de ces entités, qui comprennent désormais la nécessité d'intégrer la cybersécurité et, donc, de former des gens en interne pour répondre aux exigences réglementaires. »

Cette pression réglementaire oriente prioritairement la demande de formation continue vers les compétences de gestion de crise et de remédiation. Les organisations cherchent en premier lieu à acquérir le socle technique et méthodologique minimal pour reconnaître une attaque, contenir l'incident et remettre le système d'information en état de marche.

« Par rapport aux demandes que nous recevons des ministères sur certaines formations, il y a des formations très demandées, par exemple la gestion de crise, qui est vraiment un sujet d'actualité. […] Les entités ont besoin de connaître les bases de la sécurisation de leur système informatique. Et puis, une fois que cela est fait, que se passe-t-il s'il y a une crise cyber, s'ils se font attaquer ? Il leur faut savoir la reconnaître, la détecter, gérer la crise et remettre en état. C'est ce dont elles ont besoin. »

3.2 Anticiper les ruptures technologiques : les compétences liées à l'IA et au post-quantique

Les instances de formation doivent anticiper deux ruptures technologiques majeures aux maturités distinctes. Concernant la cryptographie post-quantique (PQC), la transition est déjà opérationnelle sous l'impulsion de l'ANSSI, car les entités ont conscience qu'il faut qu'elles s'en emparent. L'agence impose l'intégration de solutions hybrides combinant cryptographie classique et algorithmes post-quantiques pour préparer les infrastructures sur le long terme.

« Les entreprises aujourd'hui doivent toutes passer, ou a minima réfléchir, à la transition post-quantique. L'ANSSI demande que les gens utilisent de l'hybridation, c'est-à-dire un mélange de cryptographie classique et de cryptographie post-quantique. »

En parallèle, l'impact de l'intelligence artificielle redéfinit les compétences requises, bien que le marché manque encore de recul pour en mesurer les effets précis sur la transformation des métiers. L'offre de formation se structure d'ores et déjà autour de trois axes : comprendre comment l'IA peut servir d'arme offensive pour les attaquants, l'utiliser comme outil de défense pour automatiser la sécurisation, et apprendre à sécuriser les systèmes qui intègrent eux-mêmes de l'IA.

« L'IA et la cyber : cela va être complètement pris d'assaut. […] Il s'agit plutôt de comprendre le lien qui peut exister entre l'IA et la cyber, c'est-à-dire : est-ce que l'IA peut aider les attaquants à attaquer les systèmes ? Est-ce que l'IA peut servir à sécuriser mieux ces systèmes ? […] Et il y a un troisième volet : la sécurisation de l'IA, c'est-à-dire des systèmes qui utilisent l'IA. Maintenant, comment doit-on les sécuriser ? À quoi faut-il faire attention ? »

3.3 La valorisation des soft skills comme levier d'attractivité de la filière

La cybersécurité souffre historiquement d'une image technique et exclusive, souvent perçue comme un domaine réservé à des spécialistes isolés. Pourtant, l'exercice quotidien de ces métiers, et particulièrement la gestion des incidents majeurs, repose de manière critique sur les compétences comportementales (soft skills), telles que l'accompagnement humain, la communication de crise et le management d'équipe.

« Je pense qu'il y a quand même un axe qui serait intéressant à déployer : les soft skills. Parce que les gens assimilent la cybersécurité à : « C'est un métier de geeks pour les hommes, hyper technique, pas accessible. » Alors que, finalement, quand on regarde les métiers, il y a beaucoup d'aptitudes humaines : manager des équipes, accompagner les bénéficiaires, communiquer et sensibiliser sur les problématiques cyber… »

Pour attirer les jeunes générations vers ces carrières, la filière doit faire évoluer sa communication en s'inspirant, par exemple, des méthodes de l'armée. Au lieu de centrer le discours sur la complexité scientifique ou informatique, l'enjeu est de mettre en avant les dimensions humaines de la profession : le travail en équipe, la cohésion de groupe et le sens de l'engagement au service de l'intérêt général.

« Quand je vois les publicités de l'armée, par exemple, je trouve qu'elles sont bien faites, car elles parlent vraiment des compétences humaines qu'ils vont développer : être dans un groupe, être au service de quelque chose pour la nation, etc. […] Dans la cyber, il y a un peu la même chose, c'est-à-dire que les gens peuvent être rebutés par le côté technique, en tout cas les jeunes. Même si le côté technique implique des maths, de l'informatique et exige des efforts, il y a derrière tout cela beaucoup de compétences humaines. »

BCI – BRETAGNE COMMERCE INTERNATIONAL



DAVID DUTERTRE
Chargé d'Affaires Numérique
et Cybersécurité

1. Évolution du marché du travail et des profils recherchés

1.1 Le passage d'un marché de la demande à un marché de l'offre

Il y a une dizaine d'années, le marché de la cybersécurité était un marché de demande, avec plus de besoins que d'offres disponibles, ce qui poussait les entreprises à recruter des profils débutants sur la base de leurs « *soft skills* ». Dans le même temps, un déséquilibre s'est installé entre l'attractivité des métiers offensifs (tests de pénétration) et les besoins réels, concentrés sur les fonctions de défense en continu (SOC).

« Le côté romantique du hacker […] de nombreux candidats à l'embauche voulaient être en tests de pénétration […] c'était beaucoup moins fun de faire de la surveillance en 3/8 et de passer du temps à faire du triage d'alertes et de faux positifs ». Cette préférence des candidats a créé une pénurie ciblée, plus qu'une pénurie généralisée : *« il manquait du monde certes, mais surtout dans certains secteurs comme le monitoring 24/7»*.

1.2 L'impact de l'automatisation et de l'IA sur les profils juniors

« Il y a eu une sorte de ruée vers l'or, avec la cybersécurité comme nouvel El Dorado. On avait à la fois de plus en plus de monde formé mais pas forcément au bon endroit, un nombre d'acteurs en forte croissance et une montée en puissance des outils d'automatisation ».

L'afflux de nouveaux acteurs, la multiplication des formations et la montée en puissance des outils d'automatisation, même antérieurement à l'IA générative, ont progressivement transformé un marché de qualité en marché de volume/prix, notamment sur les métiers les plus automatisables comme le test de pénétration dans certains de ses domaines.

L'arrivée de l'IA accentue cette dynamique en réduisant encore davantage le besoin de « petites mains » alors même que la demande client reste stable, voire en croissance. Aujourd'hui nous avons plus de juniors formés que de demandes des entreprises :

« Le besoin en cybersécurité est toujours bien présent évidemment, mais les outils d'automatisations viennent à limiter le besoin en ressources juniors dans un marché plus exigeant passant d'un marché de demande, à un marché d'offres ».

2. L'évolution nécessaire des modèles de formation

2.1 Les limites du modèle généraliste

Le profil généraliste, qui pouvait auparavant être recruté puis formé progressivement sur plusieurs années, devient plus difficile à valoriser commercialement, faute de temps et de moyens pour l'accompagner dans sa montée en compétence face à des outils désormais capables d'assurer les tâches d'apprentissage initiales.

« Par exemple, un pentester ou quelqu'un du CSIRT issu d'un parcours de formation générale, c'est à minima 7 ans, pour qu'il devienne quelqu'un de suffisamment expérimenté. Or, aujourd'hui, on a des outils d'automatisation et l'IA qui posent la question de la rentabilité de l'embauche de profils juniors ». Il en résulte un besoin de spécialisation plus tôt dans les cursus, non pas sur une technique donnée, mais sur un métier ou un segment de la posture cyber (défense, gouvernance, réponse à incident, rétro-ingénierie), chacun nécessitant un temps d'apprentissage propre minimum de plusieurs années. »

2.2 L'obligation d'une spécialisation par métier, pas par technologie

La distinction est faite entre une spécialisation technique, rapidement obsolète compte tenu de l'accélération des cycles d'innovation, et une spécialisation par métier ou par segment d'activité, plus durable et transférable d'une technique à l'autre.

« On ne peut pas se baser sur la seule spécialisation technique. Une spécialisation dans les différents segments de la posture cyber, ça c'est important. Ce n'est pas du tout le même métier de faire du rétro-ingénierie de malwares ou de la réponse à incident que de faire de la surveillance 24/7 par exemple ».

Cette approche s'accompagne d'un appel à un dialogue renforcé entre écoles et entreprises pour mieux anticiper les segments réellement en tension, au risque sinon de continuer à former des profils trop généralistes qui peineront à trouver leur place sur le marché.

3. Besoins en compétences hybrides et spécialités délaissées

3.1 L'importance de profils technico-commerciaux

Un marché plus exigeant impose d'identifier correctement les besoins des clients plutôt que de répondre à des demandes déjà formulées, ce qui nécessite un socle de compréhension technique solide.

« On n'est plus dans un marché de demande, on est bien dans un marché d'offres. Il faut être capable de poser les bonnes questions pour créer de la valeur et des ventes additionnelles ».

Ce double profil technique et commercial reste toutefois rare à trouver. Au-delà d'un parcours de formation type, la réussite dans ce métier dépend d'un trait de personnalité essentiel, permettant de franchir le pont entre les deux mondes : *« Être à la fois dans la technique et le commerce, implique d'être quelqu'un de particulièrement curieux ».*

3.2 Le manque de formation en architecture logicielle et réseau

Le déplacement du système d'information vers le cloud a doucement fait reculer la maîtrise de l'architecture réseau et logicielle dans les parcours de formation, alors que cette compétence redevient centrale avec la multiplication des enjeux de cloud souverain et l'intégration de l'IA dans les infrastructures d'entreprise.

« Cette dimension d'architecture réseau et logicielle me semble d'autant plus importante aujourd'hui. J'ai vu des étudiants arriver de Master sans avoir le début d'une vue d'architecture. Pourtant, c'est une partie des fondamentaux. Donc je trouve que ça manque ». Cette compétence transversale est plus durable qu'une expertise sur une technique ou un outil spécifique, la connaissance de l'architecture globale et des technologies d'un système d'information restant valable indépendamment des choix purement techniques d'une entreprise. »

3.3 L'anticipation du quantique et des besoins matériels industriels

Au-delà de l'IA et de la question du cloud souverain, deux sujets sont notamment identifiés comme points d'attention aujourd'hui :

- la menace que représente, à terme, le décryptage par ordinateur quantique de données actuellement chiffrées et déjà exfiltrées ;

- et le potentiel de développement de la cybersécurité appliquée aux secteurs industriels à forte valeur d'exportation (radiofréquences, composants électroniques, spatial), qui souffrent eux-mêmes d'un déficit de compétences.

Ainsi il serait judicieux de faire un parallèle entre les grands secteurs technologiques à l'export (spatial, composants électroniques et radio fréquences) avec les besoins de compétences en cybersécurité à venir.

CAPGEMINI



EDOUARD JEANSON
CISO Capgemini France,
Europe centrale et Europe du Sud

1. Mutation des conditions d'accès au marché et transformation des attentes envers les jeunes diplômés

1.1 L'arrivée de l'IA et le besoin d' adaptabilité des juniors

La généralisation de l'intelligence artificielle redéfinit la cartographie des métiers opérationnels de la cybersécurité. Les besoins de recrutement sur les fonctions d'opérateur de SOC de premier niveau, qui constituaient historiquement le point d'entrée des jeunes diplômés sur le marché, sont aujourd'hui plus rares en raison d'une automatisation croissante.

« Il y a encore 3 ou 4 ans, nous faisions constamment le constat d'une pénurie d'opérateurs de premier niveau dans les SOC. Je rappelais souvent qu'en France, nous ne disposions réellement que d'un seul vivier de formation, à Saint-Malo, vers lequel tout le monde se tournait. Aujourd'hui, c'est un poste pour lequel les recrutements sont beaucoup plus rares, l'IA ayant largement pris en charge ces fonctions »

Cette évolution rapide modifie la temporalité de la gestion des compétences : des compétences rares il y a trois ans sont devenues obsolètes, déplaçant le besoin vers des profils dotés d'une forte capacité d'adaptation, des étudiants qui doivent « apprendre à apprendre », plutôt que vers des spécialistes d'une technologie figée.

1.2 Paradoxe de l'expérience et crise de transmission

L'automatisation des tâches de premier niveau transforme profondément les parcours d'apprentissage des jeunes talents. Historiquement, la compréhension des enjeux globaux et managériaux d'un système d'information s'appuyait sur une expérience progressive du terrain, qui permettait de développer des réflexes d'analyse, d'investigation et de résolution de problèmes. Dans ce nouveau contexte, l'enjeu pour les entreprises est d'inventer de nouveaux modes de développement des compétences afin de préserver cette montée en expertise. L'objectif est de permettre aux juniors d'acquérir rapidement le recul opérationnel et la compréhension des environnements complexes qui seront attendus d'eux tout au long de leur parcours professionnel.

« Pendant longtemps, les postes d'opérateur de SOC constituaient une porte d'entrée naturelle vers les métiers de la cybersécurité. C'est à partir de cette première expérience que les professionnels pouvaient ensuite évoluer vers des fonctions plus expertes, notamment en architecture. Aujourd'hui, ces postes de premier niveau tendent à disparaître sous l'effet de l'automatisation. Cela soulève un véritable enjeu : comment offrir aux jeunes diplômés les premières expériences indispensables à leur montée en compétences ? Par où commenceront-ils leur parcours professionnel demain ? »

Cette transformation dépasse les métiers de l'informatique et concerne de nombreuses professions. En prenant en charge certaines activités de recherche, d'analyse ou de synthèse, l'intelligence artificielle invite les organisations à repenser les mécanismes de développement de l'expertise. L'enjeu est de permettre aux nouvelles générations

d'acquérir, par d'autres voies, la compréhension des données, des contextes et des situations qui forgent le jugement professionnel. La capacité à interpréter l'information, à relier les différents enjeux et à développer une vision globale des risques et des opportunités devient un facteur clé de différenciation.

« Pendant longtemps, les jeunes diplômés en droit construisaient leur expertise en passant des années à rechercher la jurisprudence et à préparer les dossiers pour les avocats. Ce travail constituait une étape essentielle de leur apprentissage. Aujourd'hui, quelques minutes suffisent pour obtenir, grâce à l'IA, une analyse exhaustive des précédents juridiques applicables à un cas donné. La véritable question n'est donc pas celle du gain de productivité, mais de la manière dont les jeunes professionnels développeront désormais la vision d'ensemble et les capacités de jugement que cette expérience leur permettait d'acquérir progressivement. »

À court terme, ce modèle permet des gains de productivité et économiques immédiats pour les organisations. À long terme, c'est la création d'un creux générationnel. Faute de repenser les modalités d'intégration et d'accompagnement des jeunes profils, la filière s'expose à une pénurie d'experts et de cadres dirigeants capables de piloter des crises dans les dix à quinze prochaines années.

« Nous privilégions aujourd'hui des profils expérimentés, capables d'exercer leur jugement, de prendre du recul et de s'appuyer sur des situations déjà vécues. Mais cela soulève une question essentielle : si nous voulons préparer l'avenir, comment continuer à intégrer et à former les jeunes générations afin qu'elles puissent, à leur tour, acquérir cette expérience ? »

2. Adaptation de l'offre de formation et définition des nouveaux socles de compétences

2.1 La nécessaire transformation des cursus face aux cycles d'obsolescence technologique

Les programmes scolaires se concentrent sur des outils ou des logiciels précis, ce qui pose un problème de fond : en voulant s'adapter de trop près aux besoins immédiats du marché, les écoles forment des profils très spécialisés, mais dont les compétences techniques deviennent obsolètes presque aussitôt l'obtention du diplôme. Les entreprises constatent ainsi un décalage : les jeunes diplômés maîtrisent une technologie à un instant T, mais ils manquent d'agilité pour s'adapter aux ruptures technologiques majeures, comme l'arrivée de l'IA ou du quantique.

Cette accélération du marché technologique impose de revoir la manière d'enseigner. Ce qui fait la valeur d'un profil aujourd'hui, ce n'est plus l'accumulation d'un savoir figé, mais sa capacité à comprendre des concepts globaux. Maîtriser la logique de fond d'un code, développer son bon sens et acquérir des réflexes de diagnostic transversaux deviennent les seuls outils durables. Dans un écosystème où les cycles de vie des métiers se comptent désormais en années, voire en mois, l'important n'est plus d'être le spécialiste d'un produit, mais de savoir se poser les bonnes questions pour évoluer.

« Dans nos métiers, qui évoluent à une vitesse considérable, nous avons avant tout besoin de personnes qui possèdent les bons réflexes, du discernement et une véritable capacité d'apprentissage. Nous recherchons des profils qui savent se poser les bonnes questions et apprendre en permanence, plutôt que des experts ultra-spécialisés dans une technologie ou un langage précis. Car nous savons qu'en l'espace de trois ans, la technologie sur laquelle ils ont été formés peut ne plus répondre aux besoins du marché. »

2.2 La préservation des fondamentaux techniques comme condition d'exercice

Même si les sujets de gouvernance et de conformité (comme NIS2 ou DORA) prennent de plus en plus de place, les formations ne doivent pas abandonner la technique pure. On observe aujourd'hui une tendance à vouloir

former des profils directement sur l'aspect organisationnel de la sécurité. Le problème, c'est que ces parcours manquent de légitimité sur le terrain. Sans base technique solide, il est difficile de comprendre la réalité d'une menace, d'échanger avec les équipes opérationnelles et de prendre les bonnes décisions en situation de gestion de crise. Pour faire carrière et évoluer librement d'un métier à un autre, le bagage technique reste le meilleur point de départ.

« Je fais partie de ceux qui pensent qu'un socle technique est indispensable. Même si je ne fais plus de technique aujourd'hui, je comprends ce que me disent les équipes et je peux encore analyser un problème en profondeur. À mes yeux, sans cette base technique acquise au départ, il est beaucoup plus difficile d'évoluer efficacement dans nos métiers.»

L'enjeu pour l'avenir des compétences des étudiants est donc, en plus d'avoir une bonne vision haute et stratégique, d'acquérir la compréhension des basses couches de l'informatique, comme le fonctionnement des réseaux ou des systèmes d'exploitation. Un bon expert cyber doit être capable d'utiliser des outils, mais il doit aussi savoir analyser des données brutes ou des logs pour comprendre concrètement d'où vient une attaque. Cet ancrage technique permet d'acquérir les bons réflexes et évite de subir les incidents.

2.3 Soft skills et compétences de vulgarisation

La capacité à communiquer efficacement avec des profils très différents est devenue une compétence indispensable, mais elle est encore trop souvent oubliée par les écoles. Un expert en cybersécurité ne peut plus se contenter de parler uniquement le langage technique des ingénieurs. Sur le terrain, il doit être capable de faire l'interface entre le monde opérationnel et la direction de l'entreprise. L'enjeu est de savoir traduire un incident ou une vulnérabilité technique complexe en impacts stratégiques, financiers ou juridiques compréhensibles pour des non-spécialistes.

« On a besoin qu'ils parlent anglais, on a besoin qu'ils soient capables d'adapter leur discours à la personne qui est en face. »

Pour les futurs professionnels du secteur, la maîtrise de ces différents niveaux d'abstraction est une condition majeure de réussite. Il s'agit de savoir descendre très bas dans la technique pour investiguer avec les équipes de production, puis de remonter pour expliquer la situation à un chef de projet ou convaincre un décideur de prendre une mesure d'urgence. Faute de développer cette agilité relationnelle et cette capacité de vulgarisation dès la formation initiale, les futurs experts risquent de rester inaudibles auprès des comités de direction, bloquant ainsi la prise de décision lors des crises.

3. Sensibilisation des acteurs de l'entreprise et confrontation aux réalités comportementales du terrain

3.1 L'approche par le risque

« On me demande souvent quels sont les critères pour recruter quelqu'un en sécurité. Je réponds le bon sens paysan et la curiosité !»

L'intégration des outils numériques personnels et de l'IA générative au quotidien crée de nouvelles failles majeures au sein des entreprises. Le problème ne vient pas toujours d'un manque d'outils de protection, mais plutôt d'un manque de culture du risque chez les collaborateurs. Les salariés ont tendance à reproduire leurs habitudes de la vie privée dans le cadre professionnel (partage de code sur des plateformes publiques, utilisation d'IA grand public pour rédiger des documents internes), sans mesurer l'impact de leurs actions.

Pour les managers et les équipes cyber, ce constat montre que les campagnes de sensibilisation traditionnelles

ne suffisent plus. Expliquer une règle ne garantit pas qu'elle sera appliquée. Face à ces risques, la sécurité doit s'appuyer sur du *« bon sens paysan »* et une vraie curiosité pour anticiper les actions des attaquants, plutôt que sur le simple respect de normes théoriques.

3.2 La complexité réglementaire et la surcharge administrative

« La bureaucratie qu'on peut avoir en France sur d'autres sujets nous a rattrapé dans la cyber. »

Du côté des directions d'entreprises, l'accumulation des nouvelles réglementations européennes et nationales (comme NIS2 ou DORA) complexifie la gestion des incidents. Au lieu d'aider les dirigeants à mieux protéger leurs structures, ces normes imposent souvent une bureaucratie lourde et des processus redondants, en particulier pour les grands groupes qui possèdent plusieurs entités juridiques :

« La multiplication des obligations réglementaires devient un véritable casse-tête. En cas d'incident, les entreprises doivent composer avec plusieurs cadres de déclaration, comme DORA ou NIS2, chacun avec ses propres exigences. Pour les groupes présents dans plusieurs pays ou dotés de plusieurs entités juridiques, cela se traduit par une répétition des démarches administratives, sans réelle valeur ajoutée en matière de cybersécurité. Une même situation peut ainsi nécessiter plusieurs déclarations distinctes, alimentant un sentiment de complexité et d'inefficacité.»

L'enjeu est de simplifier ces démarches pour que la conformité ne devienne pas une case administrative à cocher. Les dirigeants ont besoin d'outils centralisés et de modèles de déclaration uniques pour optimiser leur temps, afin de concentrer leurs efforts sur la gestion des risques opérationnels plutôt que sur cet aspect administratif.

3.3 Le déficit global de sensibilisation

Au-delà des profils spécialisés en informatique, le manque de sensibilisation à la cybersécurité est un problème général qui touche l'ensemble de la société. Aujourd'hui, la sécurité numérique est encore trop souvent perçue comme un sujet lointain qui ne concerne que les experts techniques. Les citoyens et les professionnels entendent parler des cyberattaques dans les médias, mais ils n'en mesurent pas l'impact direct sur leur propre quotidien ou sur leur structure. Cette déconnexion s'explique par un immense angle mort dans le système éducatif : en dehors des cursus purement cyber, les grandes écoles de commerce, d'ingénieurs ou les facultés de médecine ne proposent quasiment aucun module de sensibilisation à ces sujets.

« Les écoles forment encore trop peu à ces enjeux, alors même qu'il ne se passe pratiquement pas une semaine sans qu'une cyberattaque fasse l'actualité. Malgré cette visibilité croissante, beaucoup continuent à penser que ces incidents n'arrivent qu'aux autres. »

Pour corriger ces mauvaises habitudes avant qu'elles ne s'enracinent, l'effort pédagogique doit être anticipé bien avant l'entrée sur le marché du travail ou à l'université. C'est dès l'enseignement secondaire qu'il faudrait introduire de vrais cours pratiques pour apprendre aux jeunes à protéger leur identité numérique, leurs messageries et leurs réseaux sociaux.

« La sensibilisation devrait commencer dès le collège ou le lycée. L'objectif est d'apprendre très tôt les bonnes pratiques numériques afin d'éviter de développer de mauvais réflexes sur la messagerie, les réseaux sociaux ou les outils numériques du quotidien. »

4. Conclusion et ouverture

En conclusion, la cybersécurité reste un domaine passionnant par sa complexité, qui croise la technique, le juridique et l'organisationnel. Face à des attaques et des outils qui changent tous les jours, l'expérience et l'adaptabilité sont indispensables pour réussir. Pour protéger l'avenir de la filière et former les jeunes, une des solutions pourrait être la transmission directe sur le terrain : intégrer les juniors rapidement dans des équipes d'investigation aux côtés de seniors pour leur apprendre à anticiper les menaces et à développer ce fameux « bon sens paysan ».

« La cybersécurité exige une grande capacité d'adaptation et une remise en question permanente, car les menaces et les outils évoluent sans cesse. Pour les jeunes diplômés, l'essentiel est d'acquérir de l'expérience sur le terrain, aux côtés de professionnels plus expérimentés, afin de se confronter à des cas concrets. C'est cette expérience qui leur permettra ensuite de mieux comprendre le raisonnement des attaquants et de développer les bons réflexes. »

CEA – COMMISSARIAT À L'ÉNERGIE ATOMIQUE ET AUX ÉNERGIES ALTERNATIVES

STÉPHANIE BEHEYDT
Cheffe de service/DRHRS

ESTEL CHIRON
Chargée de développement RH/DRHRS

1. Une tension de recrutement différenciée selon les profils cyber.

1.1 Des profils classiques accessibles, des profils rares plus complexes à recruter

Stéphanie Beheydt (SB) distingue deux catégories de profils cyber au CEA :

D'un côté, des métiers plus classiques comme les développeurs, pour lesquels le pouvoir d'attraction de l'organisme fonctionne bien.
De l'autre, des profils très spécialisés très recherchés, comme les analystes d'évènements et architectes de cybersécurité orientés vers la gestion des risques cyber par exemple, pour lesquels la tension sur le marché de travail rend le recrutement nettement plus complexe, quel que soit l'attrait de la structure.

En somme, l'attractivité de l'organisme fonctionne globalement bien, notamment du fait du caractère particulier du CEA, organisme public de recherche porteur de grands projets dont la vocation est d'agir pour la souveraineté scientifique, technologique et industrielle de la France et de l'Europe. Mais elle se heurte à une forte concurrence sur certains profils très recherchés.

Toutefois, elle nuance en rappelant que ces difficultés ne ciblent qu'un petit nombre de fonctions bien précises dont le recrutement se fait au cas par cas et non à grande échelle. Cette situation particulière ne reflète donc pas la situation de l'ensemble des métiers informatiques et cyber du CEA.

1.2 Un cadrage salarial propre au statut d'EPIC

Le CEA étant un organisme public, il fait l'objet de mécanismes de contrôle budgétaire rigoureux de la part de l'État et ne dispose donc pas de marges de manœuvre notamment salariales aussi importantes que les sociétés privées ; la rémunération est l'un des facteurs de choix des candidats notamment pour les emplois critiques.

« On est une structure qui est financée pour partie par des tutelles, des ministères [...] on fonctionne sur des fonds publics, ce qui fait qu'on n'a pas non plus des marges de manœuvre énorme en termes de rémunération. Et dès qu'on parle de compétences critiques, forcément il y a de la concurrence, et elle se fait sur la rémunération en partie ».

1.3 Le réseau et la cooptation comme mode de recrutement dominant pour les profils rares

Face à ces difficultés, le recrutement des profils cyber les plus spécifiques s'appuie beaucoup moins sur les canaux

classiques que sur le réseau professionnel et la cooptation, un fonctionnement qu'Estelle Chiron rattache à la culture du milieu scientifique et technique :

« Ce que nous disent les opérationnels est que la recherche de profils techniques pointus fonctionne plus en réseau ».

Cette dynamique se retrouve également dans la participation des équipes à des hackathons et des salons professionnels, occasions de rencontres entre pairs qui alimentent ensuite ce réseau.

2. Le recrutement et l'encadrement des jeunes profils

2.1 L'alternance et la thèse comme viviers de recrutement privilégiés

Le CEA mise sur une politique de recrutement précoce, dès l'alternance ou la thèse, afin de capter de jeunes profils et de leur donner envie de poursuivre leur carrière au sein de l'organisme une fois qu'ils ont découvert ses missions, moyens et infrastructures ainsi que les possibilités d'évolution parmi ses activités variées. Cette orientation fait partie des engagements de l'organisme vis-à-vis des jeunes avec notamment un objectif de taux d'alternants supérieur à 5%.

Estelle Chiron confirme cette logique de vivier :
« Le CEA a une dynamique assez forte de recrutement d'alternants et de doctorants, ce qui nous permet d'intégrer des jeunes salariés, qui ensuite souhaitent rester et évoluer au CEA. (…) Capter les alternants c'est la première étape, mais pour nous c'est vraiment notre vivier ».

2.2 Un équilibre respectant la capacité réelle d'encadrement

Si le CEA affiche des objectifs volontaristes de recrutement de jeunes de moins de 30 ans, cette dynamique reste conditionnée par la disponibilité des équipes encadrantes ou expérimentées pour assurer leur montée en compétences, ce qui privilégie des intégrations successives plutôt qu'un recrutement en nombre.

« Le CEA s'est engagé sur des objectifs de recrutement de salariés de moins de 30 ans également, et cela dans les limites de la capacité de la structure à encadrer les plus jeunes. Donc pour l'instant c'est un équilibre qui fonctionne plutôt bien ».

Stéphanie Beheydt note par ailleurs que les profils plus expérimentés posent, à l'inverse, moins de difficultés de recrutement, la rémunération, la notoriété et l'offre globale du CEA devenant plus compétitives à mesure que la carrière progresse.

2.3 Une ouverture encore timide vers de nouvelles écoles et de nouveaux modes de formation

Le CEA a engagé une réflexion pour élargir ses critères de recrutement vers des écoles plus récentes tournées vers les besoins opérationnels des entreprises ; cette ouverture se heurte encore à une culture interne plutôt attachée aux formations plus classiques et reconnues.

« Nous on a eu justement ce souhait d'ouverture vers de nouvelles écoles qui sont plus près des besoins des entreprises […] C'est pour nous une évolution culturelle à accompagner ».

3. L'apprentissage permanent et les technologies de rupture

3.1 Savoir apprendre, une compétence à prioriser aux côtés des soft skills classiques

Stéphanie Beheydt juge la capacité d'adaptation indispensable en complément des soft skills traditionnelles comme le travail en équipe. Selon elle, la fréquence d'arrivée des nouveaux outils, notamment portée par l'IA, dépasse largement celle des ruptures technologiques précédentes, ce qui rend l'aptitude à apprendre en continu plus décisive pour la suite des carrières.
En complément, le CEA affirme des valeurs fortes comme la curiosité et la coopération qui sont le socle permettant d'appréhender ces nouveaux challenges.

« Au-delà des softskills, [...] la capacité à apprendre [...] permettra de s'adapter à la fréquence à laquelle les nouveaux outils arrivent, probablement supérieure à ce que les générations précédentes ont vécu à l'arrivée du téléphone portable, d'Internet etc. Donc celui qui sera en difficulté, c'est celui qui n'arrivera pas à apprendre et à s'adapter en permanence tout en préservant le collectif.. Une troisième valeur du CEA est la conscience des responsabilités et pour ce faire nous accompagnons nos salariés pour affronter ces changements. »

3.2 Un suivi des compétences outillé par un référentiel détaillé

Le CEA a mis en place un référentiel de compétences précis et régulièrement actualisé avec les équipes opérationnelles, qui lui permet de suivre l'évolution des métiers et, en particulier, les effets encore émergents de l'IA sur les emplois, sans céder pour autant à des anticipations trop hâtives.

« Nous avons créé un observatoire des emplois qui analyse de manière prospective les évolutions en termes de compétences notamment ».

Ce suivi s'appuie sur un référentiel qui *« dépasse les 3000 compétences pour 22 000 salariés »*, construit par benchmark avec les référentiels existants tout en conservant les spécificités propres au CEA.

3.3 La combinaison IA et quantique, un facteur démultiplicateur de futurs besoins en sécurité et donc en compétences

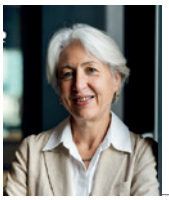
Pour Stéphanie Beheydt, l'enjeu à venir dépasse l'IA prise isolément : c'est la combinaison de la puissance de calcul et de l'intelligence artificielle qui devrait générer des méthodes et besoins de sécurisation nouveaux par rapport à ceux anticipés à ce jour, une conviction qu'elle relie directement à l'implication du CEA dans les programmes de recherche sur ces sujets.

C'est dans ce contexte que la Direction générale du CEA a regroupé depuis 2019 ses activités sur la cybersécurité dans un grand programme. Il structure aujourd'hui près de 200 ingénieurs-chercheurs au sein d'une quinzaine d'équipes appartenant à toutes les directions opérationnelles du CEA.

« Je pense qu'au-delà de l'IA, c'est plutôt quand on va pouvoir démultiplier la puissance de calcul, là on va avoir encore plus besoin de sécurité. Donc les technologies quantiques [...] vont probablement, associées à de l'IA, créer des besoins plus conséquents encore [...] C'est à la fois une puissance de calcul et une vitesse de prise de décision qui vont probablement faire qu'il y aura des vulnérabilités qui apparaîtront et donc des parades à concevoir ».

Pour anticiper ces opportunités et ces risques, le CEA doit disposer en effet de compétences diverses et en constante évolution ; la force du CEA réside dans sa capacité à innover tant pour ses besoins propres que pour ceux de la société.

CLUSIF



FLORENCE PUYBAREAU
Directrice du Clusif

1. Déconnexion entre la formation et le profil des jeunes diplômés et le marché de l'emploi

1.1 Le décalage entre les offres de formation et les attentes des entreprises

« Beaucoup de formations ont été créées en cybersécurité mais elles ne répondent pas forcément aux attentes des entreprises qui recherchent principalement des personnes ayant déjà de l'expérience »

L'offre de formation en cybersécurité a connu une croissance massive ces dernières années, mais un déséquilibre persiste entre l'insertion des profils juniors et les exigences des recruteurs. Les employeurs, particulièrement au sein des structures opérationnelles de taille moyenne, se montrent frileux à l'idée d'intégrer des alternants en raison de la charge managériale que cela représente, tout en exigeant des compétences déjà mûres à bas coût.

« L'offre de formation a explosé en quelques années,. Il y en a aujourd'hui quasiment dans toute la France. C'est une bonne nouvelle mais j'ai été plusieurs fois contactée par des directeurs d'établissements me disant qu'ils n'arrivaient pas "à caser" leurs alternants . Et parallèlement, les entreprises me disent qu'elles n'arrivent pas à trouver les bons profils. C'est surtout vrai dans les moyennes structures qui ont besoin d'experts cyber mais ne souhaitent pas prendre des alternants car elles n'ont pas les moyens (humains et financiers) et le temps de les former. Il y a un vrai problème d'adéquation entre l'offre et la demande ».

1.2 La méconnaissance du monde de l'entreprise par les profils techniques

« Les personnes formées en cybersécurité ont un bon niveau technique mais très souvent elles méconnaissent le monde de l'entreprise »

Les formations d'ingénieurs transmettent un bagage technique de très haut niveau, mais elles laissent un angle mort important sur la culture économique et managériale de l'entreprise. Les étudiants en fin de cursus ignorent souvent comment s'organise le marché, comment fonctionne un appel d'offres ou de quelle manière défendre un budget devant un comité de direction. De plus, on observe chez les étudiants une baisse d'intérêt pour les métiers techniques de terrain comme le pentest, au profit du secteur du conseil.

« Ils ont un bon bagage technologique mais dès que l'on parle de la cyber sécurité en tant que secteur industriel, [...] ils n'en ont aucune idée. Ils connaissent quelques grands acteurs du marché mais rien sur son organisation, son mode de fonctionnement, les forces en présence, les enjeux économiques... Idem sur la façon dont fonctionne une entreprise, le processus des appels d'offres, la réalisation d'un cahier des charges, la conception d'un budget que l'on va aller défendre devant sa direction. C'est ce que j'essaye de leur apporter pendant nos cours ».

1.3 Les lacunes comportementales et le besoin de profils transverses

« Lorsque l'on va dans les écoles d'ingénieurs, il y a encore le cliché du jeune avec un sweat à capuche , pas toujours très avenant . C'est encore vrai aujourd'hui même si heureusement, ça change peu à peu ».

Le déficit en soft skills (compétences comportementales et relationnelles) constitue un frein à l'intégration des jeunes ingénieurs. Par ailleurs, après une phase de recrutements massifs entre 2022 et 2024, le marché de l'emploi traverse une période de stabilisation. Les entreprises se concentrent désormais sur l'intégration de leurs outils et recherchent en priorité des profils seniors, transverses et stratégiques, capables de communiquer efficacement.

« L'un des points importants, ce sont les softskills. Aujourd'hui, les entreprises recrutent moins […] elles sont davantage en recherche de personnes qui ont un peu d'expérience technique, ou alors des profils transverses, qui vont pouvoir se former à la cyber mais possèdent les softskills pour s'adapter et parler à un comex ».

2. Impact de l'intelligence artificielle et obsolescence des compétences

2.1 L'automatisation des tâches opérationnelles de premier niveau

L'intégration généralisée de l'intelligence artificielle dans les outils de supervision transforme radicalement les centres opérationnels de sécurité (SOC). Les tâches d'entrée de gamme, autrefois dévolues aux profils juniors pour l'analyse humaine des alertes de premier niveau, sont désormais automatisées. Le besoin se déplace vers des compétences d'analyse plus complexes.

« En effet l'IA est en train de changer la donne pour beaucoup de métiers. Avant, il fallait des humains pour faire des travaux "d'entrée de gamme". Aujourd'hui, avec l'automatisation et l'IA il faut d'autres compétences […] Les premiers niveaux d'analyse sont remplacés par l'IA, et il y a besoin de gens qui analysent l'analyse, »

2.2 L'accélération des cycles de mise à jour pédagogique

La rapidité de l'évolution technologique impose une révision permanente des connaissances. Les programmes d'enseignement ne peuvent plus s'appuyer sur des bases figées d'une année sur l'autre. Pour les futurs professionnels, la compétence clé réside dans la flexibilité et la capacité à s'adapter à des métiers encore inexistants sur le marché.

« C'est une technologie qui avance tellement vite, que l'on peut craindre que les formations aient du mal à suivre. Moi-même qui ne fais pas des cours techniques, je dois revoir entièrement mes cours tous les ans car le secteur ne cesse d'évoluer. »

3. Difficultés pour les entreprises : maturité économique, gestion des risques, dépendance technologique

3.1 L'impératif de la cartographie des risques face au déficit de maturité

« Une entreprise, quel que soit son secteur d'activité doit faire sa cartographie des risques. Les grandes organisations le font mais c'est vrai aussi pour une PME ça doit être une priorité. Mais malheureusement ce n'est pas le cas »

Face à la menace cyber, la première démarche indispensable pour toute organisation, de la PME à la multinationale, consiste à formaliser une cartographie des risques. La cybersécurité ne doit plus être traitée comme un sujet

technique isolé, mais comme un risque managérial standard, au même titre que les risques RH ou de sécurité au travail. Si les outils méthodologiques gratuits existent, un grand nombre d'entreprises souffrent encore d'un manque de maturité et délèguent entièrement cette responsabilité à des prestataires externes, sans vision globale.

3.2 Les limites budgétaires de la sécurisation des PME

Si les grandes entreprises possèdent la structure financière pour investir dans leur sécurité, le tissu des PME reste largement en retrait. La cybersécurité y est rarement traitée comme une priorité face aux urgences économiques courantes. Même face aux initiatives d'accompagnement comme le référentiel RECYF de l'ANSSI, le coût d'entrée reste perçu comme un obstacle dissuasif, incitant les dirigeants à attendre de subir un incident avant d'agir.

« Les PME n'investissent pas ou très peu dans la cyber. Aujourd'hui le marché reste encore porté par les grandes entreprises et un peu par les ETI. ».

3.3 Le coût économique de l'autonomie stratégique et du cloud souverain

La dépendance des organisations françaises vis-à-vis du cloud américain (qui équipe près de 80% des entreprises) pose un défi d'autonomie stratégique. Cependant, une transition globale vers des solutions souveraines européennes se heurte à des réalités économiques majeures : les offres qualifiées SecNumCloud s'avèrent nettement plus onéreuses et les solutions européennes restent souvent moins intégrées et performantes que les suites tout-en-un des géants américains. L'enjeu à court terme repose donc sur une cartographie rigoureuse pour isoler et protéger uniquement les données les plus critiques.

« La dépendance aux solutions extra-européennes, notamment sur le cloud, est forte puisque 80 % de nos entreprises fonctionnent avec du cloud américain. Est il possible de tout basculer vers le cloud européen ? Non D'abord parce que cela a un coût. Choisir une solution SecNumCloud, peut faire augmenter l'addition de 20 à 30% par rapport à certaines solutions extra-européennes. Et puis, il y a peut être un déficit de visibilité pour les solutions européennes moins connues que leurs concurrentes américaines. Quand vous êtes une PME, une ETI, ça vous fait réfléchir ».

4. Le mot de Florence Puybareau pour la conclusion :

« Heureusement, nous travaillons dans un domaine qui évolue constamment. Pour les gens qui exercent dans les métiers de la cyber je trouve que c'est extraordinaire car cela oblige à apprendre constamment. Donc le message que j'aimerais faire passer aux jeunes, c'est : soyez curieux, informez-vous, essayez de comprendre les évolutions. Vous avez la chance aujourd'hui de faire un métier, dans 5 ans, vous en ferez un qui n'existe pas, dans 10 ans un autre qui n'existe pas encore ».

COMCYBER



COLONEL ZIMMERMAN
COMCYBER

1. Mutation des conditions d'accès au marché et transformation des attentes envers les jeunes diplômés

1.1 Concurrence du secteur privé et fidélisation des profils techniques expérimentés.

Le COMCYBER fait face à un défi structurel lié à la jeunesse et à la mobilité accrue de ses ressources humaines hautement techniques. Les métiers les plus critiques subissent une forte pression sur le marché de l'emploi. L'institution peine à stabiliser ses forces sur le long terme :

« On se retrouve avec des moyennes d'âge et des expériences, des temps de service au sein de nos entités, qui sont assez faibles, de l'ordre de 3 ans, il nous manque des profils un peu plus seniors, mais la tendance actuelle ne va pas pas dans ce sens là, on continue à avoir des facilités à recruter des juniors, mais des gens expérimentés, c'est un défi ».

Cette rotation rapide du personnel fragilise la montée en puissance de l'organisme, particulièrement dans les segments de pointe. Le Colonel identifie des besoins critiques non pourvus :

« Là où il y a un fort besoin, ce sont les métiers de l'investigation numérique (reverse engineering et analyse post-incident type forensic), où ce n'est pas toujours évident de recruter des gens qui sont pointus, c'est très compétitif avec le secteur privé ».

La concurrence directe avec les rémunérations et les conditions du secteur privé limite la capacité de la défense à fidéliser ses experts après leur phase de formation initiale.

1.2 Redéfinir le socle de l'enseignement supérieur pour développer l'agilité plutôt que l'immédiateté

Pour contrer l'obsolescence rapide des connaissances techniques, le modèle de formation ne peut plus reposer uniquement sur l'apprentissage d'outils figés. L'accent doit être mis sur des qualités comportementales et intellectuelles.

« Pour la compétence principale recherchée, je dirais la curiosité, c'est un domaine qui évolue constamment donc il faut se remettre en cause, avoir des bases solides. Je pense qu'il y a un socle de connaissances à avoir, et après savoir faire preuve de curiosité et d'agilité ».

Cette vision impose de repenser le rôle de l'enseignement supérieur. Plutôt que de chercher une employabilité immédiate et spécialisée, qui risque d'être dépassée en quelques mois, le Colonel propose une approche académique plus durable :

« Il faut armer nos jeunes étudiants des facultés qui leur permettront d'évoluer tout au long de leur carrière ».

1.3 Un dialogue encore informel avec les écoles, en décalage avec les besoins réels du terrain

Le Colonel reconnaît que ses relations avec les écoles restent aujourd'hui principalement tournées vers le recrutement, sans réel partage structuré des besoins de compétences :

« Des échanges existent mais il n'y a pas de dialogue vraiment structuré pour partager l'état de nos besoins en termes de compétences fines ».

Le Colonel formule à ce sujet une forme d'autocritique :

« nous devons aussi, côté état-major, gagner en précision dans notre approche des compétences, des travaux sont par ailleurs en cours au sein du ministère ».

Ce décalage se traduit concrètement par un long délai de montée en autonomie des jeunes recrues sur le terrain, qu'illustre l'exemple du CALID :

« Un jeune qui arrive au CALID, il a besoin d'un an et demi voire 2 ans pour pouvoir être autonome ».

Le Colonel y voit un axe de travail à explorer avec les écoles pour réduire ce temps d'adaptation, en s'appuyant sur des dispositifs de liaison existants :

« Je pense que le Pôle d'Excellence Cyber peut être une bonne courroie de transmission entre nos deux mondes ».

2. Adaptation de l'offre de formation et définition des nouveaux socles de compétences

2.1 Intégration des compétences de la donnée et hybridation des cursus face à l'IA

Les métiers de la donnée ne sont plus des spécialités isolées mais sont désormais en lien direct avec la cyberdéfense. Le COMCYBER doit intégrer des profils capables de structurer et d'exploiter de grands volumes d'informations, bien que ces compétences soient initialement éloignées du cœur de métier militaire .

« Face à la généralisation des compétences data, le COMCYBER devra recruter des profils polyvalents qu'il conviendra de spécialiser a posteriori. Cette évolution, qui s'annonce croissante, constituera un défi majeur en raison de la concurrence accrue pour ces talents. »

Sur ce sujet, le COMCYBER compte s'appuyer sur l'AMIAD, mais le Colonel nuance d'emblée l'ampleur de cet appui :

« L'AMIAD va nous aider dans ce domaine, mais on se rend compte que les moyens de l'agence sont consacrés à l'ensemble des besoins d'IA de défense, et il faudra aussi avoir dans nos organisations des personnes à même d'avoir un dialogue fructueux avec l'AMIAD ».

L'apparition d'outils d'intelligence artificielle sur le marché mondial transforme la vitesse et la nature des cyberattaques. Le ministère est dans l'obligation d'adapter ses outils.

« Aujourd'hui avec le domaine de l'IA on se rend compte qu'on va devoir accélérer, pour intégrer ces nouvelles capacités dans la cyber ».

Pour opérationnaliser cette vision, la stratégie consiste à diffuser cette expertise au plus près des équipes opérationnelles du ministère : *« il y a ce besoin de mettre des « sachants » au plus proche des métiers ».*

2.2 L'ouverture des cursus cyber aux compétences comportementales et d'influence

Le cyberespace ne se limite plus aux réseaux et aux infrastructures matériels, il englobe désormais la guerre informationnelle et cognitive. Pour la lutte informatique d'influence (L2I), les profils recherchés s'éloignent de l'ingénierie informatique classique pour rejoindre les sciences comportementales, la psychologie et le marketing social :

« Ce que nous recherchons dans nos équipes, ce sont des personnes qui sont assez performantes dans le marketing digital, nous avons également besoin de profils dotés d'expertises en cyberpsychologie, capables d'analyser l'impact des outils numériques à la fois sur la psychologie individuelle et sur les dynamiques de groupe ».

3. Sensibilisation des acteurs de l'écosystème et confrontation aux impératifs de souveraineté

3.1 Dépendance technologique et autonomie stratégique face aux solutions américaines

Les évolutions géopolitiques récentes et les incertitudes diplomatiques obligent la cyberdéfense française à réévaluer sa dépendance vis-à-vis des technologies étrangères, en particulier américaines. L'architecture actuelle des systèmes de supervision repose en partie sur des éditeurs privés extérieurs, constituant une vulnérabilité à moyen terme en cas de rupture de soutien ou de changement de posture politique :

« L'incertitude concernant le soutien américain à moyen et long terme nous amène à réévaluer notre dépendance. En réponse, des initiatives visant à renforcer notre souveraineté sont désormais menées au-delà du seul périmètre du ministère des Armées ».

Cette bascule vers plus d'autonomie technologique exige de revoir les compétences des agents, historiquement formés sur les standards du marché américain. L'enjeu est de reconstruire un savoir-faire national et européen :

« Donc il y a toute une réflexion aujourd'hui sur comment, dans les années à venir, s'affranchir et monter en maturité sur d'autres solutions ».

3.2 Le risque souverain des filières de formation externe : la dépendance aux organismes de formation américains

Au-delà de la dépendance technique aux logiciels, la souveraineté française est remise en question par la filière de formation continue. L'appareil militaire français recourt massivement à des organismes privés américains pour l'acquisition de compétences pointues. Comme le souligne le Colonel :

« Nous nous appuyons certes sur des organismes de formation français, mais pour certaines expertises les plus fines, notre dépendance à l'égard d'acteurs non-européens reste forte. »

Cette dépendance pose un problème de sécurité et de doctrine :

Un enjeu de renseignement d'origine cyber : en envoyant ses cybercombattants se faire certifier auprès d'un d'organisme étranger, l'appareil de défense français permet indirectement à un tiers de cartographier son vivier

d'experts. L'acteur étranger sait quel agent maîtrise quelle faille, quel outil, et quel niveau de technicité possède chaque unité du COMCYBER.

Un biais doctrinal et opérationnel : les formations diffusent des modèles de gestion de crise, des cadres de réponse aux incidents et des architectures de sécurité conçus par et pour d'autres modèles de sécurité . Or, les cadres juridiques, les structures de commandement et les doctrines de gestion de crise européens et français sont profondément différents. Former nos agents sur ces référentiels altère notre capacité à concevoir une réponse autonome et adaptée à notre propre écosystème régalien.

Face à ce constat, l'institution exprime une volonté claire de transformation :

« Le COMCYBER pense aussi qu'il serait très judicieux de gagner en autonomie pour les compétences pointues ».

Pour devenir une puissance numérique, la souveraineté nationale doit s'appuyer sur un réseau élargi, capable de produire ses propres cadres de pensée et ses propres formations :

« Je pense que le volet softskills sera assez important, cette capacité à savoir fédérer, et au delà finalement du monde militaire. Je ne dis pas qu'il faut copier les américains, mais on voit que pour devenir une puissance numérique, il faut s'appuyer sur des réseaux qui dépassent notre seule entité, savoir s'appuyer aussi bien sur le monde universitaire que sur le monde économique ».

CYBER'OCC



KARINE BEGUIN

Responsable du campus cyber territorial en Occitanie au sein de Cyber'Occ

Analyse des offres de formation et de l'insertion des étudiants du territoire Occitanie

1.1 L'impact des environnements technologiques selon la nature des établissements

L'intégration des étudiants au sein des entreprises par le biais de l'alternance favorise une communication directe et fluide entre le monde économique et les établissements d'enseignement. Ce dialogue permanent, grandement facilité à l'échelle régionale par les réseaux de campus territoriaux et les structures comme Cyber'Occ via le projet OSMOSE, met en évidence des disparités de fonctionnement importantes selon la nature publique ou privée des structures académiques.

Les formations initiales universitaires (comme à Toulouse ou Montpellier) privilégient l'apprentissage de l'open source et du système d'exploitation Linux. Si cette orientation garantit un excellent niveau technique, elle crée un angle mort sur l'environnement Windows, pourtant majoritaire chez les industriels. *« Un grand groupe, par rapport à l'université de Toulouse, disait que les étudiants étaient très bons sur Linux, mais étaient très mauvais sur Windows, puisque les universités travaillent beaucoup en Open source ».*

Face à ce décalage avec la réalité du terrain, les établissements privés font preuve d'une agilité pédagogique supérieure pour ajuster leurs maquettes :

« Les écoles privées comme YNOV, EPITA, EPITECH, ont réussi à intégrer dans leurs cours des spécificités sur différents systèmes d'exploitation (couvrant ainsi Linux, Windows et Mac) dès qu'un besoin est signalé par leurs entreprises partenaires. »

1.2 Les dynamiques d'accès à l'alternance

L'insertion des jeunes professionnels de la cybersécurité sur le marché occitan varie fortement selon le niveau d'études. Pour les étudiants en Master, l'accès aux stages et aux contrats d'alternance ne présente pas de difficulté majeure. Leurs compétences initiales sont jugées opérationnelles et adaptées, notamment par les grands groupes industriels qui absorbent une grande partie de ces profils. A l'inverse, pour les formations de niveau Bac+2 et Bac+3 telles que les BTS CIEL et SIO, ou les BUT informatique, les étudiants peinent à trouver des entreprises d'accueil sur le territoire, malgré une bascule progressive vers des rythmes d'alternance :

« Au niveau Master il y a très peu de soucis pour les étudiants de trouver une alternance ou un stage, par contre pour les BTS ou Bac+3 c'est plus compliqué ».

Les employeurs expriment en effet une préférence pour des niveaux de qualification plus élevés pour répondre à leurs problématiques de sécurité.

Selon Cyber'Occ, cette situation crée une polarisation du marché : alors que les grands groupes captent l'essentiel des étudiants, les petites structures qui auraient un besoin critique de compétences cyber se retrouvent exclues de ce dispositif. Pour accueillir un alternant, une entreprise doit disposer d'un maître d'apprentissage interne maîtrisant la matière.

Or, *« Il y a des entreprises qui auraient besoin de compétences cyber, mais ne peuvent pas prendre d'étudiants, puisqu'ils n'ont pas de maître d'apprentissage »*.

L'absence d'expert cyber dédié au sein des TPE et PME bloque ainsi le recrutement de ces jeunes, privant ces structures d'un levier de sécurisation pourtant accessible.

2. Évolution des compétences et intégration de profils opérationnels

2.1 La vulgarisation comme compétence prioritaire

Au-delà de l'expertise purement technique, les retours de terrain soulignent l'existence d'une rupture de communication entre les équipes de spécialistes cyber et les instances de gouvernance des entreprises. Les techniciens éprouvent des difficultés à échanger avec des dirigeants qui ne maîtrisent pas leur vocabulaire.

Dès lors, la capacité à vulgariser les concepts informatiques s'impose comme la compétence managériale et stratégique essentielle pour les futurs diplômés. Sans cette aptitude à traduire les incidents et les risques en langage clair et généraliste, les alertes des experts restent inaudibles pour les décideurs, ce qui empêche les directions d'anticiper les menaces, de piloter les crises et de débloquer les budgets nécessaires :

« Je pense que la principale qualité d'un étudiant, c'est sa capacité à vulgariser les aspects techniques. En effet, si le technicien s'adresse au dirigeant avec un vocabulaire trop spécialisé, celui-ci décrochera rapidement. Pour que chacun puisse s'inscrire dans une politique cyber ambitieuse, il est absolument nécessaire que les experts techniques sachent simplifier leur discours, afin que les décideurs et les instances de gouvernance comprennent véritablement les enjeux ».

2.2 L'hybridation des cursus avec l'intelligence artificielle et l'arbitrage des compétences

L'évolution technologique rapide transforme la structure même des programmes de formation de niveau Bac+4 et Bac+5. Poussées par la demande directe du marché professionnel, les maquettes pédagogiques doivent intégrer l'impact de l'intelligence artificielle, qui complexifie et automatise une partie des attaques, mais offre également de nouveaux leviers pour la défense des systèmes d'information, notamment via l'automatisation de la détection.

« Dans le domaine de la cybersécurité, de nombreuses formations ont ajouté des modules consacrés à l'IA. À l'inverse, certaines formations sont désormais principalement centrées sur l'IA, avec un simple module de cybersécurité. Cette évolution répond directement à la demande du marché professionnel ».

Si le socle technique initial reste commun aux étudiants en début de cursus, l'arborescence des spécialisations de fin de parcours pose un défi structurel pour les écoles.

« Il convient de se demander si les entreprises attendent d'un candidat qu'il soit spécialisé dans un domaine particulier, ou si elles recherchent plutôt une personne ayant une vision beaucoup plus large de la cybersécurité. »

Cette seconde option, axée sur la transversalité, est généralement privilégiée sur le terrain. Elle permet aux jeunes diplômés d'intégrer rapidement des structures variées, de comprendre l'ensemble des maillons de la chaîne cyber et d'évoluer de manière agile vers les différents postes managériaux et opérationnels que l'entreprise sera amenée à leur proposer.

2.3 L'agilité des forces de l'ordre face aux besoins du terrain

La gendarmerie nationale illustre une capacité d'adaptation rapide face à l'évolution des cybermenaces,

notamment par la refonte régulière de ses cursus internes et l'intégration des innovations. Alors que les structures académiques traditionnelles peinent parfois à anticiper les ruptures technologiques, l'institution militaire réajuste ses programmes de formation spécialisés (comme le Diplôme Universitaire en nouvelles technologies) au plus près de la réalité opérationnelle :

« Ils essaient de les développer progressivement, en fonction des besoins du terrain, des besoins des enquêteurs et des nouvelles attaques informatiques, afin qu'ils soient au plus près de la réalité du terrain ».

Cette réactivité se traduit également par une adoption précoce de l'intelligence artificielle pour optimiser les procédures de terrain, par exemple dans la retranscription automatique de la parole lors des auditions de mineurs afin de préserver le lien humain. Au-delà de la formation, l'institution s'appuie sur l'agilité de ses propres militaires pour pallier l'absence ou le coût élevé de certains outils commerciaux. Un vivier d'enquêteurs développe ainsi des solutions logicielles sur mesure, à l'image d'une application d'analyse rapide de la téléphonie conçue à Toulouse :

« Au sein de la gendarmerie, de nombreuses solutions payantes sont utilisées, mais l'institution dispose également d'un vivier de gendarmes particulièrement innovants, capables de développer des solutions pour améliorer les conditions de travail [...] Ces personnes peuvent également être recrutées dans le civil, afin d'apporter leur plus-value en matière d'innovation et de développement d'outils très concrets ».

Ces compétences, forgées dans l'action et l'auto-formation permanente, constituent par ailleurs un excellent vivier de profils transverses pour le secteur privé lors des reconversions.

3. Le niveau de maturité des dirigeants d'entreprises et la perception du risque

3.1 Les freins culturels et budgétaires des petites structures

L'expérience accumulée sur le terrain montre que le niveau de maturité cyber des structures de moins de 50 salariés (TPE et PME) reste globalement stagnant depuis vingt-cinq ans. Le premier obstacle réside dans une méconnaissance profonde du sujet, la cybersécurité étant perçue par de nombreux dirigeants comme un concept abstrait, voire irréel.

« Certains ne savent pas véritablement ce qu'est la cybersécurité : ils en entendent parler, mais ne cherchent pas à approfondir le sujet. On observe donc une méconnaissance du sujet, une méconnaissance des infrastructures qui pourraient les aider à monter en maturité, ainsi qu'un budget trop faible pour pouvoir se sécuriser efficacement »

Les petites entreprises allouent prioritairement leurs ressources financières à leur croissance immédiate, à la recherche de clients ou de fournisseurs, et au maintien de leur rentabilité à court terme.

De plus, ces dirigeants développent un sentiment d'immunité fondé sur la taille de leur organisation. Ils considèrent qu'ils ne représentent pas une cible d'intérêt pour les cybercriminels, faute de comprendre que les informations et les données qu'ils détiennent possèdent une valeur marchande ou stratégique exploitable :

« Selon eux, ils ne présentent pas d'intérêt pour les cybercriminels, car ils sont trop petits. Ils n'ont donc pas conscience que, même en étant une petite structure, les informations qu'ils détiennent peuvent être très intéressantes pour les cybercriminels. Ils n'arrivent pas à l'admettre. Cela fait 25 ans que je travaille dans le domaine de la cybersécurité, 25 ans que je tiens le même discours, et je constate que les choses n'évoluent pas ».

Cette perception erronée bloque la mise en œuvre des règles hygiène informatique élémentaires, qui ne nécessitent pourtant pas de coûts financiers exorbitants lors de la création d'une structure.

3.2 Les limites des campagnes de sensibilisation et de l'approche réglementaire

Les campagnes de sensibilisation traditionnelles et linéaires de masse se révèlent inefficaces pour faire évoluer les comportements. L'utilisation des retours d'expérience et des témoignages de dirigeants victimes d'attaques est également un échec : les chefs d'entreprise refusent de s'exprimer publiquement en raison du choc psychologique subi, de la crainte légitime de nuire à la réputation de leur marque et du temps considérable (souvent plusieurs années) nécessaire pour reconstruire la relation de confiance avec leurs clients. L'absence de témoignages concernant les petites structures dans les médias, qui se focalisent quasi exclusivement sur les attaques de grands groupes, entretient chez les patrons de PME l'illusion que le risque cyber ne concerne que les grandes entités :

« Vous ouvrez le journal papier, les journaux numériques, on ne parle que des gros groupes : un hôpital, des grosses structures. Donc c'est pour ça que les petites structures ont toujours ce sentiment : ah non mais moi ça ne peut pas m'arriver, de toutes façons il n'y a que les grands groupes qui se font attaquer ».

Par ailleurs, les leviers d'acculturation institutionnels et réglementaires n'atteignent pas leur cible. Des agences de l'État comme l'ANSSI, ainsi que ses référentiels de sécurité, sont totalement inconnues des dirigeants des PME issues des secteurs traditionnels comme la métallurgie. L'introduction de nouvelles réglementations européennes, à l'image du RGPD ou de la directive NIS2, est perçue comme une accumulation punitive de contraintes administratives et de normes déconnectées des réalités opérationnelles de l'entreprise :

« Lorsqu'on évoque la directive NIS2, beaucoup me regardent en me demandant : « Qu'est-ce que NIS2 ? » Ils y voient une nouvelle directive européenne de plus, impliquant encore de nouvelles normes à respecter. Je côtoie de nombreuses entreprises, notamment des petites et moyennes structures, et celles-ci sont déjà submergées par les réglementations européennes existantes ; on leur impose désormais de nouvelles obligations ».

La non-transposition immédiate de ces textes dans le droit national conforte les dirigeants dans l'idée qu'ils disposent de temps, ignorant que la responsabilité légale et financière du chef d'entreprise est désormais engagée. La prise de conscience n'intervient que face au fait accompli, lorsque l'entreprise est paralysée par une attaque.

« Moi je l'ai vu, je suis intervenue dans des entreprises qui avaient été cyberattaquées, vous arrivez en salle de crise quand il y en a une, c'est l'effondrement, le dirigeant est limite en pleurs, leurs prestataires informatiques sont vites dépassés par les évènements, au niveau comptable ils essaient de voir comment on peut limiter l'impact financier, on est sur un champ de bataille ».

DINUM–DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE

DIRECTION INTERMINISTÉRIELLE DU NUMÉRIQUE
Liberté
Égalité
Fraternité



NICOLAS TURQUET
Adjoint à la cheffe du département RH
de la filière numérique de l'Etat, DINUM

La transformation numérique de l'État s'est longtemps pensée comme un défi d'infrastructure et de budget. Elle est aujourd'hui, tout autant, un défi de ressources humaines :

« Comment identifier, faire évoluer et projeter les compétences numériques de 55 000 agents, dans des métiers dont la définition change plus vite que les outils censés la fixer ? »

La question n'est pas nouvelle et constituait l'objet même du rapport IGF-CGE de janvier 2023 intitulé « Les ressources humaines de l'État dans le numérique » ; cette question, elle se pose cependant avec une acuité particulière à mesure que l'IA irrigue l'ensemble des politiques publiques et que la pression sur les profils critiques s'intensifie. Un état des lieux s'impose, à la fois de ce qui progresse et de ce qui reste, malgré tout, à construire.

1. Ce qui est en cours : des outils qui commencent à raisonner en compétences

Une évolution structurante est engagée du côté des outils RH eux-mêmes. Pilotée par la DGAFP :

« La refonte du répertoire des métiers de la fonction publique vers une version « + » (RMFP+) vise à faire reposer la description des métiers non plus sur le détail de chaque situation d'exercice, mais sur des métiers cadres, plus macro, considérant ce qui leur est commun quel que soit le contexte administratif dans lequel ils s'exercent » ;

Les spécificités, elles, continueront d'être précisées dans des répertoires ministériels ou directionnels, le RMFP+ servant de socle commun. Il pourra par ailleurs s'agir d'un premier niveau de référence pour les employeurs ne bénéficiant pas encore de répertoire en propre. La DINUM contribue à ce chantier interministériel en animant le domaine fonctionnel numérique, data et IA, aux côtés des autres domaines pilotés par la DGAFP.

Cette bascule vers une logique de compétences n'a rien de cosmétique. C'est elle qui permet de faire de la gestion prévisionnelle des emplois et des compétences un exercice pensé à l'échelle macro, plutôt qu'un empilement de fiches métiers trop fines pour se répondre entre elles.

« Tant que le répertoire décrit chaque métier dans le détail, il reste difficile d'identifier ce qui, d'un métier à l'autre, relève de compétences réellement transférables » ;

En raisonnant par métiers macros, le RMFP+ doit pouvoir rendre au contraire visibles les compétences invariantes qui traversent plusieurs métiers proches : un data steward, un data scientist et un data analyst partagent, par exemple, une même culture de la chaîne de valeur de la donnée, quand bien même leurs compétences techniques

restent distinctes. C'est cette lecture par compétences, et elle seule, qui ouvre la possibilité de passerelles et de parcours de mobilité mieux outillés, rejoignant directement l'enjeu afférent à l'évolution des compétences de l'État au même rythme des besoins qu'elles doivent couvrir. Il est à préciser de surcroît que ce passage à une logique de compétences conditionne aussi une meilleure identification des besoins et un pilotage RH mieux nourri par la donnée :

« En partageant un même langage de compétences plutôt que des intitulés de métiers propres à chaque ministère, elle rend plus facilement comparable - et de fait agrégeables - des informations aujourd'hui dispersées entre les SIRH de chaque administration ».

Cette meilleure identification des besoins trouve d'ores et déjà une traduction concrète : en 2024, la DINUM a accompagné 345 ré-internalisations de compétences numériques au sein des ministères. La démarche mérite d'être expliquée, car elle n'a rien d'un simple réflexe de reprise en main : chaque ré-internalisation part d'un besoin identifié projet par projet, ce qui permet de faire reposer la décision sur une réalité opérationnelle plutôt que sur un principe général de méfiance vis-à-vis de la prestation externe.

« Elle poursuit malgré tout deux objectifs assez clairs : faire en sorte, d'une part, que les compétences jugées essentielles au bon fonctionnement de l'État, notamment sur les projets stratégiques de moyen ou long terme, restent maîtrisées en interne plutôt que dépendantes de prestataires, et d'autre part, de réduire les coûts ».

« Une réflexion est par ailleurs engagée autour de la planification stratégique par scénarios »,

A l'initiative de la DGAFP et de l'OCDE. L'intérêt de cette approche, soutenu par le département des RH de la DINUM, tient à ce qu'elle renonce, précisément, à l'idée d'une seule trajectoire prévisible : plutôt que de projeter les besoins futurs à partir d'une extrapolation linéaire des tendances actuelles - exercice périlleux dans un domaine aussi instable que le numérique -

« Elle consiste à construire plusieurs futurs possibles, contrastés, et à identifier pour chacun les compétences qu'il faudrait pouvoir mobiliser ».

Appliquée à la fonction publique, cette méthode change la question posée à la gestion des ressources humaines : il ne s'agit plus seulement de recruter pour couvrir des besoins déjà identifiés, mais de se donner, en amont, la capacité de réagir vite quel que soit le scénario qui se réalise. Pour la filière numérique en particulier - où un choc technologique, une crise cyber ou une rupture réglementaire peuvent redéfinir en quelques mois les compétences critiques -, l'intérêt d'une telle démarche est direct :

« Elle offre un cadre pour anticiper l'incertitude elle-même, plutôt que de chercher, en vain, à la réduire ».

2. Une approche par le cycle professionnel : l'expérience collaborateur

Ces chantiers structurels ne suffiraient cependant pas sans une action plus directement tournée vers les agents eux-mêmes. La DINUM initie ainsi, avec le concours d'autres ministères, une dynamique d'expérience collaborateur propre à la filière numérique de l'État, qui prend en compte l'ensemble des étapes du cycle professionnel de l'agent et de l'agente du numérique - du recrutement à la mobilité, en passant par l'accompagnement professionnel et la formation. L'ambition est double : renforcer, à l'entrée, l'attractivité des compétences numériques de l'État, et consolider, une fois les agents et agentes en poste, leur engagement et donc leur rétention. Le programme d'accompagnement ADA, destiné aux femmes du numérique de l'Etat, la création de communautés ou encore l'action du Campus du numérique public en faveur de la montée en compétences des agents de l'État constituent des exemples d'actions à impact.

Cette approche par le cycle professionnel donne aussi un sens plus concret à l'accompagnement et à la formation.

« Bien pensés, ils cessent d'être des outils isolés, déconnectés des priorités de recrutement, pour devenir le moyen de faire coïncider l'évolution des compétences des agents avec celle des besoins de l'État ».

3. Ce qui pourrait encore progresser : vers un référentiel réellement dynamique

Ces avancées, aussi réelles soient-elles, ne suffisent pas à résoudre un problème de fond : celui du temps. Un référentiel, quelle que soit la qualité de sa construction, se fige au moment où on le publie ; les métiers critiques du numérique, eux, continuent d'évoluer, parfois radicalement, d'une année sur l'autre.

« Il est probable qu'une partie des métiers considérés aujourd'hui comme prioritaires n'occupe plus, dans cinq ans, le même niveau de criticité, et inversement, que des compétences aujourd'hui marginales deviennent stratégiques sans qu'aucun référentiel ne l'ait anticipé ».

La refonte en cours pose les bases d'un référentiel plus macro ; elle ne dit pas encore comment le maintenir vivant.

C'est ici qu'un référentiel dynamique des compétences prendrait tout son sens - un outil qui ne se contenterait plus d'être révisé périodiquement, au gré des arbitrages, mais qui s'actualiserait en continu, à mesure que les signaux du marché de l'emploi et des besoins ministériels évoluent. Le sujet est encore peu documenté ; il mérite pourtant qu'on s'y arrête, car les moyens de le construire existent déjà, ou presque.

« L'intelligence artificielle peut permettre d'analyser en continu de grands volumes de données aujourd'hui dispersées et sous-exploitées : les offres d'emploi elles-mêmes, publiques comme privées, pour repérer l'apparition de compétences émergentes avant même qu'elles ne soient nommées dans un répertoire ; les délais et les difficultés de recrutement, comme indicateurs précoces d'une tension qui s'installe ; les mobilités et les formations suivies par les agents, pour objectiver, plutôt que supposer, les passerelles réellement empruntées entre métiers ».

Un tel dispositif changerait la nature même du référentiel : d'un document que l'on consulte, il deviendrait un instrument que l'on interroge, capable de signaler, par exemple, qu'une compétence en forte croissance dans les offres d'emploi du secteur privé n'est pas encore identifiée comme critique dans la sphère publique, ou que la criticité d'un métier décroît plus vite que prévu. Il ne s'agirait pas de remplacer l'expertise humaine qui construit aujourd'hui ces référentiels, mais de lui donner un instrument de veille continue, là où elle ne dispose aujourd'hui que de points de mesure espacés dans le temps. C'est un chantier qui reste, pour l'essentiel, devant nous ; il mériterait d'être exploré avec la même ambition que celle portée sur la refonte des métiers eux-mêmes.

4. Des tensions de recrutement qui restent, elles, très concrètes

« Deux domaines cristallisent aujourd'hui l'essentiel des tensions : la cybersécurité, dont l'acuité s'est trouvée renforcée par les incidents récents, et l'intelligence artificielle, devenue en peu de temps un sujet politique de premier plan, porté directement par les cabinets ministériels. »

Sur le terrain, cela se traduit par des profils très spécialisés que les ministères peinent à identifier autant qu'à recruter.

Ces tensions ne se répartissent pas non plus de façon homogène. Les grands ministères, mieux dotés en ingénierie RH, parviennent généralement à anticiper leurs besoins. Les structures plus petites affrontent des défis numériques tout aussi complexes, avec des équipes plus réduites ; ce déséquilibre mériterait d'être davantage pris en compte dans l'allocation des moyens et l'accompagnement RH.

4.1 Le nœud juniors-seniors : l'angle le moins résolu

« Reste un dernier point, plus sensible, mais qui conditionne la soutenabilité de tout le reste : celui de l'équilibre entre profils expérimentés et jeunes diplômés ».

Face à des besoins jugés critiques, les administrations privilégient assez naturellement le recrutement de profils immédiatement opérationnels. Le réflexe se comprend ; il appelle cependant une vigilance particulière, car l'âge moyen des experts numériques en poste se situe aujourd'hui, selon l'INSEE, autour de 39 à 41 ans (vraisemblablement plus élevé dans le secteur public eu égard à une pyramide des âges globalement plus élevée) : ces chiffres, à eux seuls, invitent à regarder au-delà du prochain recrutement.

« Faire reposer la réponse aux tensions actuelles sur les seuls profils seniors, c'est prendre le risque de reporter le problème plutôt que de le résoudre : ces experts partiront un jour à la retraite, et le vivier capable de prendre le relais ne se constitue pas du jour au lendemain. »

Recruter un junior suppose un investissement - du temps de formation, un accompagnement resserré - que la pression du recrutement immédiat n'encourage pas toujours. C'est précisément ce que la dynamique d'expérience collaborateur engagée par la DINUM cherche à structurer : un accompagnement pensé sur la durée du parcours, plutôt qu'un effort ponctuel au moment du recrutement, seul à même de faire tenir ensemble l'urgence des besoins d'aujourd'hui et la continuité des compétences de demain. Cette réflexion est de surcroît à mener pour rompre ce décalage entre l'enseignement supérieur qui investit dans la filière numérique et promeut à notre demande le secteur public, et des employeurs qui ne se saisissent pas de ces viviers en puissance.

En somme, la gestion des compétences numériques de l'État avance sur plusieurs fronts à la fois, à des vitesses différentes. Les fondations sont désormais en place ; l'enjeu est de les faire vivre dans la durée, en articulant anticipation des besoins, accompagnement des agents et évolution continue des compétences.

TERRITOIRE GRAND-NANCY

MADAME E
Professionnelle de l'accompagnement RH des entreprises

1. Un marché de l'emploi local structuré autour du secteur public et des profils seniors

1.1 La baisse des aides à l'apprentissage recentre les recrutements sur les profils expérimentés

Le retrait progressif des financements publics dédiés à la formation numérique a engendré la disparition de plusieurs organismes de formation privés et une réduction du nombre de places en alternance dans les structures plus anciennes. Ce contexte amène les entreprises à recentrer leurs recrutements sur les besoins qu'elles jugent prioritaires, avec un effet observable sur les profils juniors.

« La baisse des financements dédiés à l'apprentissage a clairement pesé sur la manière dont les entreprises priorisent leurs recrutements. Le recrutement de profils juniors ne constitue pas nécessairement un besoin directement exprimé par les entreprises que nous accompagnons : nous sommes davantage dans une logique de construction de vivier. A l'inverse, les entreprises expriment surtout des besoins portant sur des profils expérimentés, qui ne correspondent ni aux dispositifs d'apprentissage ni, dans la plupart des cas, aux profils de jeunes diplômés. »

Ce contexte se traduit par un besoin de profils expérimentés qui reste aujourd'hui difficile à satisfaire pleinement : *« A l'heure actuelle, cette demande constitue le véritable point de tension dans les recrutements. »*

1.2 Un tissu économique porté par les secteurs utilisateurs du numérique et les employeurs publics

« Notre marché compte relativement peu de grands acteurs spécialisés dans les services numériques et très peu d'entreprises dont l'activité est exclusivement consacrée à la cybersécurité. La majorité des recrutements provient plutôt de DSI des secteurs utilisateurs, qui doivent avant tout sécuriser leurs propres systèmes et activités. »

Cette configuration a une incidence directe sur la nature des emplois proposés. Les postes entièrement consacrés à la cybersécurité restent relativement rares. Dans de nombreuses organisations, notamment les structures de petite ou moyenne taille, les missions de cybersécurité sont intégrées à des fonctions informatiques plus larges.

« Les offres d'emploi correspondant à des postes exclusivement consacrés à la cybersécurité restent peu nombreuses. Dans beaucoup d'organisations, les missions de cybersécurité sont associées à d'autres responsabilités, avec une recherche importante de profils polyvalents. »

La demande locale porte ainsi moins sur des spécialistes cyber très fortement segmentés que sur des professionnels capables d'articuler cybersécurité, administration des systèmes, réseaux, infrastructures ou gestion informatique.

2. IA et post-quantique : des sujets encore émergents dans les usages locaux

2.1 Une appropriation de l'IA encore progressive

Certaines structures de grande taille, comme les établissements hospitaliers ou bancaires, ont commencé à intégrer des solutions d'IA dans l'analyse des menaces. Cette adoption reste toutefois encore émergente à l'échelle du territoire.

« Nous n'arrivons pas encore à mesurer avec précision les besoins liés à l'intelligence artificielle. Le sujet est très présent dans les discours et les réflexions prospectives, mais il ne se traduit pas encore partout par des usages concrets. »

Ce constat se retrouve aussi dans l'offre de formation, où les compétences liées à l'IA agentique appliquée à la détection de menaces restent peu intégrées à ce stade, une évolution jugée possible via des formats pédagogiques immersifs ou des cas d'usage concrets plutôt que par une refonte complète des diplômes.

2.2 La cryptographie post-quantique et le cloud souverain, des sujets qui n'ont pas encore atteint les entreprises locales

Contrairement à l'IA, la cryptographie post-quantique et le cloud souverain restent, à ce stade, des sujets peu présents dans les préoccupations opérationnelles des entreprises du territoire.

« La cryptographie post-quantique est aujourd'hui principalement portée par les acteurs de la recherche et de l'expertise technologique. Ce n'est pas un sujet qui remonte jusqu'à nous depuis les entreprises. »

Sur le cloud souverain, le constat est similaire : les entreprises locales n'ont pour l'instant pas engagé de réflexion structurée sur le sujet. Ce décalage illustre un temps d'appropriation encore nécessaire entre les capacités de recherche académique et leur diffusion vers les entreprises utilisatrices, notamment les structures les plus petites, moins directement connectées aux centres de recherche que les grands comptes.

GRAND GROUPE INTERNATIONAL DE SERVICES NUMÉRIQUES

MADAME M
Professionnelle de la transformation du travail, de l'intelligence collective et de la neurodiversité

Quand l'accélération technologique transforme notre manière de penser les compétences

L'accélération technologique, notamment avec l'essor de l'intelligence artificielle, transforme les métiers mais aussi la manière dont les organisations doivent penser le développement des compétences.

Le défi n'est plus seulement d'anticiper les compétences nécessaires à trois ou cinq ans. Il consiste également à développer une capacité d'adaptation continue : détecter les évolutions, faire émerger rapidement de nouvelles compétences, actualiser les dispositifs et mieux identifier les expertises déjà présentes dans les organisations.

1. Des compétences qui évoluent plus vite : passer de la planification à l'adaptation continue

1.1 Des horizons d'anticipation qui se raccourcissent

La planification des compétences reste nécessaire, mais l'accélération technologique rend plus difficile la construction de trajectoires figées à moyen ou long terme.

Le temps nécessaire à l'identification d'un besoin, à la conception d'un parcours de montée en compétences et à son déploiement peut désormais être long au regard de la vitesse d'évolution des technologies et des usages.

« Si on prévoit des parcours de montée en compétence, le temps qu'on les construise, il y aura des technologies, des choses qui auront évolué. Avant, on pouvait se dire : on fait un plan sur trois ans, même avant cinq ans, et on était sûr que c'était OK. Ce n'est plus le cas. »

Cette évolution ne signifie pas qu'il faille renoncer à l'anticipation. Elle conduit plutôt à travailler avec des horizons plus courts et à accepter davantage d'itérations.

« On essaye d'anticiper, mais on devient parfois plus en réactivité par rapport aux nouvelles technologies. »

L'enjeu est donc progressivement de compléter la planification par une capacité à ajuster rapidement les priorités et les dispositifs de développement des compétences.

1.2 Des formats d'apprentissage plus courts et plus facilement actualisables

Cette évolution concerne également les dispositifs de formation. Pour certains sujets dont les connaissances évoluent rapidement, comme l'intelligence artificielle, la data ou la cybersécurité, il peut être pertinent de proposer un socle commun régulièrement actualisé, puis de différencier les parcours en fonction des besoins d'expertise.

Des formats courts permettent notamment de diffuser rapidement une première compréhension commune et de faire évoluer les contenus sans devoir reconstruire systématiquement des parcours longs.

L'objectif n'est donc pas de remplacer les parcours structurés, mais de les compléter par des boucles d'apprentissage plus courtes, plus fréquentes et plus facilement actualisables.

1.3 Observer les compétences dans la durée

La même question se pose pour l'identification et l'évaluation des compétences.

Les campagnes d'évaluation annuelles peuvent constituer un repère utile, mais elles risquent de ne pas rendre compte suffisamment rapidement de compétences qui évoluent désormais à un rythme beaucoup plus soutenu.

« Une campagne d'évaluation, en termes de communication, désormais un an c'est très long : les compétences que les managers auront vues et que l'on aura analysées seront déjà obsolètes une fois que l'on aura les résultats. »

Cela invite à compléter les démarches annuelles par une observation plus continue : échanges avec les équipes, veille sur les évolutions des métiers, communautés d'experts, retours du terrain ou identification régulière des nouvelles compétences.

L'enjeu n'est pas nécessairement de multiplier les évaluations, mais de réduire le décalage entre l'apparition d'un nouveau besoin et le moment où l'organisation est capable de le repérer et de l'accompagner.

2. Faire de l'organisation un espace d'apprentissage collectif

2.1 Les métiers comme acteurs de la construction des compétences

Lorsque les métiers évoluent rapidement, les dispositifs de développement des compétences gagnent à être construits en lien étroit avec les équipes opérationnelles.

Les personnes qui connaissent les métiers et leurs transformations permettent de vérifier que les contenus proposés correspondent bien aux réalités du travail.

« Il faut savoir parler à son public. Soit les personnes viennent du terrain, soit elles le côtoient au quotidien, et garantissent que ce qui va être réalisé et proposé ne tombe pas à côté. »

Cette proximité permet également d'actualiser plus facilement les contenus et d'identifier de nouvelles compétences à développer.

Le développement des compétences devient ainsi moins un processus exclusivement descendant qu'un processus de co-construction entre les experts des métiers et ceux qui accompagnent les apprentissages.

2.2 L'apprentissage ne se limite pas à la formation

Le développement des compétences ne se joue pas uniquement dans les formations formelles.
Une part importante des apprentissages se construit également dans l'activité : en expérimentant, en résolvant des problèmes, en échangeant avec des collègues ou en sollicitant des collaborateurs disposant déjà d'une expertise particulière.

Les collaborateurs experts peuvent ainsi jouer un rôle de transmission particulièrement important, notamment

lorsqu'ils interviennent comme ambassadeurs ou relais auprès de leurs pairs.

« C'est beaucoup plus enrichissant et constructif, et surtout retenu dans la durée. »

Cette approche conduit à considérer l'organisation non seulement comme un lieu où l'on se forme, mais aussi comme un environnement dans lequel on apprend en permanence.

2.3 Faire circuler les compétences plutôt que seulement les identifier

L'un des enjeux majeurs est également de mieux identifier les compétences dont l'organisation dispose déjà. Certaines expertises sont développées en dehors du périmètre strict du poste occupé : à travers des projets personnels, des expériences antérieures, des activités associatives ou des centres d'intérêt développés en parallèle du métier.

Une compétence qui reste isolée chez un individu ne produit pas nécessairement toute sa valeur pour l'organisation. L'enjeu est aussi de créer les conditions de sa transmission, de sa mise en relation avec d'autres expertises et de sa mobilisation dans de nouveaux contextes.

« On a des compétences, mais peut-être pas là où on pense regarder. »

Dans un contexte où les organisations recherchent rapidement de nouvelles compétences, mieux connaître les expertises déjà présentes constitue donc un levier important.

La question n'est ainsi plus seulement :
« De quelles compétences avons-nous besoin ? », mais se déplace pour devenir aussi : *« Quelles compétences avons-nous déjà, où sont-elles et comment pouvons-nous les mobiliser ? »*

3. Élargir notre regard sur les compétences

3.1 Ne pas remplacer les stéréotypes négatifs par des stéréotypes positifs

Cette réflexion conduit également à interroger la manière dont certaines catégories de collaborateurs sont associées à des compétences particulières.

La neurodiversité permet d'interroger de manière particulièrement concrète nos façons d'identifier et de valoriser les compétences.

Après avoir longtemps été principalement abordés sous l'angle des difficultés et des besoins d'adaptation, les profils neurodivergents peuvent aujourd'hui faire l'objet d'un mouvement inverse : leur attribuer automatiquement certaines qualités ou compétences.

« Avant, les stéréotypes étaient en général plutôt négatifs. Là, on est en train de vivre un changement de paradigme, voire on tend à basculer parfois vers des stéréotypes plutôt positifs… mais qui restent des stéréotypes. La question ne doit pas se poser ainsi. »

L'enjeu n'est donc pas de remplacer une vision déficitaire par une vision idéalisée, mais de revenir à une approche individuelle des compétences.

L'utilisation plus précoce de certains outils, notamment d'outils d'IA, peut par exemple être observée chez certaines personnes neurodivergentes. Elle peut cependant répondre à un besoin concret, comme la réduction d'une surcharge cognitive ou la facilitation de certaines tâches, plutôt qu'à une aptitude générale que l'on pourrait

attribuer à l'ensemble des personnes concernées.

3.2 Concevoir des environnements qui répondent à une diversité de besoins

La question de l'accompagnement reste également liée à la capacité des organisations à identifier les besoins individuels.

Lorsque les dispositifs spécifiques sont conditionnés à une reconnaissance administrative, ils ne peuvent concerner que les personnes qui disposent de cette reconnaissance et souhaitent communiquer leur situation. Une autre approche consiste à développer des dispositifs qui bénéficient plus largement à l'ensemble des collaborateurs : développement des compétences relationnelles, communication, coopération, expression, nouvelles pratiques de travail ou encore gestion de la charge cognitive.

Il ne s'agit pas de nier les besoins spécifiques, mais de compléter les dispositifs dédiés par une réflexion plus large sur la conception des environnements de travail et d'apprentissage.

4. Vers une nouvelle approche des compétences

L'accélération technologique conduit finalement à déplacer la question, pour se demander « *Sommes-nous capables d'identifier rapidement les compétences dont nous avons besoin, de faire émerger celles qui manquent et de mobiliser celles qui existent déjà ?* »

Cette évolution suppose de rapprocher davantage les métiers, la stratégie, le développement des compétences et le travail réel.

Dans un environnement où les technologies évoluent rapidement, la capacité d'une organisation à apprendre collectivement, à faire circuler les connaissances et à mobiliser la diversité des compétences dont elle dispose devient une compétence en elle-même.

L'enjeu devient alors de construire des organisations capables d'apprendre suffisamment vite pour s'adapter à ce qu'elles n'avaient pas encore prévu.

OVALT GROUP



JÉRÔME CHAMPENOIS
DSI groupe OVALT

1. Les spécificités de la cybersécurité industrielle face aux approches classiques

1.1 Des cycles de vie et des contraintes de production incompatibles avec les pratiques du SI de gestion

La cybersécurité industrielle ne peut pas s'appuyer sur les mêmes recettes que celles utilisées pour les systèmes d'information de gestion, du fait de cycles de vie beaucoup plus longs et de contraintes de continuité de service bien plus fortes (la production ne peut pas être arrêtée régulièrement pour installer les patch ou les montées de versions).

« Les cycles de vie qui sont très longs. Généralement quand ils construisent une usine, les industriels achètent « les murs », les machines, l'informatique qui vient avec, et ils vont amortir cet investissement sur 20 ans […] contrairement à l'informatique de gestion où l'on a plus de facilité à faire évoluer les versions de nos logiciels, à les patcher et où les cycles d'amortissement sont plus court[…]. Cette compréhension des cycles de vie industriels et des contraintes de production est essentielle ».

Cette réalité se traduit par des systèmes qui restent en exploitation bien au-delà de leur obsolescence technique, et par l'absence d'environnements de test iso-production, ce qui complique toute mise à jour :
« On n'a jamais deux usines, une de production et une de recette […]. Le risque de régression n'est pas négligeable ».

1.2 Deux approches complémentaires pour adresser le sujet : stratégique et technique

Deux méthodologies distinctes coexistent pour engager une démarche de cybersécurité : une approche descendante, centrée sur l'analyse des risques et la continuité d'activité. Elle nécessite une prise de hauteur et correspond à une approche « stratégique » souvent attendue par les CODIR. L'autre approche est ascendante. Elle est fondée sur des audits terrain, plus adaptée aux équipes opérationnelles qui souhaitent avoir une vision plus technique des problèmes existants pour gérer des plans d'actions à court et moyen termes.

« Vous avez deux façons d'adresser le sujet : soit c'est du top-down. Vous prenez de la hauteur et travaillez avec une direction sur la continuité de son activité. Soit on réalise des audits terrain, on se retrouve avec des états des lieux assez précis […] vous avez un automate à tel endroit, dans telle version, il est obsolète… ». Les deux approches ne s'opposent pas mais le choix prioritaire entre ces deux approches dépend fortement des attentes de l'interlocuteur. Les équipes d'exploitation se montrant en général plus réceptives à une approche très technique et pragmatique :

« On ne protège bien que ce qu'on connaît bien ».

Les équipes de direction ont une vision plus globale des enjeux.

2. Le besoin de profils hybrides et les lacunes de la formation

2.1 Un profil idéal encore rare, à la croisée de la cyber et de l'automatisme

Le profil recherché pour le conseil en cybersécurité industrielle combine une formation cyber classique avec une spécialisation sur les protocoles, architectures et interfaces propres au monde industriel, une combinaison encore peu répandue sur le marché.

« L'idéal ça serait quelqu'un qui a une formation cyber comme on en a aujourd'hui, mais qui en plus a une spécialisation un peu plus forte sur les solutions et architectures industrielles, protocoles industriels [...] interfaces, supervision ».

La démarche inverse, consistant à former des automaticiens à la cybersécurité serait tout aussi pertinente, notamment pour intégrer la sécurité dès la conception des systèmes. Cette tension sur les profils se retrouve concrètement sur certains projets, où les donneurs d'ordre peinent à identifier des compétences combinant maîtrise des automatismes et sécurisation des systèmes.

2.2 Un déficit marqué de formations initiale et continue sur la sécurisation des systèmes industriels

Alors que les normes de sécurité classiques (ISO 27001) sont largement évoquées, les référentiels spécifiques à la sécurité des systèmes industriels (IEC 62443, NIST (CSF) 2.0 par exemple) restent quasiment absents des cursus. Un constat qui se retrouve également côté formation continue. Quant aux formations alliant cyber et industrie, elles sont rarissimes alors que les besoins sont eux extrêmement importants.

« Tout le monde connaît ISO 27001. par contre on parle peu des normes de sécurité des SI industriels ».

Cette lacune concerne aussi bien les jeunes diplômés que les professionnels en poste souhaitant monter en compétence sur des approches de sécurisation dès la conception (security by design) :

« Nous cherchions un cursus de formation pour former nos équipes et garantir que la sécurité soit systématiquement prise en compte dès la conception de nos livrables, ce qu'on appelle security by design [...]. Je n'ai pas trouvé de formation qui nous fasse dire génial, on va proposer ça à tout le monde ».

2.3 L'automatisme happé par l'informatique, une sensibilisation cyber encore insuffisante

La frontière entre automatisme et informatique s'estompe progressivement avec la numérisation des solutions industrielles, sans que la sensibilisation à la sécurité des automaticiens n'ait suivi ce même rythme.

« De plus en plus, la frontière entre l'informatique et l'automatisme s'estompe, et les automaticiens n'ont pas initialement été formés à penser à la sécurité. Ce n'était pas non plus une attente des clients ».

Ce décalage s'explique en partie par une fausse impression de protection héritée de l'ère analogique :

« On se sentait un peu à l'abri de tout ce qui était cyberattaques. La bascule dans l'ère du numérique, pourtant plus si récente, ne s'est pas accompagnée d'une sensibilisation et d'une prise de conscience immédiate sur les risques liés à la cyber sécurité ».

3. L'impact de l'IA et la nécessaire prise de conscience des dirigeants

3.1 L'IA, une source d'opportunités mais aussi de risques encore mal maîtrisés

L'intégration croissante de l'intelligence artificielle dans le développement de solutions industrielles fait émerger de nouveaux risques, notamment lorsque le code généré n'est pas pleinement compris par les développeurs qui l'utilisent.

« On a déjà rencontré un problème sur une ligne sur un bout de code qui avait été généré par IA et qui n'avait pas été bien compris par le développeur ».

Cette situation interroge la capacité des jeunes générations à développer une expertise technique suffisante pour challenger la production de l'IA, dans un contexte où l'usage de ces outils reste par ailleurs inégal chez les plus jeunes profils :

« pour être capable de comprendre, de relire et de challenger ce qui est produit par l'IA, il faut avoir un certain niveau de maîtrise. Comment on peut avoir cette expertise si dès la sortie de l'école on fait tout faire par des moteurs d'IA ? ».

3.2 Cloud et cryptographie post-quantique, des sujets encore distants pour l'industrie

Le cloud et la cryptographie post-quantique restent des sujets peu investis par le secteur industriel, qui privilégie des solutions éprouvées et proches des équipements de production plutôt que des innovations technologiques récentes.

« Les industriels aiment bien avoir leurs solutions informatiques proches de leurs machines pour se prémunir de problématique de connexion externe et garantir un fonctionnement autonome de leur installation. L'externalisation n'est pas encore un sujet ».

Sur la cryptographie post-quantique, la maturité du secteur reste plus limitée encore, avec une préférence marquée pour des solutions validées de longue date plutôt que pour des technologies émergentes :

« L'industrie préfère s'appuyer sur des solutions éprouvées plutôt que d'aller vers des solutions très innovantes qui peuvent coûter cher. Je pense que l'on a encore un peu de temps là-dessus ».

3.3 La prise de conscience du risque cyber, un préalable porté par la direction

L'évolution vers une meilleure prise en compte de la cybersécurité dans le secteur industriel dépend largement d'une prise de conscience au niveau de la direction. Elle intervient souvent à la suite de consolidations d'entreprise qui apportent des moyens, des visions et des stratégies nouvelles ou malheureusement à la suite d'un incident…

« Ceux qui ont pris conscience des risques cyber et des enjeux ont fait évoluer leur organisation vers une plus grande collaboration entre les DSI et les directions techniques ou de production ».

Certaines organisations n'engagent cette transformation qu'après avoir subi un incident marquant, tandis que d'autres l'amorcent à l'occasion de rapprochements capitalistiques qui renforcent la structuration des fonctions informatiques. Cette prise de conscience reste toutefois conditionnée à la vision portée par la direction sur le rôle de l'informatique dans l'entreprise, entre simple centre de coûts à limiter et fonction stratégique à part entière :

« Il doit y avoir dans les CODIR quelqu'un qui porte les sujets Système d'information pour accompagner la stratégie, faire en sorte que le digital apporte de la valeur dans un contexte sécurisé ».

SCIENCES PO RENNES



FRANCK NICOL
Ancien officier général, sparring partner de dirigeants, co-directeur du master sécurité défense et intelligence stratégique de sciences po Rennes.

1. Repenser nos modèles d'enseignements

1.1 L'université doit revoir son modèle

« Les universités doivent absolument se transformer. Le modèle économique qui préexistait jusqu'à maintenant est en train de disparaître, démographiquement mais pas que ».

Ce modèle de l'Université est également sous la pression d'autres facteurs structurels majeurs, tels que la transformation numérique globale, l'émergence de nouvelles formations concurrentes, et la recherche permanente d'adéquation des diplômes aux besoins du marché de l'emploi, tout en développant l'approche par les compétences. Dans un contexte budgétaire contraint et face à la difficulté à se projeter sur le long terme (dans un contexte où les technologies évoluent très vite), l'enjeu est de doter les universités de dispositifs plus agiles pour anticiper et intégrer ces ruptures technologiques sur le long terme.

1.2 Les écoles d'ingénieurs doivent se transformer (3 modèles)

Si les cursus actuels préparent efficacement aux compétences techniques (sécurisation du SI, détection et de réponse aux incidents), la rapidité des évolutions technologiques (IA, quantique) invite à enrichir ces parcours. Au-delà des approches d'auto-formation par les défis techniques (type CTF), l'enjeu est d'apporter aux futurs ingénieurs une culture managériale, stratégique, juridique et géopolitique globale.

« La matière évolue tellement vite, elle est immatérielle (quantique, IA…), on est dans des champs assez incroyables, on est dans une révolution dans les métiers avec des conséquences qu'on ne mesure pas ».

Face à des technologies en mutation rapide (exemple outil d'attaque avec IA embarquée),

« Il faut des ingénieurs agiles, qui apprennent à apprendre, à défendre, mais aussi à attaquer. Car quand on apprend à attaquer, quand on se met à la place de l'autre, on se protège mieux ».

Pour répondre à ce défi, l'introduction de modules croisant IA et cybersécurité (prompt engineering appliqué, sécurisation des agents IA) est un levier clé de souveraineté numérique.

Pour structurer cette évolution, pour prendre en compte l'absence de frontière entre sécurité intérieure, défense et sécurité collective (fusion des espaces de confrontation physique et immatériel), trois scénarios se présentent aux écoles d'ingénieurs selon Franck Nicol :

- **L'école rempart** : l'école du domaine régalien (tout ce qui a trait à la défense et à la sécurité), pleinement intégrée dans l'écosystème de la défense nationale (COMCYBER, DGA, ANSSI). Orientée vers la cyberdéfense souveraine, elle forme des ingénieurs capables de protéger les infrastructures critiques en maîtrisant la PQC, l'IA défensive et la LIO dans un cadre strictement encadré.

- **L'école laboratoire** : ce modèle est axé sur la technique pure, l'innovation de rupture, l'IA et l'interaction avec le matériel (data centers, robots, jumeaux numériques). Il vise à sortir les enseignants chercheurs de leur isolement en créant des fablabs et des incubateurs connectés aux entreprises pour tester de nouvelles formes d'attaques et développer des projets souverains en open source.

- **L'école hybride** : ce modèle, préconisé par Franck Nicol, fusionne des modules des deux précédents. Il brise les silos en forçant la rencontre entre les ingénieurs techniques et les profils issus des sciences humaines et politiques. C'est le modèle à privilégier pour moderniser les infrastructures académiques, en finançant et en imposant des fablabs et des incubateurs au sein des écoles pour que les étudiants et chercheurs puissent tester des attaques/défenses en temps réel sur des jumeaux numériques en mode open source.

1.3 L'importance des softskills

L'ingénieur de demain ne peut plus se cantonner à la technique pure.

« Il doit être capable de parler comme un expert mais avec des mots de généraliste, d'être compris. Il doit aussi comprendre les problèmes des autres, les conséquences de ce qu'il se passe, pour que l'autorité qu'il sert, qu'il soit politique, chef d'entreprise, ou chef d'administration, comprenne ce qu'il se passe, anticipe ce qu'il pourrait se passer, et prenne les bonnes décisions ».

C'est pourquoi la cybersécurité dépasse le cadre des ingénieurs. Il faut y associer des philosophes et des anthropologues pour appréhender la transformation de la société numérique. L'accent mis sur l'ouverture d'esprit et la communication doit permettre de former des profils capables de vulgariser la complexité technique auprès des décideurs.

2. Dirigeants d'entreprises : l'urgence d'une prise de conscience

Il existe aujourd'hui un écart important entre l'urgence des enjeux cyber et les priorités opérationnelles des entreprises. Dans un contexte économique complexe, les salariés et les entrepreneurs se concentrent légitimement sur la gestion du quotidien et les impératifs à court terme, ce qui rend les discours purement prospectifs sur le numérique plus difficiles à appréhender pour une majorité d'entre eux.

Par ailleurs, l'approche purement réglementaire montre ses limites : le déploiement de normes structurantes, telles que la directive NIS2, est perçu comme un ensemble de contraintes formelles et d'objectifs chiffrés dont le sens profond n'est pas toujours explicite. Ce formalisme risque de limiter l'appropriation active du sujet par les acteurs, incitant les entreprises à s'en tenir à une logique de conformité administrative vis-à-vis de l'ANSSI, plutôt qu'à appréhender le cyberespace comme un environnement dynamique en constante évolution.

« Nos dirigeants doivent intégrer, et pas que ceux dans le numérique, qu'une entreprise ce n'est pas que ce qui est physique, mais que nous sommes dans un autre monde. Le monde numérique/virtuel est superposé à tout ça ».

En développant des jumeaux numériques qui virtualisent leurs architectures, les organisations créent aussi de nouveaux points d'accès et des vulnérabilités potentielles que des agents d'intelligence artificielle peuvent exploiter.

« C'est un autre monde. On est dedans et on peut y agir, et on peut réagir, et on peut anticiper, et on vit dans un autre champ ».

Il devient donc essentiel pour les dirigeants d'intégrer pleinement cette dimension virtuelle afin d'en saisir les opportunités (optimisation du fonctionnement de leur entreprise) et d'en maîtriser les risques (cyber criminalité…).

3. Incarner la cyber … un rôle pour des technos stratèges

Pour renforcer la portée des messages cyber et valoriser la cybersécurité comme un levier de performance économique plutôt que comme une contrainte réglementaire subie, il convient de faire évoluer les campagnes de sensibilisation de masse traditionnelles, dont l'impact reste aujourd'hui limité. L'effort d'acculturation gagne à s'orienter vers des approches immersives et des expérimentations de terrain menées avec des acteurs clés. Cette démarche cible en priorité des dirigeants moteurs, dotés d'une forte maturité professionnelle et d'une vision prospective, capables de devenir les ambassadeurs de cette transformation au sein de leur écosystème.

Pour opérationnaliser cette vision, la stratégie repose sur deux piliers majeurs :

3.1 Le concept de techno-stratège

Il est impératif de former des techno-stratèges capables de faire la liaison entre la technique et la décision politique ou économique. Tous les ingénieurs cyber ne sont pas destinés à être des techno-stratèges, car les besoins en techniciens purs restent réels.

L'enjeu est de repérer, parmi les élèves ingénieurs démontrant un fort potentiel et un intérêt marqué pour les enjeux stratégiques, que ce soit en fin de cursus ou après une première expérience professionnelle favorisant la maturité, les profils aptes à s'engager dans des parcours bi diplômants. L'adossement à des passerelles avec des instituts de sciences politiques, d'intelligence économique ou de géopolitique (tels que Sciences Po) permettra à ces profils d'associer un solide bagage technique à une maîtrise fine des rapports de force et d'influence. Ces compétences transverses les prépareront à devenir des RSSI stratégiques, pleinement outillés pour dialoguer efficacement avec les instances dirigeantes.

3.2 Incarner la réussite par une taskforce et l'expérimentation

« Il faut trouver des gens qui incarnent, non pas qui parlent, mais qui incarnent des réussites, qui font, qui réalisent ».

Face à l'immensité de la menace et à l'obsolescence des méthodes traditionnelles de sensibilisation, la gestion du risque cyber exige un changement de méthodologie : il faut adopter une posture agile orientée vers le résultat concret. L'objectif est de substituer aux discours abstraits des victoires tangibles, portées sur le terrain par des leaders reconnus :

« Vous ne pouvez pas raisonner observation-analyse-décision, ça va plutôt être observer-expérimenter. On est face à l'urgence, il faut réagir vite, aujourd'hui il faut travailler selon un mode taskforce. Quand on veut changer les choses, il faut trouver des gens idoines capables d'incarner, de peser sur le cours des choses, leur confier une mission, leur accorder une liberté d'action pour identifier les modalités. Ces personnes doivent rendre compte au plus haut niveau, ne font valider que ce qui n'est pas de leur niveau. Ils sont surtout dans l'action. »

S3NS (THALÈS)



DELPHINE CHADOZEAU
Responsable Ressources Humaines
chez S3NS



ROMAIN BRÉCHET
Deputy Chief Security Officer
chez S3NS

1. Des tensions de recrutement concentrées sur quelques profils très spécifiques

1.1 L'analyste de sécurité, un mouton à 5 pattes

Si S3NS ne rencontre pas de difficulté généralisée de recrutement, un point de tension précis se dégage en particulier autour des profils capables d'assurer des missions de supervision de la sécurité. S3NS recherche des profils fullstack, en mesure d'intervenir sur l'ensemble de la chaîne: de l'architecture à l'analyse forensique en passant par la définition des règles.

« Aujourd'hui, nous rencontrons des difficultés à trouver des profils réunissant l'ensemble des compétences recherchées et immédiatement opérationnels ». <Delphine>

Le profil recherché est une personne capable de dialoguer avec les équipes projet, de travailler sur l'architecture, de créer des règles de corrélation et, si besoin, de faire du forensic.

« On parle d'un mouton à 5 pattes [...] aujourd'hui chez S3NS, on n'en a pas beaucoup. ».

Cette tension s'explique à la fois par la rareté de ces profils et par l'évolution des modèles d'organisation et de recrutement : *« ces métiers-là sont en tension [...] pas uniquement parce qu'ils sont rares, c'est aussi une question liée à nos exigences de recrutement jusqu'à présent ».*

En effet, les organisations ont longtemps privilégié un découpage en silos étanches (niveaux L1, L2, L3) et recherché une spécialisation très pointue sur un maillon unique (comme l'analyse forensic). Ce modèle d'organisation cloisonné montre aujourd'hui ses limites dans des environnements opérationnels de plus en plus hétérogènes. Dès lors, la difficulté rencontrée par les recruteurs ne relève pas tant d'un manque d'expérience ou de séniorité sur le marché que de la rareté de candidats disposant d'une compréhension globale de l'infrastructure et de la chaîne de détection.

1.2 Le reverse engineering, une expertise particulièrement rare

À l'inverse, le reverse engineering représente un besoin volumétrique faible mais une compétence extrêmement difficile à recruter.

« Ces profils sont particulièrement rares. La spécificité de la discipline nécessite une recherche approfondie ». <Romain>

Sur ces profils, l'alternance atteint aussi ses limites :
« C'est une vocation le reverse engineering [...] Pour un stagiaire qui ne s'est pas déjà familiarisé avec cette discipline, la marche peut être importante et nécessite un accompagnement soutenu du maître de stage ».

2. L'impact de l'IA et l'anticipation des ruptures technologiques

2.1 L'IA comme levier d'efficacité, non comme substitut aux compétences humaines

« Tous les métiers que nous connaissons aujourd'hui vont devoir s'adapter et intégrer l'IA. […] Celle-ci répondra à un besoin d'efficacité, mais n'a pas vocation, dans notre vision, à remplacer les compétences humaines ».

L'ensemble des métiers de la cybersécurité devront progressivement intégrer l'IA dans les prochaines années. Il s'agit toutefois d'un gain d'efficacité et non d'une substitution aux compétences humaines, y compris sur des métiers pointus comme le reverse engineering.

« Nous sommes encore au début de la courbe d'apprentissage. […] Nous devons apprendre à travailler avec ces nouveaux outils et à en maîtriser les usages ».

2.2 Anticiper les 5 à 6 prochaines années

L'automatisation croissante de certaines tâches de premier niveau pourrait modifier les conditions d'intégration et d'apprentissage des jeunes profils, sans qu'une réponse claire n'existe encore pour anticiper ce risque. Un enjeu se pose alors à plus long terme : comment former les profils expérimentés de demain si les juniors disposent de moins d'occasions d'acquérir leurs premières expériences opérationnelles ?

« Nous devons anticiper l'impact de ces évolutions sur les cursus et sur les parcours des juniors, afin d'éviter un déficit de profils expérimentés dans cinq ou six ans».<Delphine>

Ce risque ne tient pas à un remplacement réel des juniors par l'IA, mais à une mauvaise interprétation de ce qu'elle peut réellement prendre en charge :

« L'IA ne doit pas être considérée comme un moyen de remplacer les collaborateurs. En revanche, elle devient indispensable pour améliorer l'efficacité de certaines activités. ».

2.3 Sécuriser l'IA comme nouvelle infrastructure à part entière

« L'IA est un outil, mais c'est aussi une infrastructure […] Nous protégeons nos applications ; nous devons appliquer le même niveau d'exigence aux systèmes d'IA, qui introduisent eux aussi de nouveaux risques. » <Romain>

Au-delà de l'usage de l'IA comme outil d'aide à la productivité, elle constitue elle-même une infrastructure à sécuriser, ce qui fait émerger de nouveaux besoins de compétences liés à son déploiement (on-premise ou SaaS) et à la maîtrise de ses risques spécifiques.

Chez S3NS, les expérimentations sont cadrées autour d'objectifs identifiés. Des ressources internes développent également leurs compétences sur ces sujets afin de faire émerger des projets répondant à des enjeux concrets pour l'entreprise.

2.4 Ruptures technologiques : cryptographie post-quantique et cloud de confiance

La cryptographie post-quantique fait déjà l'objet de travaux concrets chez S3NS, en s'appuyant notamment sur les avancées technologiques disponibles dans l'écosystème Google Cloud.

Pour opérer et sécuriser un cloud de confiance, deux types de compétences se distinguent : celles des SRE[6], qui

6 SRE = Site Reliability Engineering = discipline à la croisée de l'ingénierie logicielle et de l'administration système, visant à automatiser l'exploitation des infrastructures complexes pour en garantir la disponibilité, la scalabilité et la sécurité continue.

gèrent l'infrastructure sous-jacente à l'échelle d'un hyperscaler[7], et celles liées à l'usage sécurisé des services cloud par nos équipes projets et clients.
Certaines compétences nécessaires à l'exploitation d'infrastructures cloud à très grande échelle ne s'acquièrent pas uniquement dans les cursus académiques. Elles se développent également par l'expérience opérationnelle et la pratique.

Sur le second volet, un besoin de renforcement des cursus se fait sentir, notamment autour de la configuration sécurisée des environnements cloud :

« Une part importante des incidents de sécurité dans le cloud est liée à des erreurs de configuration plutôt qu'à l'exploitation de vulnérabilités inédites. La formation sur ce volet doit encore progresser.» <Romain>

3. Formation, écoles et attractivité de la filière

3.1 Un dialogue avec les écoles à renforcer sur l'IA

Le lien avec les écoles s'appuie notamment sur une structure dédiée au sein de Thales, à laquelle S3NS fait remonter ses besoins et les évolutions observées sur les métiers :

« certains sont pris en considération, d'autres sont un peu plus compliqués à développer […] on travaille notamment avec l'EFREI […] S3NS a été notamment le sponsor de la création d'une majeure ». <Delphine>

Le rythme particulièrement rapide des évolutions liées à l'IA peut cependant créer un décalage avec le temps nécessaire à l'adaptation des cursus académiques. Les jeunes les plus intéressés par ces technologies se tournent alors vers des entreprises spécialisées pour approfondir leurs connaissances et continuer à progresser.:

« Les technologies d'IA évoluent extrêmement rapidement. Les écoles doivent pouvoir anticiper davantage ces transformations, même si l'entreprise conserve naturellement un rôle essentiel dans le développement des compétences les plus récentes ».

3.2 Des compétences techniques solides, une vision d'ensemble à développer

Le niveau technique atteint par les jeunes diplômés est élevé, souvent supérieur à celui des recruteurs actuels au même stade de carrière, mais une hyperspécialisation limite leur capacité à prendre du recul face à des problèmes plus larges que leur périmètre technique initial.

« Le niveau technique a considérablement progressé et les jeunes diplômés sont souvent très performants dans leur spécialité […] L'étape suivante consiste à les aider à élargir leur analyse et à répondre à des problématiques dépassant leur périmètre technique immédiat ».

Ce constat est relié à l'évolution des cursus, davantage centrés sur des compétences techniques immédiatement opérationnelles qu'il y a quelques années. Leur capacité d'adaptation reste néanmoins un point positif, notamment grâce à leur familiarité avec des environnements technologiques en évolution rapide.

En revanche, il est nécessaire de continuer à développer les compétences soft skills dans le parcours de formation :
« Nous recherchons des personnes qui disposent des compétences techniques attendues, mais qui savent également travailler en groupe et répondre à des problématiques complexes avec le savoir-être approprié. Cette composante n'est pas encore suffisamment intégrée dans les parcours scolaires. ». <Delphine / Romain>

7 Gigantesque fournisseur de services cloud (tel que Google Cloud, AWS ou Microsoft Azure) disposant d'infrastructures informatiques à très grande échelle, capables d'adapter dynamiquement leurs ressources financières et techniques pour traiter des volumes massifs de données à l'échelle mondiale.

3.3 La féminisation des métiers techniques, un enjeu qui se construit dès l'orientation

La représentation des profils féminins reste très déséquilibrée au sein de l'entreprise, concentrée sur les métiers de conformité et quasi absente sur les métiers techniques :

« on doit être à 18 % de femmes au sein de l'entreprise, dont une très grande partie dans les directions commerce et support. Côté SRE […], le taux de femmes est plus proche des 7 % ou 8 % ». Les raisons de cette sur-représentation des femmes dans les métiers de la conformité restent posées sans réponse tranchée.

Ce déséquilibre se construit bien avant le recrutement et renvoie notamment aux choix d'orientation, à la représentation des métiers techniques et aux modèles auxquels les jeunes filles sont exposées. Les jeunes filles intéressées par le numérique sont par ailleurs souvent mises en avant sur des métiers transversaux plutôt que techniques, ce qui limite l'effet d'entraînement par des modèles inspirants :

« Les femmes sont encore souvent mises en avant sur des sujets réglementaires, comme NIS2, ou dans les métiers de la gouvernance, des risques et de la conformité, et moins sur les fonctions techniques. Il reste donc un travail important à mener sur l'attractivité de ces métiers et la visibilité des parcours féminins. ». <Delphine>

SOPRA STERIA

MADAME C
Collaboratrice Sopra Steria

1. Une inversion du marché des jeunes diplômés et un déplacement des attentes vers la posture

1.1 Un marché junior qui s'est retourné en quelques années

Alors qu'il y a quelques années le marché de la cybersécurité souffrait d'une pénurie de profils juniors, la multiplication des formations spécialisées a inversé la tendance, avec aujourd'hui davantage de candidats juniors que de postes ouverts.

« Il y a une vraie inversion sur le marché des jeunes diplômés, où on a plus de candidats que de besoins […] on rencontre une explosion de profils juniors, et plus de profils juniors sur le marché que de besoins ouverts ».

Ce recentrage s'explique aussi par l'évolution des besoins clients, avec une activité junior en partie réduite par l'IA :

« Avec l'évolution de l'IA, on a peut-être moins aussi d'activité pour des profils juniors qu'au préalable ».

Le volume de recrutement junior reste néanmoins stable plutôt qu'en déclin : sur un plan de recrutement annuel de 160 personnes pour l'entité cyber, environ 50 correspondent à des jeunes diplômés, complétés par 70 stagiaires et alternants.

« On continue à recruter des profils juniors mais on n'augmente pas ce volume, on le stabilise ».

1.2 La posture, première compétence attendue d'un junior

Dans un modèle de société de service, la compétence prioritaire recherchée chez un jeune diplômé n'est pas d'abord technique, mais comportementale : la capacité à interagir avec un client, à reconnaître les limites de ses connaissances et à faire preuve de transparence.

« Ça va être vraiment sa posture. Est-ce qu'il est capable d'écouter un client ? C'est sa capacité à dire qu'il ne le sait pas. Ne pas savoir, ce n'est pas grave. On prend l'information, on pose la question, et on va rechercher la réponse ».

2. Des tensions concentrées sur les profils hybrides et expérimentés

2.1 Le manque de profils alliant expertise technique et management

La difficulté de recrutement la plus marquée porte sur les profils seniors capables de conjuguer expertise technique et compétences managériales, un double profil nécessaire à l'accompagnement des équipes plus juniors et jugé rare sur le marché.

« Là où on a des difficultés, c'est sur les profils qui ont à la fois l'expertise technique et le management, là où

on a le plus de difficultés en volumétrie, c'est d'avoir des personnes qui sont à la fois techniques et qui soient capables d'être managers ».

Cette double compétence est en partie travaillée en interne via des dispositifs de mise en situation, notamment un rôle de tutorat confié à des profils de 2 à 5 ans d'expérience, davantage que par un problème de catalogue de formation.

2.2 L'émergence de profils à double compétence IA et cybersécurité

Une nouvelle catégorie de profils, alliant recherche en intelligence artificielle et cybersécurité, commence à être recrutée, bien qu'elle reste très rare sur le marché. Deux approches sont mobilisées en parallèle : des data analysts formés ensuite à la cyber, et des profils issus de la recherche (doctorat) accompagnant la réflexion prospective sur l'impact de l'IA chez les clients.

« On commence à recruter des profils qui ont la double compétence IA et cyber. Ils sont très très durs à trouver sur le marché puisque c'est quand même très rare ».

Cette dynamique reste à ce stade orientée recherche et anticipation plutôt que déploiement à grande échelle :

« Aujourd'hui on fait plus de la recherche sur l'IA, la cyber, et on ne serait pas en capacité de dire ce que vont rechercher nos clients dans 5 ans ».

2.3 Une exigence croissante mais sans réel bouleversement pour les compétences cloud

Sur les compétences cloud, la croissance du recrutement se poursuit sans difficulté majeure de fond, mais les attentes des équipes opérationnelles restent élevées, ce qui allonge les délais de recrutement plutôt que de créer une véritable pénurie.

« On arrive quand même à en trouver, jamais aux attentes que nos opérationnels ont. Ils veulent tant de personnes seniors qui ont cette capacité expertise/management, et au final, ils vont voir des candidats qui n'ont pas forcément le niveau qu'on attend ».

3. Anticipation des ruptures réglementaires et enjeux d'inclusion de la filière

3.1 NIS2 et post-quantique, des sujets encore en phase d'anticipation

La montée en puissance des besoins liés à NIS2 est jugée plus lente qu'anticipé, avec une croissance des demandes clients attendue plutôt pour 2027. Une double compétence juridique et technique est nécessaire pour accompagner efficacement les clients sur ce terrain.

« On commence à avoir des demandes qui émergent, mais un petit peu moins vite qu'on le pensait. Je pense plutôt que c'est en 2027 qu'on aura un gros boom ».

Sur la cryptographie post-quantique, la structuration reste également embryonnaire, portée par une petite équipe dédiée :

« On a une petite équipe, à date on a peu de demandes. On essaie de l'anticiper, de structurer, de faire des recherches, beaucoup de veille ».

3.2 La féminisation de la filière, un objectif structuré mais des équilibres encore fragiles au fil de la carrière

Le taux de femmes au sein de la business line cyber avoisine 27%, un niveau au dessus des moyennes du secteur, mais encore éloigné d'une équité recherchée via des dispositifs internes (collectif Women in Cyber, partenariat CEFCYS). On observe un phénomène de départ des profils féminins du domaine technique vers 35-40 ans, en parallèle d'un intérêt croissant de profils en reconversion à ce même âge.

« On a quand même pour objectif de féminiser. On a un taux qui est très bien par rapport au secteur d'activité, mais là où nous avons le plus de difficultés, c'est qu'il y a beaucoup moins de femmes dans les écoles d'ingénieurs cyber que d'hommes ».

Un travail est engagé pour mieux intégrer les profils féminins en reconversion professionnelle issus de parcours non IT.

La conclusion de Madame C.

« Moi, je pense qu'on a besoin de personnes qui sont capables d'anticiper et de se former à tout ce qui va venir, tout ce qui va évoluer, puisqu'il y aura sûrement beaucoup de changements pour eux. Il faut vraiment qu'ils soient plus souples, de manière à ce qu'ils puissent être agiles et s'adapter ».

UNIVERSITÉ CÔTE D'AZUR



MARINA TELLER
Professeure de droit à l'université Côte d'Azur

1. Le droit doit s'emparer du risque cyber

1.1 Une matière encore cantonnée aux marges du droit bancaire

Dans le monde universitaire, les enjeux cyber restent aujourd'hui abordés de manière très ciblée, essentiellement à travers les grands textes réglementaires européens (DORA, NIS2) qui s'imposent aux acteurs systémiques, sans être intégrés de façon transversale aux autres branches du droit.

« Je ne suis même pas certaine que dans la plupart des Masters 2 spécialisés en droit bancaire et financier, cette question de la résilience des risques cyber soit vraiment au cœur des formations ».

Une comparaison est faite avec la trajectoire du droit de l'environnement, longtemps traité comme une branche à part avant de devenir une composante transversale de l'ensemble des disciplines juridiques : *« la thématique des cyber risques devrait innerver à présent quasiment toutes les branches du droit ».*

Ainsi, il faudrait que dans tous les masters de droit (pas uniquement ceux en droit bancaire ou financier), il y ait une sensibilisation aux risques cyber pour irriguer tous les domaines d'activités.

1.2 Un module pionnier pour anticiper le risque quantique

Un certificat spécifique, intégré à un Master de droit bancaire et Fintech, a été mis en place pour sensibiliser des étudiants juristes à des sujets encore peu traités dans le paysage académique, dont la menace que représente l'ordinateur quantique pour les infrastructures financières.

« On a commencé à essayer de se projeter, de faire un exercice de prospection juridique, pour imaginer ce qui peut se passer pour le secteur financier mondial, si l'ordinateur quantique permettait par exemple de hacker une blockchain telle que Bitcoin ».

Ce travail s'inspire des méthodes utilisées dans le domaine militaire, avec des exercices de gestion de crise en mode cellule de crise. Il s'agit d'une initiative individuelle plutôt que d'une orientation portée par l'institution :

« Cela tient beaucoup à ma démarche personnelle en tant qu'enseignant chercheur et ce n'est pas du tout représentatif de ce que l'université peut offrir dans sa généralité ».

1.3 Des entreprises de plus en plus demandeuses de profils hybrides

Le regard des employeurs sur ce type de formation a évolué ces dernières années, ce module étant désormais perçu comme un véritable atout pour les étudiants plutôt que comme un contenu déconnecté de la réalité du métier.

« Il y a peut-être 5, 6 ans, les entreprises me disaient : « c'est intéressant, mais c'est pas du tout abordé dans nos métiers, et c'est très loin des réalités du terrain ». Puis, de plus en plus, les entreprises ont commencé à dire que c'était précisément pour cette raison qu'elles avaient choisi de recruter un étudiant ayant suivi cette formation ».

Ce constat reste toutefois à nuancer à l'échelle de l'organisation dans son ensemble : le dialogue entre juristes et les autres métiers du risque demeure limité par un fonctionnement encore très cloisonné, en particulier sur des sujets aussi nouveaux que le risque quantique, initialement peu identifié par les grands acteurs bancaires.

2. Repenser la pédagogie face à l'accélération numérique

2.1 Sortir du cours magistral par des mises en situation concrètes

Face à des sujets qui évoluent rapidement et à une génération d'étudiants qui a un accès immédiat à l'information, les formats pédagogiques les plus efficaces reposent moins sur la transmission de connaissances que sur des mises en situation actives.

« Aujourd'hui l'information est en ligne donc parfaitement accessible. Mais les étudiants ont besoin de nous pour leur mettre le pied à l'étrier sur des enjeux majeurs ».

Des exercices comme une négociation internationale fictive sur la non-prolifération des technologies quantiques ou l'écriture de scénarios d'attaque ont suscité une forte adhésion.

2.2 Une génération d'étudiants en demande de collectif

« On a une génération d'étudiants qui est très angoissée. Il faut donc leur montrer comment raisonner à plusieurs, en insistant sur le collectif. Cela permet de contrebalancer des modèles de formations qui isolent beaucoup, à l'image de la société ».

Au-delà de l'aspect pédagogique, ces formats de travail en groupe répondent aussi à un besoin plus large chez les jeunes générations, confrontées à un contexte anxiogène et à des formations jugées parfois isolantes. Le travail collectif permet également de développer des compétences transversales en coopération, en communication.

2.3 Le retour du tronc commun face à la sur-spécialisation

L'évolution du système d'enseignement supérieur vers des formations professionnalisantes, pensées pour rendre l'étudiant immédiatement opérationnel sur un métier précis, s'est faite au détriment d'un socle de culture générale partagé, pourtant nécessaire pour appréhender des sujets transversaux comme les risques cyber.

« On a spécialisé énormément au niveau des M2, au détriment d'un tronc commun général de connaissances qui se perd très vite dès la licence. On forme de plus en plus des profils d'experts et de moins en moins des étudiants polyvalents, qui auront la capacité d'être curieux dans différents sujets ».

Une piste évoquée consisterait à inscrire un module cyber dans chaque référentiel de formation (fiches RNCP), quel que soit le métier visé, plutôt que de réserver ce sujet aux seules filières numériques.

3. Une prise de conscience encore très inégale, jusque dans les institutions publiques

3.1 Un déficit de sensibilisation qui dépasse largement le monde de l'entreprise

Le manque de culture numérique et de vigilance sur les enjeux cyber ne se limite pas aux petites structures : il touche aussi des institutions publiques et des environnements a priori sensibilisés à la protection des données.

Ce constat illustre un enjeu de sensibilisation qui reste à construire à tous les niveaux, y compris chez les agents publics eux-mêmes, en dehors des équipes directement opérationnelles sur ces sujets.
Tous les acteurs (public privé, institutionnels) gagneraient ainsi à être alertés et formés aux risques cyber dans les nouvelles technologies.

3.2 L'importance des softskills : empathie et culture numérique

Deux compétences transversales sont identifiées comme prioritaires pour les années à venir : la capacité à se mettre à la place de notre interlocuteur pour mieux comprendre son positionnement et ses réactions, et une compréhension minimale du fonctionnement des outils numériques utilisés au quotidien.

« Le numérique nous habitue à avoir la satisfaction immédiate de tous nos besoins, ce qui fabrique des individus impatients et égotiques. C'est un enjeu majeur, celui de l'apprentissage de l'empathie et du vivre ensemble ».

Sur le second point, le même constat vaut pour l'usage des outils numériques eux-mêmes : *« on nous a mis des outils dans les mains sans nous apprendre véritablement à nous en servir, là où on exige un permis de conduire avant de conduire une voiture »*. Un travail de sensibilisation dès le plus jeune âge est nécessaire pour construire cette culture numérique de base.

3.3 La régulation, un levier nécessaire mais qui doit s'accompagner de pédagogie

Face à la lenteur de la prise de conscience spontanée des acteurs économiques, la réglementation reste jugée indispensable pour accélérer la mise en conformité, en complément d'un travail de fond sur la sensibilisation plutôt qu'en substitution.

« Si l'on n'avait pas ces textes qui, à un moment donné, peuvent devenir punitifs et donner lieu à des sanctions, l'inertie serait bien plus lourde. L'alternative serait de laisser des acteurs privés développer leurs propres outils de régulation, ce qui ne me convient pas. »

Ce constat s'accompagne d'une observation empirique sur le comportement des acteurs économiques face au risque :

« Qu'est-ce qui pousse une entreprise à prendre, à un moment donné, la mesure du risque cyber ? C'est soit qu'elle est elle-même victime d'une cyberattaque, soit qu'elle est sanctionnée. Tant qu'elle n'est pas exposée à la menace, elle n'en tient pas compte. »

UNIVERSITÉ CÔTE D'AZUR



CHRISTIAN TAFANI
Université Côte d'Azur
Docteur en sciences de l'information et référent national pour les nouvelles technologies auprès du Secrétariat général de la Garde Nationale

1. Former à des métiers en profonde mutation

1.1 L'obsolescence accélérée des compétences techniques

L'évolution extrêmement rapide des technologies impose aujourd'hui de repenser notre manière de former les étudiants. Une partie des métiers auxquels ils se préparent connaîtra, dans les prochaines années, des transformations majeures, tandis que d'autres apparaîtront sous l'effet des progrès de l'intelligence artificielle et de l'automatisation.

« Cette réalité doit néanmoins être expliquée avec lucidité aux futurs diplômés. Leur véritable compétence résidera moins dans la maîtrise d'un outil donné que dans leur capacité à apprendre, à s'adapter et à évoluer tout au long de leur parcours professionnel ».

Cette évolution concerne également certaines compétences techniques qui semblaient constituer un socle incontournable, comme le développement informatique. L'intelligence artificielle modifie déjà profondément les méthodes de production logicielle et conduit à s'interroger sur la nature même des compétences qui devront être développées demain.

1.2 Revenir aux fondamentaux pour mieux préparer l'avenir

Face à cette accélération des changements, il paraît essentiel de ne pas concentrer l'enseignement uniquement sur les outils et les logiciels du moment. Ceux-ci évoluent rapidement et peuvent devenir obsolètes en quelques années.

À l'inverse,
« Une connaissance approfondie des principes fondamentaux, de l'histoire des technologies et des mécanismes qui ont conduit aux architectures actuelles constitue un investissement durable. Comprendre les origines d'une discipline permet de mieux appréhender les évolutions futures ».

Cette démarche trouve une illustration dans l'enseignement de la cryptologie, dont les principes remontent à l'Antiquité, ou dans l'étude de langages historiques tels que le COBOL ou le FORTRAN. Il ne s'agit pas de former aujourd'hui des spécialistes de ces technologies anciennes, mais de montrer comment elles ont contribué à construire les environnements numériques contemporains.

« Cette perspective historique apporte aux étudiants un recul intellectuel précieux. En comprenant les étapes qui ont façonné les technologies actuelles, ils développent une capacité d'analyse et d'adaptation bien plus solide que celle reposant sur la seule maîtrise d'outils appelés à évoluer rapidement ».

1.3 La culture générale, un levier essentiel de la formation

L'observation des étudiants de niveau master met en évidence un déficit préoccupant de culture générale, historique, géographique, géopolitique ou linguistique. Cette situation constitue un véritable handicap pour appréhender les enjeux contemporains de la cybersécurité.

En effet,
« Les menaces cyber ne peuvent être comprises sous leur seul angle technique. Elles s'inscrivent dans des contextes internationaux complexes, où se mêlent considérations stratégiques, économiques, diplomatiques et culturelles ».

Former des spécialistes capables d'appréhender cette complexité suppose donc de développer une véritable culture de l'environnement dans lequel ils exerceront leurs responsabilités.

« La maîtrise de la langue française constitue également un enjeu majeur. De nombreux jeunes ingénieurs possèdent d'excellentes compétences techniques, mais rencontrent encore des difficultés lorsqu'il s'agit de rédiger une note de synthèse ou de présenter clairement une analyse à des décideurs non spécialistes ».

Or les responsabilités auxquelles ils sont destinés exigeront précisément cette capacité à expliquer, convaincre, et dialoguer avec des interlocuteurs issus d'horizons très différents. Les compétences techniques ne sauraient se substituer aux qualités rédactionnelles, à l'esprit de synthèse et à la culture générale, qui constituent désormais des compétences professionnelles à part entière.

2. La transversalité et les compétences humaines : des atouts stratégiques

2.1 Décloisonner les disciplines pour mieux appréhender la complexité

Le système de formation français demeure largement fondé sur une spécialisation précoce des parcours.
« Cette organisation montre aujourd'hui ses limites face à des problématiques complexes, telles que la cybersécurité, qui mobilisent simultanément des dimensions techniques, juridiques, humaines, économiques et géopolitiques ».

Le risque est de former des experts éprouvant davantage de difficultés à appréhender les interactions entre les différentes composantes d'une même problématique. Or les défis contemporains exigent précisément cette capacité à croiser les regards et à articuler plusieurs champs de compétences.

Il paraît donc souhaitable d'encourager des parcours plus ouverts, permettant aux étudiants d'acquérir une véritable culture interdisciplinaire. L'objectif n'est pas de faire de chacun un spécialiste de toutes les disciplines, mais de former des professionnels capables de dialoguer avec des experts issus d'autres domaines.

2.2 Encourager la double compétence sans céder à la logique de l'obligation

Le développement des doubles compétences constitue une évolution particulièrement prometteuse. Les organisations recherchent de plus en plus des profils capables d'associer, par exemple, des compétences techniques et juridiques, scientifiques et managériales, ou encore informatiques et géopolitiques.

« Pour autant, cette évolution ne me paraît pas devoir être imposée de manière uniforme à l'ensemble des cursus. Une obligation réglementaire risquerait de produire un effet inverse à celui recherché, en conduisant certains établissements à créer des enseignements répondant davantage à une exigence administrative qu'à une véritable ambition pédagogique ».

Il semble préférable d'encourager les initiatives, de valoriser les parcours atypiques et de favoriser les passerelles entre disciplines. La qualité d'une double compétence repose avant tout sur la cohérence du projet de formation et sur la motivation de l'étudiant, davantage que sur le respect d'une obligation formelle.

2.3 La réflexion éthique et philosophique : une composante indispensable de la formation

Les métiers de la cybersécurité, du renseignement ou de l'investigation numérique confrontent quotidiennement les professionnels à des situations complexes qui exigent une grande rigueur intellectuelle. L'analyse d'une menace, d'un groupe d'attaquants ou d'une opération d'influence suppose de distinguer les faits des jugements de valeur.

« L'expérience montre que certains étudiants abordent spontanément ces questions sous un angle essentiellement moral. Cette sensibilité constitue une richesse, mais elle peut parfois rendre plus difficile l'exercice d'une analyse strictement factuelle, indispensable dans les métiers de la sécurité et du renseignement ».

Développer le sens critique apparaît dès lors comme une mission essentielle de l'enseignement supérieur. Il ne s'agit pas d'apprendre aux étudiants ce qu'ils doivent penser, mais de leur apprendre à construire un raisonnement, à confronter des points de vue, à distinguer les faits des opinions et à exercer leur libre arbitre.

« Dans cette perspective, la philosophie, la géopolitique, l'histoire et les sciences humaines occupent une place fondamentale. Elles permettent de développer l'ouverture d'esprit, l'empathie, la capacité à comprendre des logiques culturelles différentes ainsi que le recul indispensable face à des situations souvent complexes ».

3. Université, entreprises et décideurs : construire une culture commune de l'anticipation

3.1 Renforcer le dialogue entre l'université et le monde économique

Le rapprochement entre l'université et les entreprises constitue aujourd'hui un enjeu majeur pour adapter les formations aux évolutions rapides des métiers. Si certaines écoles ont développé depuis longtemps des relations étroites avec le monde économique, l'université reste parfois plus prudente dans cette démarche.

Cette réserve s'explique en partie par une tradition académique attachée à l'indépendance de l'enseignement supérieur. Toutefois, cette exigence d'indépendance ne doit pas empêcher un dialogue régulier avec les acteurs économiques afin de mieux identifier les compétences émergentes et les besoins des organisations.

« Il ne s'agit naturellement pas de laisser les entreprises définir les contenus pédagogiques, mais de construire un partenariat équilibré dans lequel chacune des parties apporte son expertise. L'université conserve pleinement sa liberté académique, tandis que les entreprises contribuent à mieux faire connaître les réalités opérationnelles ».

De nombreuses initiatives locales démontrent déjà l'intérêt de cette coopération. Les rencontres entre étudiants, enseignants et industriels favorisent non seulement une meilleure connaissance des métiers, mais facilitent également l'insertion professionnelle des jeunes diplômés.

3.2 Préparer les étudiants aux réalités concrètes de la vie professionnelle

L'acquisition de connaissances scientifiques et techniques de haut niveau constitue naturellement la mission première de l'enseignement supérieur. Cependant, cette formation gagnerait à être complétée par un apprentissage plus systématique des compétences pratiques qui conditionnent l'entrée dans la vie professionnelle.

« Certains étudiants, pourtant brillants sur le plan académique, se trouvent démunis lorsqu'ils doivent accomplir des démarches pourtant essentielles : rechercher un stage, identifier des entreprises susceptibles de les accueillir, préparer un entretien de recrutement ou développer un premier réseau professionnel ».

Cette situation révèle une insuffisance de l'accompagnement proposé durant leur parcours universitaire. Former un étudiant, ce n'est pas seulement lui transmettre des connaissances ; c'est également lui donner les outils qui lui permettront de valoriser ses compétences et de construire progressivement son projet professionnel.

3.3 Développer une véritable culture du risque cyber chez les dirigeants

La sensibilisation des dirigeants de PME aux risques cyber demeure un défi majeur. Malgré la multiplication des campagnes d'information, les résultats restent souvent en deçà des attentes.

« Une partie importante des dirigeants continue de percevoir le risque cyber comme une menace abstraite ou improbable. Cette perception conduit fréquemment à repousser les investissements de prévention jusqu'à la survenue d'un incident. Pourtant, les conséquences d'une cyberattaque peuvent être particulièrement lourdes pour une PME : interruption de l'activité, perte de données, atteinte à la réputation, difficultés financières ou responsabilité juridique ».

À cette sous-estimation du risque s'ajoute une contrainte économique bien réelle. Les investissements nécessaires pour mettre en œuvre une politique de cybersécurité efficace représentent un coût parfois difficile à assumer pour les petites structures. Il est donc indispensable de poursuivre les actions de sensibilisation, mais également de développer une approche plus pragmatique, adaptée aux réalités des PME. La cybersécurité ne doit plus être perçue comme une dépense exceptionnelle, mais comme un investissement participant directement à la continuité de l'activité et à la pérennité de l'entreprise.

Conclusion :

Les transformations technologiques actuelles imposent de repenser en profondeur la formation en cybersécurité.

« Si la maîtrise technique demeure indispensable, l'efficacité des futurs professionnels reposera tout autant sur leur capacité à comprendre un monde complexe, à mobiliser une culture générale pluridisciplinaire et à faire preuve d'un esprit critique aiguisé ».

Concrétiser cette ambition exige d'encourager la transversalité des parcours et de sceller un dialogue durable entre l'enseignement supérieur, le monde économique et les institutions publiques. En définitive, former aux métiers de demain ne réside pas dans la simple transmission d'outils voués à devenir obsolètes, mais dans l'apprentissage permanent, la curiosité et l'exercice du discernement face à des environnements en constante évolution.

NOTES :

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org
02 23 06 10 30 | contact@pole-excellence-cyber.org