PÔLE D'EXCELLENCE CYBER

ÉVOLUTION DES MÉTIERS ET COMPÉTENCES EN CYBERSÉCURITÉ

Un axe stratégique pour la Bretagne

Octobre 2023

PRÉFET DE LA RÉGION BRETAGNE
Liberté
Égalité
Fraternité

Direction régionale de l'économie, de l'emploi, du travail et des solidarités

apec

Région BRETAGNE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Table des matières

Étude :

Co-écrite par le Pôle d'excellence cyber, Monsieur Patrick ERARD, Délégué général adjoint, en charge de l'axe formation, et ConseilSI, Monsieur Jehan du FRETAY, Maître d'oeuvre en système d'information.

Conception, maquette :

Madame Naïké FREMIN du SARTEL, Responsable communication du Pôle d'excellence cyber & Monsieur Dylan MASSIEUX, adjoint communication.

Remerciements

Nous remercions chaleureusement pour leur collaboration et leur aide précieuse, pour les documents fournis ainsi que pour leurs conseils avisés :

- L'Association pour l'emploi des cadres :

  - Direction des données et études : Pierre Lamblin, Emmanuel Kahn, Sébastien Thernisien, Gaël Bouron, Caroline Legrand, Kaoula Ben Messaoud.

  - Délégation régionale Apec Bretagne : Olivier Maurin.

- Les gens de la **Direction de l'orientation et de la prospective emploi-compétences (DOPEC) du Conseil Général de Bretagne (CRB) :**

  - Madame Laurence JOUAN, **Directrice du Service animation et prospective emploi-compétences (SAPEC)** ;
  - Madame Anne-Véronique CAP, **Cheffe du Service information, orientation et évolution professionnelle (SIOEP)**;
  - Madame Céline ATTAGNANT, **Chargée de mission Emploi-Formation-Orientation.**

- Les gens de la **Direction régionale de l'économie, de l'emploi, du travail et des solidarités (DREETS) de Bretagne - Préfecture de la région Bretagne** :

  - Monsieur Fabrice GILLARD, **Délégué Régional à l'Accompagnement des Reconversions,** Pôle 3E, Économie, Entreprises, Emploi, Service Mutations économiques, **DREETS Bretagne**,
  - Monsieur Jérôme LAINE, **Délégué à l'information stratégique et à la sécurité économiques**, Service de l'information stratégique et de la sécurité économiques (Sisse), **DREETS Bretagne,**
  - Monsieur Damien BEGOC, **Référent cyberdéfense-cybersécurité**, Correspondant DGA, de la **DREETS Bretagne**.

AVANT PROPOS

C'est en 2014 que le Pôle d'excellence cyber fut créé sous l'égide du ministère des Armées et de la Région Bretagne, une association de loi 1901 qui a vocation à développer l'écosystème de la cybersécurité et de la cyberdéfense sur trois axes, la formation, la recherche et le développement industriel et économique, cela depuis la Région Bretagne avec un rayonnement national, européen et international. Il associe des acteurs civils et militaires, publics et privés, académiques et industriels, en s'appuyant sur leurs compétences et leurs champs d'intervention respectifs.

En 2017 l'étude-action n°2017-25 avait été commandée à l'Agence pour l'Emploi des Cadres (APEC) et au Pôle d'excellence cyber par la Région Bretagne et la DREETS, elle portait sur l'emploi formation et était financée dans le cadre du contrat de plan État-Région (CPER) : « La cybersécurité en Bretagne : l'enjeu des compétences ». Depuis sa création, le Pôle d'excellence cyber stimule l'offre de formation cyber (qu'elle soit initiale ou continue) afin que chaque acteur dispose des ressources nécessaires pour répondre aux besoins de développement d'une filière souveraine et européenne en cybersécurité. Il promeut la recherche académique en adéquation avec les besoins des ministères, des industries et des entreprises de services du numérique (ESN), il soutient et participe au développement économique de la filière en définissant et en mettant en œuvre avec ses membres des solutions innovantes de protection, de défense et d'investigation à destination des organisations.

Parce que le territoire breton s'était déjà spécialisé dans l'électronique et les télécom sous le général de GAULLE, avec l'implantation du CNET à Lannion, du Centre de télécommunications spatiales à Pleumeur-Bodou, puis du CELAR au Sud de Rennes, à Bruz (devenu depuis DGA-Maîtrise de l'information), parce que la Bretagne est un territoire riche de nombreux laboratoires de recherche, l'IRT[1] b<>com, les Universités bretonnes (Rennes, UBO[2] , UBS[3] : IETR[4] , IODE[5] , IRMAR[6] , IRISA[7] , Lab-STICC[8] , etc.), des Grandes Écoles civiles et militaires (CentraleSupélec, CNAM[9] , IMT-Atlantique[10] , ENS [11], ENSAI[12] , ESIR[13] , ENSSAT[14] , INSA[15] , ISEN[16] , Sciences-Po, École Navale, Écoles de Saint-Cyr Coëtquidan, École des Transmissions), des Grands Groupes (Airbus, Atos, Capgemini, Orange, Nokia, Sopra-Steria, Thales, etc.) et des ETI, PME/PMI & start-ups innovantes (Amossys, AnozrWay, Diateam, SecureIC, etc.), la Bretagne est depuis les années 60 une terre cyber. Depuis 2013 le territoire Breton n'a cessé de consolider sa place au niveau national et européen en termes de savoir-faire, d'expertise et d'implantations, avec la création du Pôle d'excellence cyber et plus récemment du Groupement Cyber des Armées[17] par le Commandement de la cyberdéfense .[18]

Les administrations et entreprises françaises sont à la recherche de talents, de compétences pour les différents métiers de la cyber, cela va de profils de techniciens aux personnes les plus pointues issues du monde de la recherche, surtout des profils ingénieurs qui oeuvrent de la conception à la vente de produits ou de services. Et dans ce monde des technologies, les tendances et les métiers évoluent vite, et les bons profils sont embauchés sans même avoir à envoyer leur curriculum vitae par des DRH ultra-connectées qui recrutent via les réseaux sociaux.

Cette étude est plus qu'une remise à jour de l'étude de 2017, car elle se veut Nationale et prend aussi en compte tant les évolutions technologiques que celles des mœurs après la difficile période post-COVID19. Dans une seconde partie de l'étude, celle-ci fera un focus sur le territoire Breton et les différents bassins d'emploi qui le constitue. Enfin, cette étude-action aura pour but de faire des recommandations au niveau National et à celui du territoire pour consolider la filière cyber française. La formation dès la troisième, recherche la parité dans les filières techniques permettront, par exemple, d'augmenter significativement la ressource pour les années à venir.

1 Institut de Recherche Technologique.
2 Université de Bretagne Occidentale.
3 Université de Bretagne Sud et son École Nationale Supérieure d'Ingénieurs de Bretagne-Sud (ENSIBS).
4 L'Institut d'Électronique et des Technologies du Numérique.
5 L'Institut de l'Ouest Droit et Europe.
6 L'institut de Recherche Mathématique de Rennes.
7 L'Institut de Recherche en Informatique et Systèmes Aléatoires .
8 Le Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance.
9 Conservatoire National des Arts et Métiers Bretagne.
10 Institut Mines-Télécom Atlantique à Brest, Rennes et Nantes .
11 L'École Normale Supérieure de Rennes à Bruz.
12 L'École Nationale de la Statistique et de l'Analyse de l'Information à Bruz.
13 L'École Supérieure d'Ingénieurs de Rennes, qui tout comme l'ENSSAT dépend de l'Université de Rennes.
14 L'École Nationale Supérieure des Sciences Appliquées et de Technologie de Lannion.
15 L'Institut National des Sciences Appliquées de Rennes.
16 L'Institut Supérieur de l'Électronique et du Numérique Yncréa Ouest à Brest.
17 Le GCA, créé le 1er septembre 2020, le GCA constitue pour le COMCYBER le support de sa montée en puissance et le lieu de développement et de décloisonnement des compétences en cyberdéfense par la création d'une entité accueillant les centres techniques.
18 Placé sous l'autorité directe du chef d'état-major des armées, le COMCYBER est un commandement opérationnel, qui rassemble l'ensemble des forces de cyberdéfense du ministère des Armées sous une autorité interarmées.

PETIT LEXIQUE INTRODUCTIF :

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

- **Cyberprotection :** Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité. La cyberprotection s'appuie notamment sur des mesures prises pour préserver la sécurité des systèmes d'information.[1]

- **Cyberdéfense :** Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

- **Cyber-résilience :** La capacité d'anticiper, de résister, de récupérer et de s'adapter à des conditions défavorables, à des tensions, à des attaques ou à des compromissions sur des systèmes qui utilisent ou sont activés par des ressources cybernétiques. [2]

Cybercriminalité : Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberespace : Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. [3]

1 Wiktionnaire - licence *Creative Commons* attribution partage à l'identique 3.0.
2 *National Institute of Standards and Technology.*
3 Autres définitions glossaire de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

INTRODUCTION

Depuis les années 80, tout comme de nombreux pays industrialisés, la France a concentré son économie sur le domaine tertiaire, pensant pouvoir vivre surtout de la production de brevets et de services au détriment des industries traditionnelles et au profit d'industries plus modernes et des nouvelles technologies qui font du pays l'un des leaders mondiaux de l'innovation : automobile, aéronautique, aérospatiale, agro-alimentaire, électronique, nucléaire civil, pharmacie, cosmétique, luxe, etc. La désindustrialisation accélérée, qui a détruit près de 500 000 emplois industriels entre 2008 et 2016, période durant laquelle l'Allemagne en créait 129 000[1], s'est aussi accompagnée d'une digitalisation des entreprises, la part du digital dans le PIB de la France étant aujourd'hui de 6%[2].

L'emploi dans les trois secteurs d'activité de l'économie française en 2020

	Millions d'emplois	% du total
Secteur tertiaire	22,7	79,6
Secteur secondaire*	5,2	18,2
Secteur primaire	0,6	2,1

** dont 3,3 millions dans l'industrie et 1,9 million dans la construction*

Tableau: Vie-publique.fr / DILA • Source: Insee - Tableau de bord de l'économie française • Récupérer les données • Créé avec Datawrapper

Le développement incessant du numérique dans les organisations[3] , fait qu'aujourd'hui on distingue même un quatrième secteur d'activité, transverse aux trois autres secteurs, définit par Michèle DEBONNEUIL comme étant *« de nouveaux services incorporant des biens, la mise à disposition temporaire de biens, de personnes, ou de combinaisons de biens et de personnes »*, secteur dont les produits ne sont ni des biens, ni des services, mais des activités qui visent à fournir des services qui nécessitent une main d'œuvre qualifiée (innovation, R&D, conseil/expertise, services numériques tels ceux dispensés par les NATU[4] , transport, communication & médias).

Les freins à la digitalisation soulignés par les entreprises

1 Jean KOGEJ, « Miracles et mystères de l'économie allemande », Conflits, no 8, janvier-mars 2016, p. 50-53.
2 Contre 8% aux Etats-Unis, 9,2% en Chine, 10% au Royaume-Uni et 10,1% en Corée du Sud.
3 Les technologies de l'information (TI) ou *Information Technology (IT)* d'abord, l'Internet, les smartphones, les ordinateurs, les appareils portables, les progiciels de gestion intégré (PGI) ou *Enterprise Resource Planning (ERP)*, la gestion de la relation client (GRC) ou *Customer Relationship Management (CRM)*, les bases de données, le cloud computing, puis les technologies opérationnelles de surveillance et du contrôle d'actifs et de processus industriels ou *Operational Technology (OT)*, la robotisation des chaînes de production, des systèmes de contrôle/commande industriels ((*Distributed Control Systems (DCS)* & *Industrial Control Systems (ICS)* dotés de logiciels de supervision ou *Supervisory Control and Data Acquisition (SCADA)*), les interfaces homme-machine (*Human-machine interface, HMI*) et machine-machine maintenant, les *programmable logic controllers (PLC) & remote terminal units (RTU) and, la radio-identification (RFID, Radio Frequency IDentification*), les objets connectés (*IoT, Internet of Things) avec une utilisation croissante de l'Intelligence artificielle, et d'algorithmes d'apprentissage.*
4 Les NATU, pour Netflix, Airbnb, Tesla et Uber, sont de jeunes entreprises américaines à forts taux de croissance depuis leur création dans les années 2000. Elles évoluent dans des métiers différents des GAFAM et leur stratégie est la disruption des modèles économiques existants afin d'être plus compétitifs, d'affaiblir la concurrence et de devenir rentable dans une perspective d'investissements, Wikipedia.

La transformation digitale des entreprises passe d'abord par la formation de tous les utilisateurs de produits et services numériques, les employés, les fournisseurs et les clients, par un accompagnement des humains pour qu'ils acquièrent les compétences nécessaires pour assurer la sécurité de leurs usages au quotidien.

Le mot cybersécurité recouvre un vaste domaine du numérique, la protection, ce qui se passe avant, qui va de l'entrainement à la création de plans de continuité ou de reprise d'activité, la défense, temps de l'action et des opérations, qui inclut aussi la gestion des crises, et enfin la résilience, après, l'investigation numérique post incident et la recherche de la preuve. La liste des métiers de la cybersécurité commence par le métier de formateur, c'est-à-dire permettre aux autres d'acquérir les connaissances et des compétences nécessaires pour embrasser ce vaste domaine technique qui demande aussi une pratique régulière ; on parle d'ailleurs d'acquérir de bonnes pratiques en matière de technologies et d'usages, pour s'assurer de la bonne utilisation des outils informatiques et de la bonne gestion des données produites ; gestion de la sécurité des systèmes d'information, pilotage des projets numériques, conception et maintien en condition opérationnelle ou de sécurité (MCO/MCS), bonne gestion des risques, normalisation, Droit du numérique (Délégué à la protection des données, juriste, assureur), aspects politiques et géopolitiques : la cybersécurité procèdent de toutes ces disciplines.

La logique voudrait que les dirigeants, qui sont responsables de la sécurité, s'assurent bien de la souveraineté numérique des outils qu'ils utilisent ou font utiliser à leurs employés, car il s'agit d'un enjeu stratégique pour leur organisation, mais aussi d'une gestion responsable, donc raisonnée, de toutes les données qui sont produites. Ordinateurs, téléphones, automates, objets connectés (*IoT*), systèmes d'exploitation, suite bureautique, Progiciel de Gestion Intégré (PGI) ou enterprise ressource planning en anglais (*ERP*), informatique industrielle ou embarquée, chaque brique qui constitue le système d'information devrait être ainsi maîtrisée, et plus encore si celle-ci n'était pas souveraine. La cybersécurité doit bien évidemment aussi prendre en compte les aspects économiques, les tendances sociales, les usages (tel le *BOYD*, abréviation de l'anglais *bring your own device* , en français AVEC pour « apportez votre équipement personnel de communication », par exemple, les modes), les aspects juridiques et géopolitiques.

Plus le développement des technologies s'accélère, plus leur appropriation est rapide, plus leurs usages et la bonne maîtrise technique de celles-ci par de simples humains devient complexe. L'augmentation croissante de la puissance de calcul des ordinateurs, des téléphones, l'utilisation des algorithmes d'apprentissage et de l'intelligence artificielle viennent accélérer encore les capacités techniques et scientifiques des humains. Les organisations ont donc de plus en plus besoin de sachants qui sont capable d'adapter ces environnements complexes qui sont toujours en perpétuel développement. Enfin, la menace de se faire commander un jour par ces machines compliquées qui s'imposent peu à peu à nous et que nous avons voulu apprenantes est bien réelle.

Certains humains l'avaient compris, ces technologies pouvaient être détournée de l'usage pour lequel elles avaient été conçues, ils les challengeaient, les modifiaient et arrivaient à en détourner les usages. Depuis les années 2007 nous avons changé de paradigme, et le mot hacking est rentré dans nos mœurs, mieux, au lieu de féliciter ceux qui produisent nos machines, nos produits ou nos services, on s'est mis à complimenter ceux qui y trouvent des failles, qui les détournent de leur usage premier, qui les utilisent pour contraindre, cela pouvant aller jusqu'à la destruction.

En apprenant maintenant à nos puissantes machines à rechercher des failles, à fonctionner comme ces humains indisciplinés, n'allons-nous pas détruire ce monde technique qui était censé nous soulager des tâches pénibles et répétitives ? Nous voyons ici que l'humain doit bien être remis au centre des réflexions, et que les technologies doivent continuer à être maîtrisées. Certains parlent de conception selon les méthodes formelles, de sécurité dès la conception, security *by design* en anglais, d'un monde qui ne donnerait plus la part belle à notre instinct pionnier, conquérant, guerrier. Croire en l'humain est véritablement essentiel pour assurer l'avenir de nos sciences et techniques.

LA CYBERSÉCURITÉ : UNE NECESSAIRE PRISE DE CONSCIENCE

Comme nous venons de le voir, la menace cyber s'est intensifiée ces dernières années. L'attaquant a été mis plus en lumière que le défenseur, le mot hacker est entré dans le langage courant, jusqu'à être adjectivé parfois d'éthique. Celui-ci exploite des vulnérabilités techniques qui sont généralement connues, car publiées sur des sites spécialisés (*CVE*, *NVD*, etc.), sachant par ailleurs que la surface d'exposition aux attaques devient de plus en plus grande, les matériels et logiciels proposant de plus en plus de fonctionnalités et l'interconnexion entre eux, ce qui les rend de plus en plus complexes à bien maîtriser. Ces pirates exploitent aussi les faiblesses humaines, en particulier celles liées aux usages, car 4/5ième des problèmes informatiques sont le fait des humains, dus à de mauvaises implémentations, à de mauvaises configurations, à la non-application des mises à jour de sécurité, entre autres exemples.

Développés par les services étatiques des grands États cyber, mais aussi par des criminels regroupés en organisations parfois soutenus par des États bandits, les outils offensifs se sont fortement développés, l'innovation a changé de camp. Ce changement de paradigme fait que l'offre d'outils offensifs sur étagère, qu'ils soient proposés par des entreprises privées, des groupes cyber-criminels, la communauté du logiciel libre ou les chercheurs des laboratoires universitaires, abonde et contribue aussi à la multiplication des acteurs malveillants.

Dans le même temps, dans les pays industrialisés, les administrations ont imposé aux citoyens une trop rapide dématérialisation, cela sans que ces derniers soient formés en amont aux usages numériques. Les particuliers utilisent à fortiori de plus en plus les systèmes d'information pour y mettre leurs données personnelles et confidentielles, des pratiques dont ils n'ont pas la maîtrise. Si l'ANSSI et la plupart des organismes professionnels (ANSSI, MEDEF, CGPME, CCI, BPI, etc.) ont sorti des guides se sécurité numérique, le Pôle d'excellence cyber est le seul organisme à avoir produit un Guide pratique à destination des collectivités, PME/PMI et petites organisations, augmenté de 23 tutoriels, qui existent aussi sous la forme de 15 vidéos YouTube, pour que tous les utilisateurs du système d'exploitation Windows 10 puissent se protéger.

Les technologies vont vite, de plus en plus vite, les écrans sont de plus en plus présents dans nos villes, dans nos véhicules, dans nos foyers, et nos ordinateurs, nos téléphones, sollicitent de plus en plus notre vue et notre ouïe, des flots d'informations très hétéroclites s'imposent à nous, concentrent notre attention sur un présent agressif qui distrait notre pensée et limite nos réflexions. L'espionnage *by design* de nos outils modernes, la reconnaissance faciale, l'analyse de nos discussions, de nos textes, y compris dans nos photographies, fait que l'informatique devance nos simples envies, oriente délibérément nos choix, motive « nos » décisions.

Les données que nous produisons ne nous appartiennent plus, elles sont stockées, analysées, souvent sans que nous n'ayons donné notre accord (tout est en *opt-in*), cela pour optimiser les réponses que ces machines séductrices nous proposent. Les enfants aussi accèdent de plus en plus tôt à ces objets interactifs qui leurs sont dorénavant familiers et leur semblent très rapidement indispensables, les mouchards connectés inondent nos villes, nos aéroports, nos gares, nos véhicules, le *Web*, ils y modifient peu à peu les relations humaines, puisqu'une partie considérable de notre vie passe maintenant par le filtre de ces réseaux.

Des lacs de données (*data-lakes* en anglais) humaines émergèrent dans le *cloud*, explorés par des intelligences artificielles qui analysent notre vie numérique gravée sur les disques durs de gigantesques datacenters, qui apprennent aussi des métadonnées que nos outils produisent. Les grandes compagnies de l'Internet vivent de ces analyses qu'elles revendent aux marchands, aux laboratoires de R&D, aux assureurs, à tous ceux que nos données intéressent. Savoir-faire, dessins & modèles, brevets, messages, pièces jointes, échanges en visioconférence, données confidentielles des administrations et entreprises sont exposées à de redoutables logiciels qui renseignent multinationales et États, qui ont compris depuis longtemps qu'espionner est bien plus rentable que de partir d'une feuille blanche, que ces données sont l'or du 21ième siècle.

Cela nous ramène sur terre. Le monde physique et le monde virtuel sont bien liés, tout comme nos réseaux de neurones sont parfois connectés aux réseaux informatiques, et l'identité numérique, que ceux qui nous contraignent ont tenté de séparer de l'identité physique, n'est rien d'autre qu'une partie, de plus en plus considérable, de ce qu'est l'individu. L'utilisation des outils numériques, qui est certes une aide précieuse à la réalisation, à la conception, à la décision, aux échanges, peut faire basculer peu à peu l'individu dans une certaine dépendance, qui peut aller jusqu'à l'addiction, lorsque celui-ci en oublie la finalité première. Le citoyen devient alors le cobaye des algorithmes, un homme au service des machines, sujet d'études. Nos données à caractère personnel ou notre propriété intellectuelle sont devenues des cibles, des armes même, lorsque celles-ci tombent aux mains d'acteurs malveillants (on parle de *hack and leak*, vente de données sur l'Internet clandestin pour les exploiter à des fins de renseignement humain).

À l'exception de la couche physique, dont les composants sont territorialement situés (nos câbles électriques et sous-marins, nos centres de données, les relais Internet, 5G, etc.), le cyberespace ne connaît pas de frontière.

Il peut ainsi être vu comme étant un espace en tension permanente. Les États et acteurs paraétatiques s'y confrontent, observent l'évolution de la menace, développent des arsenaux offensifs et dissimulent ces activités. Le but est d'espionner de manière efficace et discrète les données sensibles, de saboter les infrastructures critiques et les réseaux, en appui d'opérations plus classiques, de manipuler les humains et leur information. Des cyber-criminels organisés en réseaux gagnent des sommes importantes en produisant des rançongiciels cachés dans des pièces jointes ou derrière des liens dans nos mèls, c'est la principale menace pour les entreprises et institutions françaises en 2022. Les dégâts ne sont pas que financiers, car les cibles sont parfois des infrastructures critiques ou médicales. Ils déstabilisent des organisations, défigurent des sites Web, prennent le contrôle des SI, exfiltrent des données pour les revendre ou les divulguer. La menace est multiple, les attaques sont de plus en plus sophistiquées et complexes, et la France est ciblée par des acteurs aux intérêts hétérogènes.

Face à la concurrence du privé, où les salaires ont augmenté ces dernières années, les administrations et les PME/PMI pures players de la cyber ont des difficultés pour recruter des profils techniques expérimentés pour sécuriser leurs clients, et donc pour pérenniser leur métier. Car les bons profils s'arrachent à des salaires bien plus élevés que la moyenne des salaires Nationaux dans la plupart des métiers techniques : c'est aussi vrai pour les soudeurs du domaine naval, par exemple, ce sera le cas bientôt pour le nucléaire civil qui va recruter 1000 ingénieurs, des soudeurs et tuyauteurs, pour la construction de nouveaux réacteurs nucléaires de type EPR2, et ce seront entre 6000 et 8000 techniciens, ingénieurs et chercheurs qui seront recrutés chaque année par la filière nucléaire pour les 15 années à venir. [1]

Ce qui est rare est cher. Certains en profitent aussi pour se vendre au plus offrant et faire des progressions de carrière rapides, tant que le domaine est porteur. Former des gens compétents devient donc une priorité pour les écoles, qui sollicitent aussi les entreprises pour forger des cursus très opérationnels, basés sur l'alternance. La cybersécurité se prête aussi très bien à des certifications métier (*ISO 27K, DPO, CEH, CISA, CISM, CISSP*, etc.) ou service & produit (*Cisco Certified Network Associate, CCNA, Certified Stormshield Network Expert, CSNE*, etc.) qu'intègrent maintenant la plupart des solutions du marché.

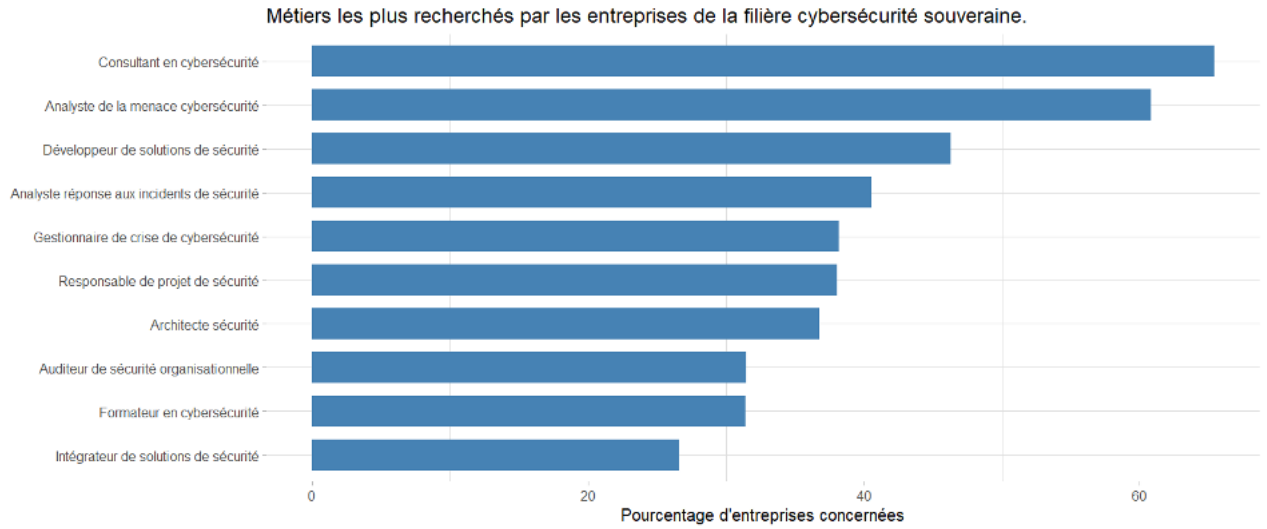
Des métiers en tension : une comparaison des métiers cyber les plus recherchés et des profils cyber les plus difficiles à recruter.

Le tissu économique français est principalement constitué d'Entreprises de Service du Numérique (ESN) et de cabinets conseils, dont les « consultants en cybersécurité » sont la cheville ouvrière. Le consultant recherché est bien souvent ce mouton à cinq pattes, doté de bonnes qualités d'écoute et de synthèse et d'une capacité à s'approprier vite les problématiques clients ; riche de ses expériences il saura s'adapter aux particularismes de l'organisation, c'est un chef de projet multi-casquettes avec une expertise pointue et un fort sens du service client.

« *Analyser la menace cyber* », c'est tenter de comprendre quelles sont les vulnérabilités du moment, c'est suivre l'activité des groupes d'attaquants ainsi que leurs méthodes, savoir ce que ceux-ci vont cibler, entreprises ou administrations, des personnes et leurs usages, des logiciels ou des matériels. Ce métier d'analyste a d'abord été créé par les services de renseignements, pour tenter, à partir d'un faisceau d'indices, parfois de signaux faibles, de qualifier au mieux la réalité du monde. Types d'individus, motivations, modes opératoires, outils utilisés, le renseignement est un avantage essentiel les défenseurs. Les Centres des Opérations de Sécurité (souvent réduit à son acronyme anglais *security operation centers*, ou *SOC*)) utilisent à la fois des profils techniques qui possèdent une bonne maîtrise des outils de sécurité réseaux ou systèmes, de la réponse à incident, la cyberdéfense, mais aussi d'autres profils issus aussi des sciences humaines et sociales (les gens du le renseignement sur la cyber-menace ou *cyber threat intelligence, CTI* en anglais, du Droit ou parlant certaines langues étrangères afin d'investiguer dans d'autres pays, souvent à partir d'outils libres du Renseignement d'origine sources ouvertes, ROSO ou *open source intelligence, OSINT*, en anglais.

Il est donc bien normal que les « analystes de la menace cybersécurité » représentent le second métier en grande tension, un métier où l'expérience est essentielle, car c'est aussi à force de pratique que ces profils se bonifient.

1 https://www.i2en.fr/metiers-competences/les-besoins-de-lindustrie/



Source : Pôle d'excellence cyber

Les « développeurs de solutions de sécurité » sont aussi des profils très recherchés, c'est eux qui permettent aujourd'hui aux grands éditeurs de logiciels ou de matériels de produire des solutions sécurisées *by design*. Ainsi, le nouveau métier de DevSecOps, désigne celui qui intègre la sécurité dès le début et tout au long du processus de développement du projet. Cela est très important dans le milieu industriel, et en particulier pour le code embarqué (Linux embarqué dans la filière automobile, par exemple).

Aujourd'hui la plupart des Centre des Opérations de Sécurité, les *SOC*, proposent aussi un service de centre d'alerte et de réaction aux attaques informatiques, *computer security incident response teams (CSIRT)* en anglais, aussi connu sous le nom de *computer emergency response teams (CERT®)*, une dénomination populaire qui est une marque déposée par l'Université de Carnegie-Mellon), des spécialistes expérimentés, compétents et réactifs, qui interviennent lors des cyber-crises. Le financement par l'ANSSI dans le cadre du dispositif France Relance de tels dispositifs au sein des régions françaises témoigne de la volonté de l'Agence Nationale de protéger le tissu économique et administratif français, et d'avoir désormais accès à une synthèse de la menace cyber consolidée à l'échelle des territoires et domaines métiers. Nombreux sont les opérateurs de *SOC* (qu'il soit interne ou externe) qui proposent aussi un service de centre d'alerte et de réaction aux attaques informatiques (*CSIRT*), ce métier récent est en pleine explosion tant le périmètre de menaces, y compris humaines, géopolitiques et législatives, devient vaste. Les « analystes réponse aux incidents de sécurité » deviennent les pompiers du numérique, ce sont eux qui réagissent dès les premières heures des attaques et qui tentent de les contrôler et de les comprendre pour leurs clients.

Attention tout de même lorsque le prestataire de service de sécurité est étranger, et que lors d'une remédiation sur votre SI, il récupère tous les marquants de l'attaque ainsi que les données touchées, car vous pouvez juridiquement vous retrouver alors dépouillé de éléments de preuve, ainsi que d'une partie ou de toutes les données de votre entreprise. La Loi de blocage[1] oblige maintenant les entreprises à ne pas répondre aux injonctions émanant de pays étrangers, mais de passer par le Service de l'Information Stratégique et de la Sécurité Economique, le SISSE, qui par le réseau des ambassades, pourra rappeler que la Loi française prime sur les Lois extraterritoriales.

Le « gestionnaires de crise de cybersécurité » travaille avec les gens de la réponse à incident, ils ont souvent un périmètre plus large et gèrent la crise dans sa globalité, avec les aspects humains, communication, ils pilotent le plan de continuité d'activité (PCA) ou plan de reprise d'activité si le SI a été mis KO (PRA). Ces nouveaux métiers sont très demandés dans les moyennes et grandes entreprises, et il existe encore peu de cursus spécialisés, tel le Mastère spécialisé Gestion des crises cyber des écoles de Saint-Cyr Coëtquidan (ESCC). Car gérer une crise cyber n'est pas que recouvrer le fonctionnement technique normal du SI, c'est pouvoir comprendre ce qui s'est passé, les dégâts occasionnés, mais aussi et surtout permettre à l'entreprise dans sa globalité de continuer son activité dans les meilleures conditions, c'est-à-dire permettre à tous les domaines métiers (RH, finance, mercatique, comptabilité, achats, qualité, production, stocks, etc.) d'être à nouveau opérationnel.

1 https://www.economie.gouv.fr/protection-economique-entreprises-reforme-loi-dite-blocage-1968#:~:text=blocage%20%C2%BB%20de%201968-,Protection%20%C3%A9conomique%20des%20entreprises%20%3A%20r%C3%A9forme%20de%20la,dite%20%C2%AB%20de%20blocage%20%C2%BB%20de%201968&text=Deux%20textes%20de%20lois%20viennent,men%C3%A9es%20par%20des%20autorit%C3%A9s%20%C3%A9trang%C3%A8res

Les hommes clés de la défense restent les « responsables de projets de sécurité » ou les « architectes de sécurité ». Car si l'architecture est robuste et bien pensée dès le démarrage d'un projet, qu'il a été géré grâce à des DevSecOps bien encadrés, le SI aura d'autant moins de chance d'être attaqué. Ces métiers sont proches des intégrateurs de solutions de sécurité.

Enfin, il manque cruellement de « formateurs en cybersécurité », et les Universités et Grandes Écoles emploient souvent des intervenants dits « extérieurs », c'est-à-dire issus du monde industriel ou de la défense qui enseignent les dernières techniques de la cybersécurité et entrainent les étudiants avec des scénarii opérationnels, très similaires aux situations que vivent les professionnels en poste dans les entreprises et administrations. L'alternance est aussi basée sur ce modèle, l'étudiant est en immersion dans l'entreprise où il apprend rapidement son métier au contact de collègues aux compétences éprouvées. De nombreuses formations techniques, telle la cybersécurité, ont développé de tels modèles.

Enfin, un problème majeur remonté par les industriels est la grande difficulté qu'ils ont de recruter sur le long terme des « managers d'équipes techniques » qui sont reconnus pour leurs qualités techniques et managériales par les techniciens. Un manager sorti d'une école de commerce ou de management n'est souvent pas reconnu comme étant légitime par des gens qui viennent des sciences dures. Le management d'équipe se fait beaucoup par les méthodes agiles au sein des organisations du numérique. On privilégiera un ingénieur qui possède déjà une bonne expérience dans le domaine technique et qui s'est formé au management spécifique à ces milieux techniques.

Avec près de 62 000 recrutements attendus cette année, la fonction informatique est la plus dynamique du marché de l'emploi des cadres. (Source: Apec/Crédit image: Apec)

Puisque la plupart des entreprises françaises sont des ESN, les « chefs de produits techniques », de bons technico-commerciaux capables de bien comprendre et maîtriser tant les fonctionnalités que les enjeux des solutions, et donc d'être légitimes pour les vendre à leur carnet d'adresse fourni, sont aussi très demandés. Les entreprises innovantes ont besoin de ce type d'ingénieurs commerciaux pour valoriser leurs produits et services au sein des entreprises et administrations.

Ces deux derniers métiers sont aussi des pistes de reconversion par des formations tout au long de la vie pour des ingénieurs venant des télécom ou d'autres métiers. Une formation de « manager des équipes techniques » est en projet de construction entre le Pôle d'excellence cyber et la Rennes *Cyber Shool of Business*, une Unité d'Enseignement, UE, chef de produit technique est envisagée.

Deux typologies de formations

Les Formations Cyber Socles FCS

Celles-ci s'adressent à des personnes qui souhaitent acquérir de bonnes connaissances et compétences techniques pour aller vers les métiers de la cybersécurité, cela va du code, aux métiers d'analyste (Gestion de l'information et des événements de sécurité, en anglais *security information and event management, SIEM*, Centres des Opérations de Sécurité, *SOC*, centre d'alerte et de réaction aux attaques informatiques, *CSIRT/CERT*, la cyberdéfense) ou du forensique (l'analyse post-mortem, la cyber-résilience, et la recherche de la preuve), d'architecte ou d'urbaniste, etc. Devenir informaticien demande à minima 2 à 3 années d'études post Bac, c'est une action à moyen terme pour un jeune sorti du Bac.

La cybersécurité entre aussi de plus en plus tôt dans les cursus, ainsi dès la seconde les enseignants doivent faire 1h30 d'enseignement à la sécurité du numérique. Les élèves, qui vivent dorénavant dans un monde plus technique, arriveront ainsi au Bac avec une plus grande appétence pour les métiers de la cybersécurité.

Les Formations Cyber Connexes FCC

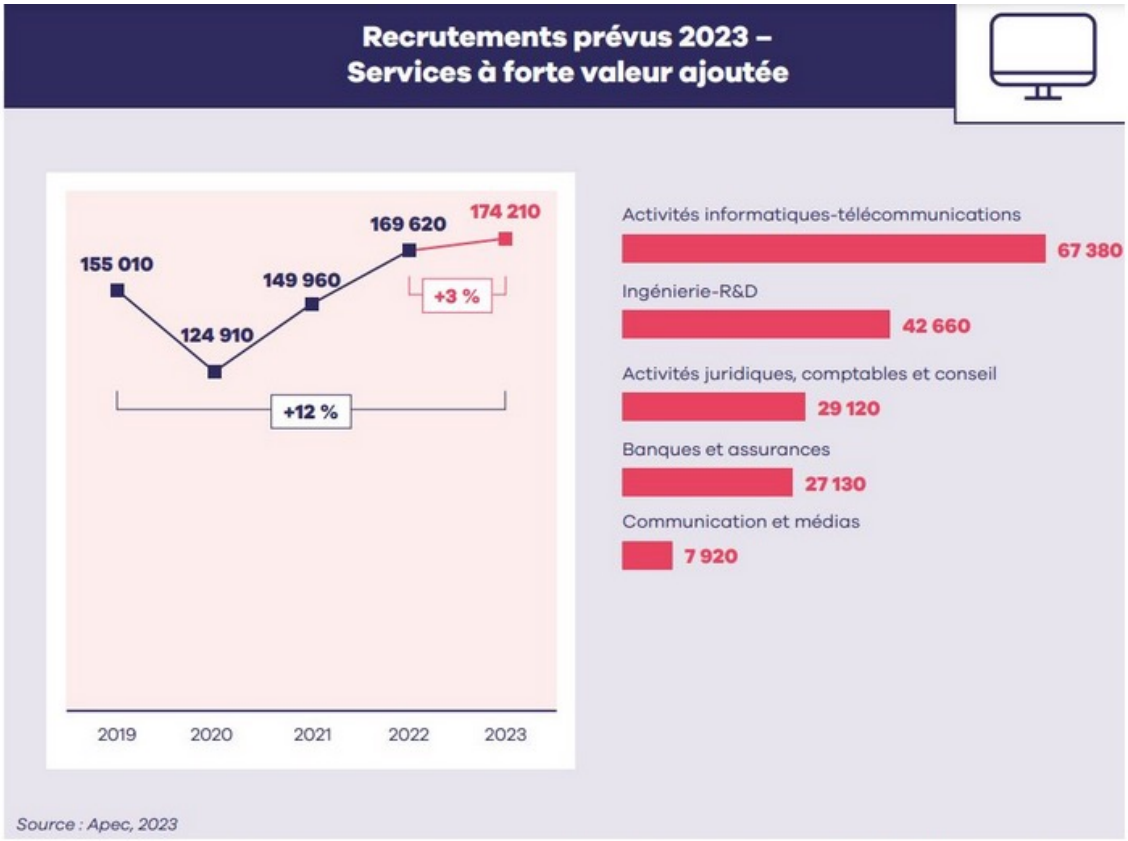
Celles-ci s'adressent à des personnes qui disposent d'une expérience dans un autre métier que ceux du monde de l'informatique ou des télécommunications, et qui souhaitent se réorienter ou acquérir une double compétence, augmenter leur périmètre d'intervention.
Dans le cadre de l'un de ses groupes de travail, le Pôle d'excellence cyber a travaillé un référentiel listant les prérequis pour entrer dans les différentes formations aux métiers de la cybersécurité. Certaines formations connexes (juridique, sciences humaines et sociales, géopolitique) ne nécessitent pas forcément d'avoir fait des études dans les sciences dites dures et elles sont accessibles à tous moyennant l'acquisition de prérequis, d'éventuelles adaptations et des durées de formation plus ou moins longues.
Le tableau ci-dessous définit les parcours accessibles pour adresser les principaux métiers de la cybersécurité, y compris les sciences humaines et sociales (SHS) et le Droit, en fonction des cursus initiaux des candidats (avec un parcours scientifique, numérique ou tout autre), il liste les prérequis pour entrer dans les formations. Il inventorie aussi les spécialisations possibles vers certains métiers, tel développeur, gestionnaire de crise, auditeur ou juriste. Ce tableau a été produit en consultation avec les écoles partenaires du Pôle sur le territoire, qui proposent aux prospects potentiels les offres de formations qui correspondent et qui sont listées sur leurs catalogues respectifs.

	formation autre	formation scientifique	formation numérique	spécialisation
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Opérateur								
Juriste spécialisé								
audit et contrôle orga								

Source : travail du GT A01 du Pôle d'excellence cyber avec les contributeurs.

Si l'emploi des cadres en informatique & télécommunications continue d'augmenter, cela baisse tout de même par rapport à la progression qu'il y avait eu entre 2020 & 2022. Cela pour plusieurs raisons. D'abord la main d'œuvre qualifiée est rare et les *turn over* de personnels ont été nombreux ces dernières années sur un marché qui est en partie caché (les gens sont embauchés par leur réseau, ou démarchés par des chasseurs de têtes qui travaillent pour des concurrents[1]) certains profitent aussi de la crise des compétences pour augmenter leur salaire. De plus, il n'y a toujours pas suffisamment de jeunes qui sont formés aux métiers techniques, pour les composants, le code embarqué, la programmation sécurisée, la MCO/MCS des systèmes & des réseaux, l'intelligence artificielle, la cryptographie, etc.



En 2023, Les intentions d'embauche devraient rester toujours élevées dans l'informatique.(Source: Apec/Crédit image: Apec)

C'est dès le collège et au début des années lycées qu'il faut aiguiser la conscience et donc l'appétence des jeunes afin qu'ils prennent bien en charge la sécurité de leurs outils numériques, qu'ils puissent en assurer la maintenance et la sécurité a minima. Pour cela, le Pôle d'excellence cyber travaille avec le rectorat de Rennes pour former les enseignants des lycées des filières Services Informatiques aux Organisations, SIO, et Systèmes Numériques, SN, en construisant un M@gistère avec le Rectorat de Rennes, qui devront à leur tour former leurs élèves à l'intérêt pratique de ces métiers et leur donner envie de continuer vers les études d'informatique. L'expérience montre que tous se satisfont de cet ambitieux et nécessaire programme.

Dans la même veine, le ministère des Armées (COMCYBER[2] & Dgesco[3]) proposent un challenge aux lycéens de la Région parisienne au nom évocateur « Passe ton hack ». Inscrits par leurs professeurs, les étudiants rivalisent de réflexion pour trouver les solutions techniques à des problèmes numériques. Cette initiative qui est un franc succès, pourrait être généralisée sur tout le territoire.

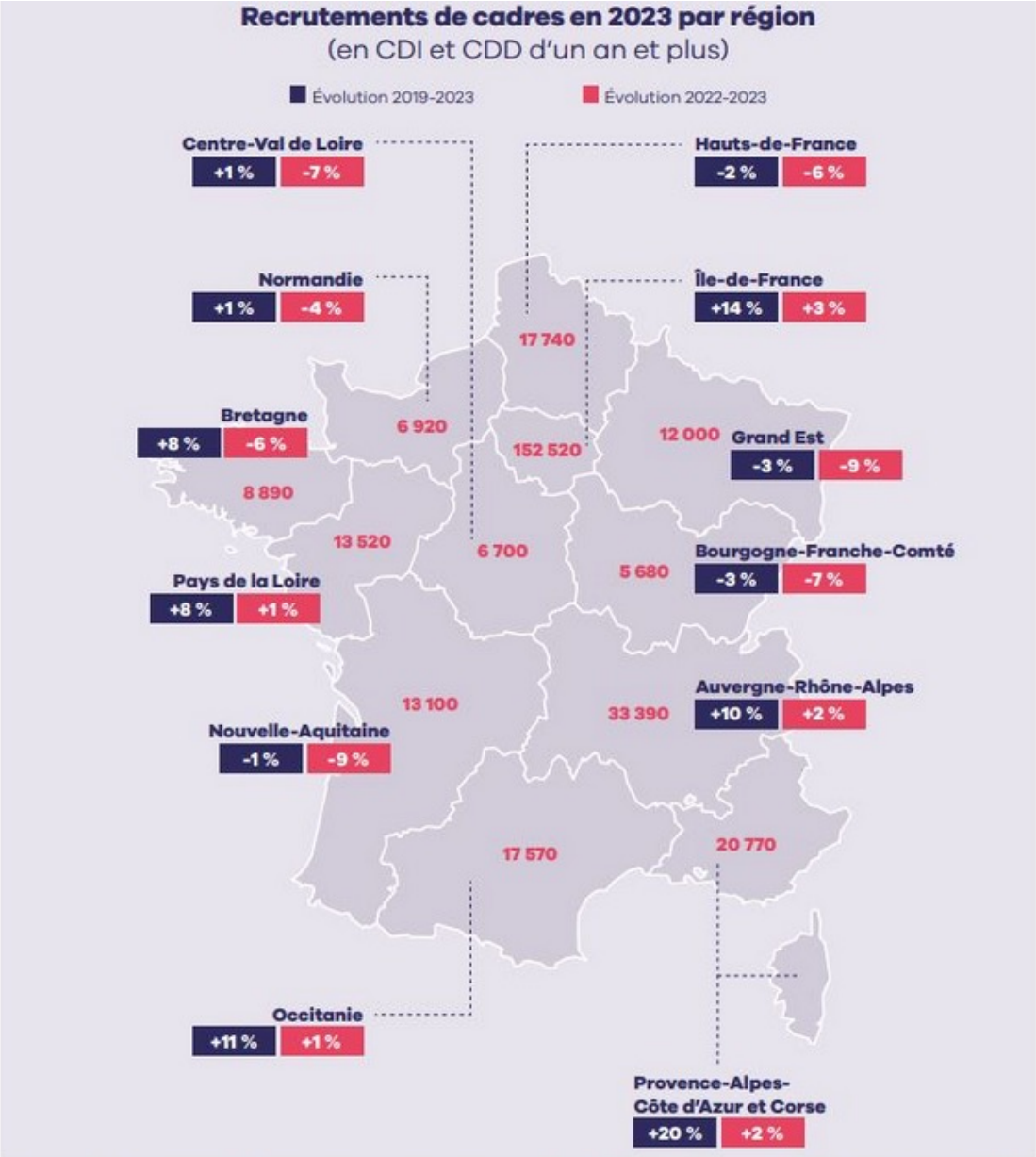
1 « Les réseaux sociaux sont désormais le deuxième canal de recrutement le plus utilisé par les entreprises, derrière l'offre d'emploi, alors qu'il n'était que le 4e en 2019. Les entreprises y ont de plus en plus recours pour diffuser leurs offres d'emploi (68 % en 2022 vs 62 % en 2021) mais également pour contacter directement des candidat.es (54 % vs 50 %). Le recours à un intermédiaire de recrutement (cabinet de recrutement, agence d'emploi, etc.) progresse nettement et dépasse son niveau d'avant-crise (48 % en 2022 contre 42 % en 2019). » Pratiques de recrutement des cadres 2023 - 25 mai 2023 - Apec

2 Commandement de la cyberdéfense.

3 Direction Générale de l'Enseignement Scolaire.

Le MinArm a aussi en projet de créer une Académie Cyber pour coordonner et piloter toutes les formations cyber pour les trois Armées. Défense mobilité qui définit les orientations de la politique générale de reconversion et la met en œuvre, assure l'accompagnement vers les emplois cyber des personnels civils des armées en situation de réorientation professionnelle hors des fonctions publiques, propose l'organisation du dispositif de reconversion et d'accompagnement vers l'emploi, et assure le financement, le contrôle et l'évaluation des actions qui ont été engagées. Rennes Métropole ainsi que le MEDEF 35 sont en appui du projet.

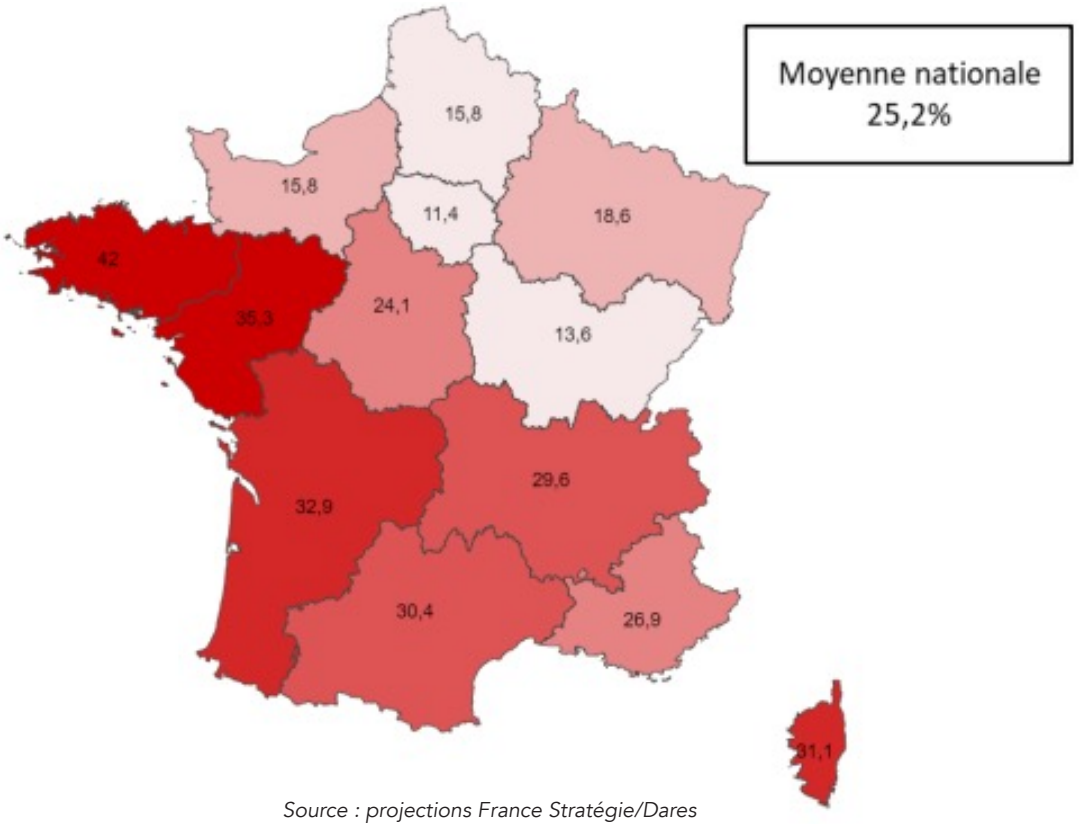
La dynamique de recrutement pour la filière informatique est toujours là, car pour valoriser au mieux leurs produits et services, les entreprises, recherchent aussi de nombreux profils commerciaux ou en études, recherche & développement. Ce schéma montre bien que si l'innovation est essentielle aux entreprises, il faut aussi pouvoir la marketer et la vendre. D'ailleurs, les start-ups qui marchent le mieux, sont souvent l'association d'un chercheur et d'un ingénieur commercial. La France a toujours un riche tissu d'entreprises innovantes portées par de nombreux dispositifs, tel France Relance, la *Cyber Factory, Cyber Booster,* etc. Le Pôle d'excellence cyber promeut ces dispositifs auprès de ses membres et de la communauté cyber.



L'Apec note des hauts volumes d'embauches dans les places fortes de l'emploi IT cadre. (Source: Apec/Crédit image: Apec)

Si nous faisons un focus Région par Région, on voit qu'en 2023 les embauches vont globalement baisser, et qu'elles vont rester positives que dans le Sud et l'Est, dans les Pays-de-la-Loire et en Île-de-France. Ces chiffres s'expliquent aussi parce que le recrutement a été très élevé les 3 années passées durant lesquelles de nombreux cadres ont aussi changé de Région. Notons toujours une forte dynamique dans les Régions cyber, PACA, Occitanie, Auvergne-Rhône-Alpes, Île-de-France. La Bretagne et la Région Pays de la Loire continuent à consolider leurs grandes métropoles, Rennes, Brest, Nantes. La Nouvelle-Aquitaine, la Normandie et le Grand-Est semblent être les Régions où l'embauche est la plus difficile.

Part des emplois exercés dans des métiers dont les tensions s'accentueraient d'ici 2030, par région



Source : projections France Stratégie/Dares

Après la période Covid19, l'attrait de l'arc Atlantique, et en particulier de la Bretagne, est très significatif et ne cessera sans doute de croitre dans les années à venir, au détriment aussi des autres régions, cela générant une migration des différents profils métiers de l'IT.

DES TECHNOLOGIES EN CONSTANTE ÉVOLUTION

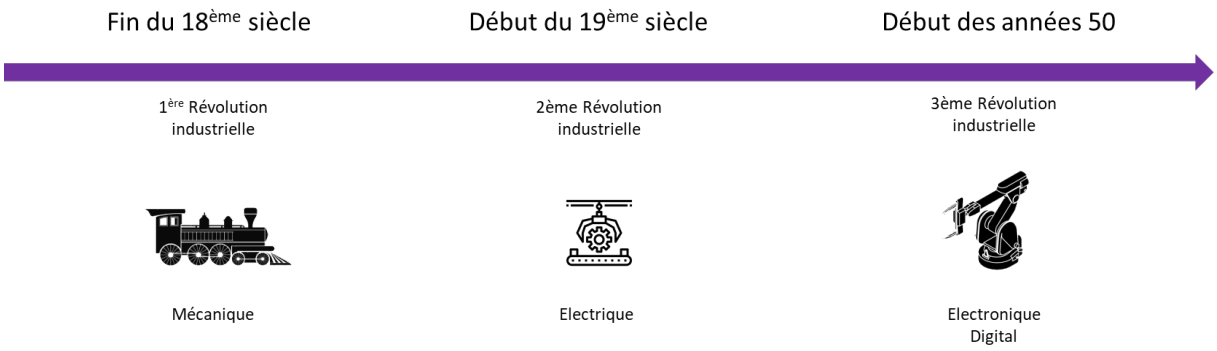
Les flux entre les organisations

Les interactions entre les différentes organisations ne cessent de croître avec la numérisation des échanges, la réduction des délais avec l'application du « juste à temps », la réduction des stocks et les interconnexions entre les systèmes d'informations rendent les organisations plus dépendantes entre elles, et par conséquent aux réseaux et systèmes d'informations qui pour beaucoup sont devenus interopérables.

Les interdépendances entre les organisations sont aussi devenues de plus en plus fortes, les grandes entreprises sous-traitent aux ETI, qui ont elle-même besoin de s'appuyer sur les innovations de PME spécialisées qui dépendent aussi de la micro entreprise, et inversement. Chaque organisation se retrouve souvent en position de fournisseur et de client. Alors, la mise à l'arrêt du SI d'un acteur économique, quelle que soit sa taille, peut mettre en péril l'ensemble d'une chaine de production d'un produit ou d'un service, constituée d'entreprises complémentaires.

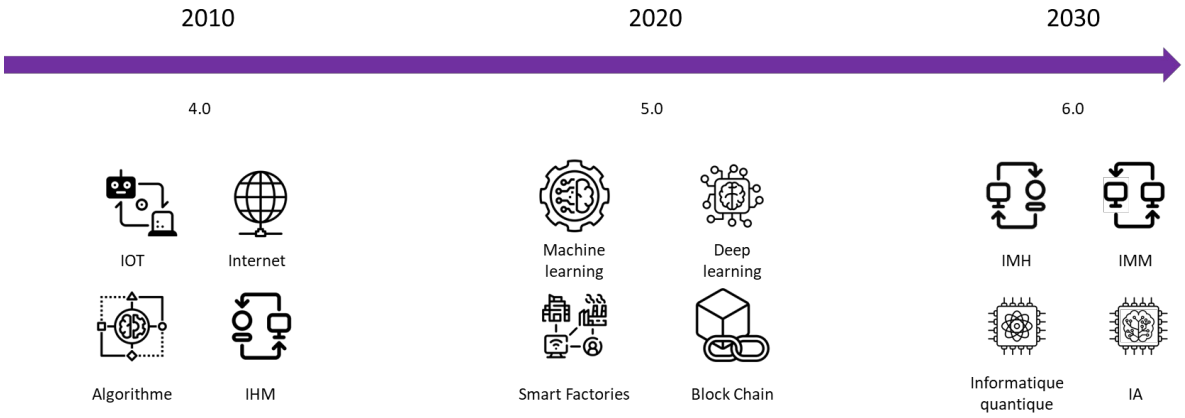
De plus, le contexte économique fait que de nombreuses entreprises sont aussi racheté par des ETI ou des Grands-Groupes, sans qu'il n'y ait forcément de remise à plat à la suite de l'ensemble du SI de l'acheteur. Les systèmes d'information deviennent donc de plus en plus complexes, et de ce fait leur protection devient plus critique. Au-delà du tissu d'entreprises innovantes, un territoire puise sa force dans un fin équilibre entre les laboratoires de recherches, les sociétés de services à forte valeur ajoutée et les industries de pointe dans les différents domaines d'innovations stratégiques et technologiques.

L'évolution des technologies



Source : Schémas : ConseilSI / Icônes : Antony Bayo, Nithinan Tatah, Lluisa Iborra de Noun Projet

Si les premières révolutions industrielles étaient dues à l'exploitation d'une nouvelle source d'énergie (ou à son traitement) qui permettait d'alimenter des usines toujours plus grandes et productives, et de conquérir (transport routier, maritime ou aérien) les vastes espaces encore vierges du vaste monde, les révolutions industrielles modernes ont permis d'accélérer le développement de ces grandes entreprises mondialisées, devenues riches aussi grâce à des innovations basées sur le développement des réseaux sous toutes leurs formes (la téléphonie, l'Internet, la téléphonie mobile, la XG, le satellitaire, les réseaux de neurones, l'IA, le lobbying, le juridique, etc.), par l'interconnexion des technologies de l'information et de la communication.

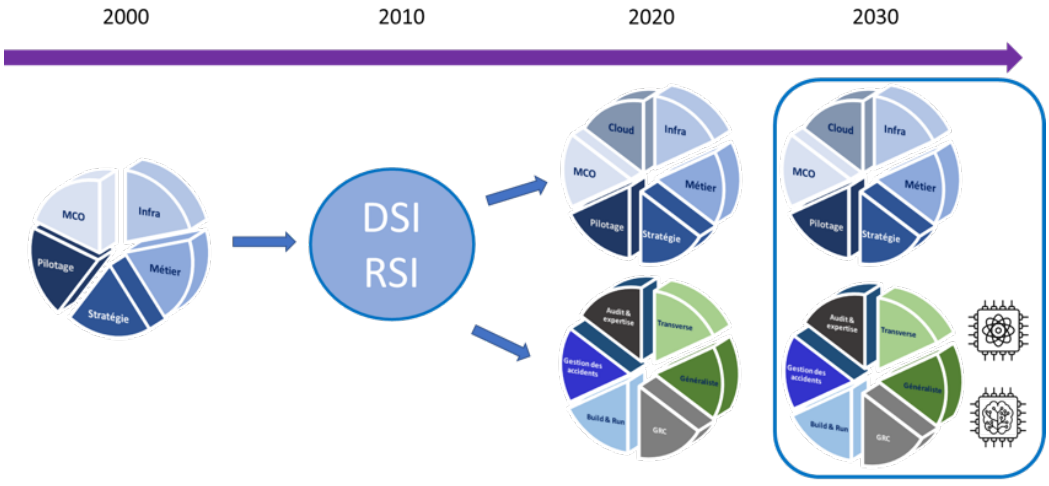


Source : Schémas : ConseilSI / Icônes : Misbahul Munir, icon 54, Nithinan Tatah, Timofei Rostilov, Lars Meiertoberens, Tippawan Sookruay, Juicy Fish, Abd Majd, ProSymbols de Noun Projet

Légende : *IoT*, objets connectés pour *Internet of Things* de l'anglais, IHM, Interface Homme Machine, IMH, Interface Machine Homme, IMM, Interface Machine Machine, IA, Intelligence Artificielle.

Issues de disciplines scientifiques complémentaires, telles les mathématiques, la thermodynamique, la physique, devenue nucléaire & quantique, l'informatique, la biologie, la chimie, etc. de très nombreuses technologies ont été développées, et, combinées entre elles pour donner naissance à de nouveaux outils pour les organisations, qui sont aussi à l'origine de nouveaux usages.
L'agrégation de ces nouvelles technologies augmentent considérablement la surface des vulnérabilités de ces architectures complexes, ce qui complexifient d'autant plus leur protection.
De surcroit, nous avons changé de paradigme entre 2000 et 2010 et des personnes malveillantes se sont mises à utiliser aussi ces nouvelles technologies pour subtiliser, détruire ou modifier des informations confidentielles des organisations, s'attaquer à l'image des marques ou de leurs dirigeants, etc. Le Gendarme ou le Policier, qui eux agissent dans le cadre légal, doivent donc aujourd'hui plus que jamais rivaliser d'ingéniosité dans cette course permanente à l'innovation.

L'évolution de la DSI vers la Cybersécurité



Source : Schémas : ConseilSI / Icônes : Abd Majd, ProSymbols de Noun Projet

Entre les années 2000 et 2010, la gestion des évènements de sécurité, pouvant aller jusqu'à des crises cyber parfois, a fait émerger ces nouveaux métiers de la cyberdéfense et du forensique, qui structurent aujourd'hui la filière. Dans ces années, la défense était assurée par des bidouilleurs de génie, parfois sans diplôme, mais surtout sans véritable contrainte légale. Puis, la Loi s'est emparée de ces sujets de spécialistes, obligeant, par exemple, les organisations à conserver leurs logs, une dynamique qui s'est étendue à l'Europe. Les métiers de l'investigation judiciaire, de la continuité d'activité, de la gestion des crises étaient nés. De nombreux services étatiques se sont mis à rechercher des profils techniques, et de nombreuses formations très opérationnelles ont émergées au sein des Universités et Grandes Écoles.

Dès les années 2000, des groupes d'activistes ou étatiques cyber ont perpétué des attaques de très grande envergure vers de grandes organisations ou des États. Citons l'Estonie, l'Iran, l'Ukraine, les États-Unis, la France, etc. On parle de déni de service distribué, ou *Distributed Denial of Service (DDoS)*, de nom comme Olympic Games, Titan Rain, Stuxnet, Duqu, Flame, Night Dragon, Nitro ou encore Energic Bear. Les grands états cyber avaient commencé à se faire la guerre, s'octroyant parfois au prix fort les compétences de groupes d'activistes ou de cybercriminels. Ces États légiférèrent aussi, car ils prenaient du même pas la pleine conscience de l'urgence à mieux maîtriser la sécurité de leurs SI.

États et entreprises se battaient déjà pour embaucher les rares spécialistes du domaine, et demandaient que leurs ingénieurs ou universitaires à BAC+5 soient formés tout au long de la vie. C'est dans ces années-là que les organisations nomment un responsable du périmètre cyber (la fonction de Responsable de la Sécurité des Systèmes d'Information, RSSI, (*Chief information security officer* ou *CISO* en anglais), définit par l'Organisation internationale de normalisation, *International Organization for Standardization* en anglais, ISO/CEI[1] 27002 & ISO/CEI 27001 en 2005) qui va motiver le déploiement d'outils de sécurité au sein des réseaux, des systèmes, des Directions des Systèmes d'Information, DSI.

Dans les années 2005 la cybersécurité prend son indépendance de l'IT, elle se professionnalise, se normalise, s'adapte aux évolutions complexes du SI qui s'outille face à une menace toujours croissante. Dans les années 2010 le RSSI gagne en indépendance par rapport au DSI, son chef, il devient le garant de la bonne décision en termes de choix techniques, de la parole de l'ANSSI, de la bonne sécurité de son organisation, un mandat qui pourrait aller jusqu'à s'opposer à certaines décisions de sa DSI. Ainsi, certaines organisations modernes ont ainsi choisis de faire en sorte que le RSSI dépende directement de la Direction générale et non pas du DSI, ce qui facilite véritablement son travail.

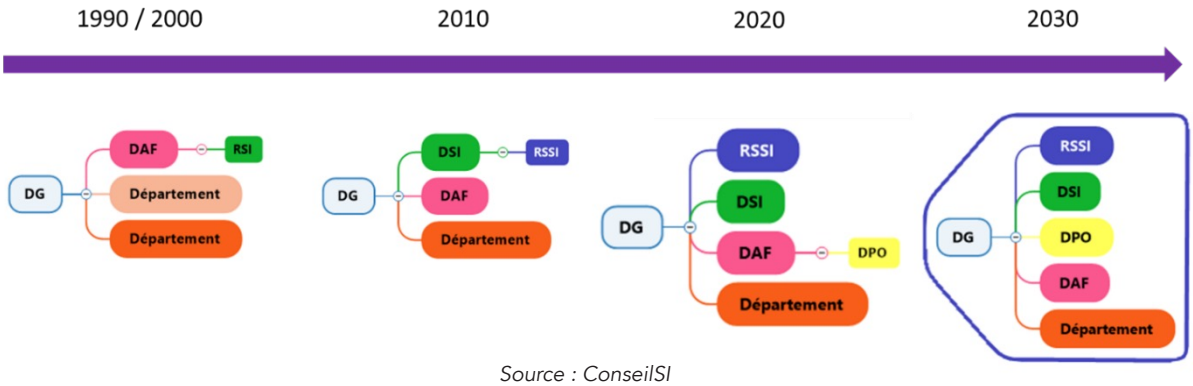
Dès 2013, des problématiques de souveraineté du *cloud* apparaissent, et les documents publiés par Edward SNOWDEN ne vont que venir renforcer la volonté européenne d'indépendance face aux outils étrangers, cela étant d'autant plus une préoccupation au sein des administrations qui ont le devoir d'archiver.

De plus, la multiplication des attaques qui engendraient des incidents fréquents dans les organisations, qui impactaient souvent des données à caractère personnel ou sensible, très encadrées par la Loi Informatique & Libertés et la CNIL, et métadonnées des administrés, des patients des hôpitaux ou clients des banques, poussèrent les organisations à nommer un Délégué à la protection des données (DPD, ou *DPO* en anglais pour *Data Protection Officer*) à plein temps en remplacement du Correspondant Informatique et Libertés (CIL)), fonction que cumulait souvent le RSSI.

Ce métier de RSSI (*CISO*) est très complexe, ce sont souvent des gens très expérimentés, qui ont touché dans leur début de carrière à de nombreuses fonctions techniques au sein des SI, ont tenu des postes très opérationnels et connaissent généralement bien les produits et services de sécurité du marché, les architectures et leurs problématiques. Toutefois, la sécurité des systèmes d'information d'une organisation ne peut pas, ne doit pas à l'évidence, être l'apanage d'une seule femme ou d'un seul homme. La plupart des RSSI manquent cruellement de budget, ils ont de grandes difficultés pour embaucher des personnels techniques et se sentent aussi isolés dans l'organigramme. Ainsi, soumis à de trop fortes responsabilités, à un stress quasi permanent, 50% des RSSI disent vouloir changer d'emploi d'ici à 2025, et 25 % d'entre eux envisagent même de changer de métier (analyse de Gartner). Enfin, l'ancienneté moyenne d'un *CISO* n'est que de 26 mois (rapport de Nominet), ce qui est très inquiétant pour la filière[2].

Dans les années qui viennent, le métier de RSSI devra donc nécessairement faire l'objet d'adaptations, d'évolutions, la fonction pourrait par exemple être portée par plusieurs personnes dans l'organisation, avec un responsable présent au sein des CoDir. Ensuite, puisque tout métier comporte des prérequis en termes de connaissances & de compétences, Grandes Écoles et Universités devraient pouvoir proposer des formations initiales de RSSI aux étudiants pour former à ce métier complexe, des cursus qui prendraient aussi en compte la gestion du stress et la gestion de crise. De tels cursus devraient voir le jour rapidement.

1 Commission électrotechnique internationale.
2 https://www.lesechos.fr/tech-medias/hightech/cybersecurite-une-profession-au-bord-du-burn-out-1933733



Source : ConseilSI

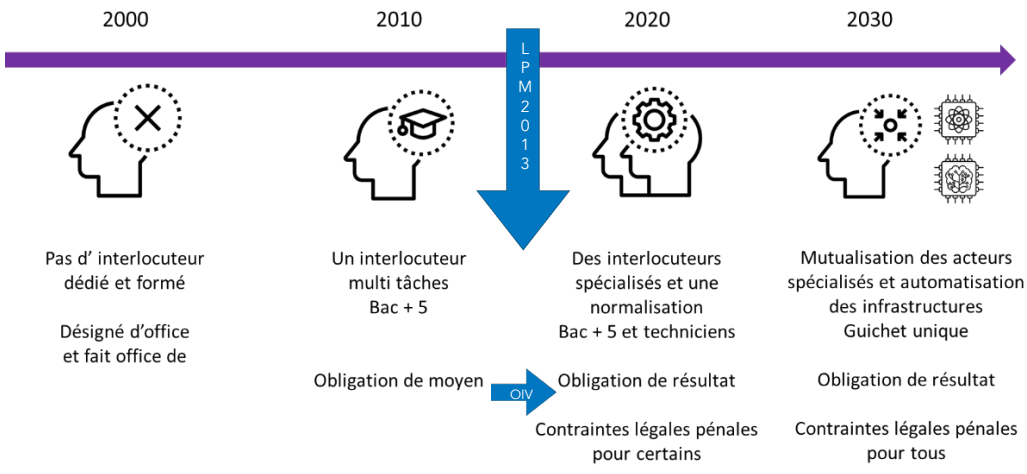
La cybersécurité a évolué au rythme des transformations numériques au sein de l'organisation, mais aussi et surtout par la prise de conscience du responsable et des salariés de la menace à laquelle ils se trouvaient exposés. La taille de l'organisation, son métier, les moyens qu'elle était capable de consacrer à sa sécurité ont été autant des paramètres décisifs pour la bonne prise en compte de la sécurité numérique. Certains métiers liés à la défense, en particulier, ou à l'innovation et aux nouvelles technologies avaient pris en main ce sujet à bras le corps depuis de longues années déjà. Enfin, certains services d'intelligence économique de l'État (DGSI, SISSE, DRSD, Gendarmerie) suivaient et sensibilisaient déjà ces nombreuses entreprises importantes pour la Nation.

Avant les années 2000, et encore aujourd'hui parfois dans les métiers de la vieille industrie, le RSI dépendait du directeur administratif et financier (DAF), si ce n'était le DAF qui faisait « office de » au final. Car c'était le DAF qui bien souvent était en responsabilité des activités transverses. Puis, la direction des systèmes d'information (DSI) est devenue indépendante, en responsabilité des matériels (*hardware*), des logiciels (*software*, dont les *ERP*) et de la sécurité. Cette indépendance a surtout permis au CoDir de consacrer des budgets à la bonne gestion du SI, et de faire en sorte d'éviter que la cybersécurité ne soit qu'un faible pourcentage d'un budget global.

L'évolution des acteurs de la cybersécurité

La structuration de la filière cyber s'est surtout faite grâce au dispositif interministériel de sécurité des activités d'importance vitale (SAIV), piloté par le Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN, qui a été créé en 2006. Il vise à protéger les opérateurs publics ou privés, appelés les opérateurs d'importance vitale (OIV), de la malveillance au sens large, et notamment la menace terroriste. Ce dispositif est venu se consolider en 2013 avec la sortie de la Loi de programmation militaire, qui obligeât les opérateurs d'infrastructures vitales (OIV, au-delà des différents moyens de sécurité déjà mis en place au sein des SI (pour identifier, protéger, détecter, répondre & recouvrer), à avoir une obligation de résultat, c'est-à-dire d'assurer quoi qu'il en coûte la continuité de l'activité. Voilà pourquoi les IOV se sont mis à embaucher des profils ingénieurs sortis des Grandes Écoles, cela pour pouvoir, si une interruption d'activité due à des attaquants devait avoir lieu, démontrer à un juge qu'ils avaient embaucher les meilleurs.

Ce dispositif a été étendu aux opérateurs de services essentiels (OSE), les opérateurs tributaires des réseaux ou systèmes d'information, qui fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. La création de centres d'alerte et de réaction aux attaques informatiques (*CERT* ou *CSIRT*) au sein même des Régions françaises est un pas de plus vers une centralisation de la gestion des menaces.



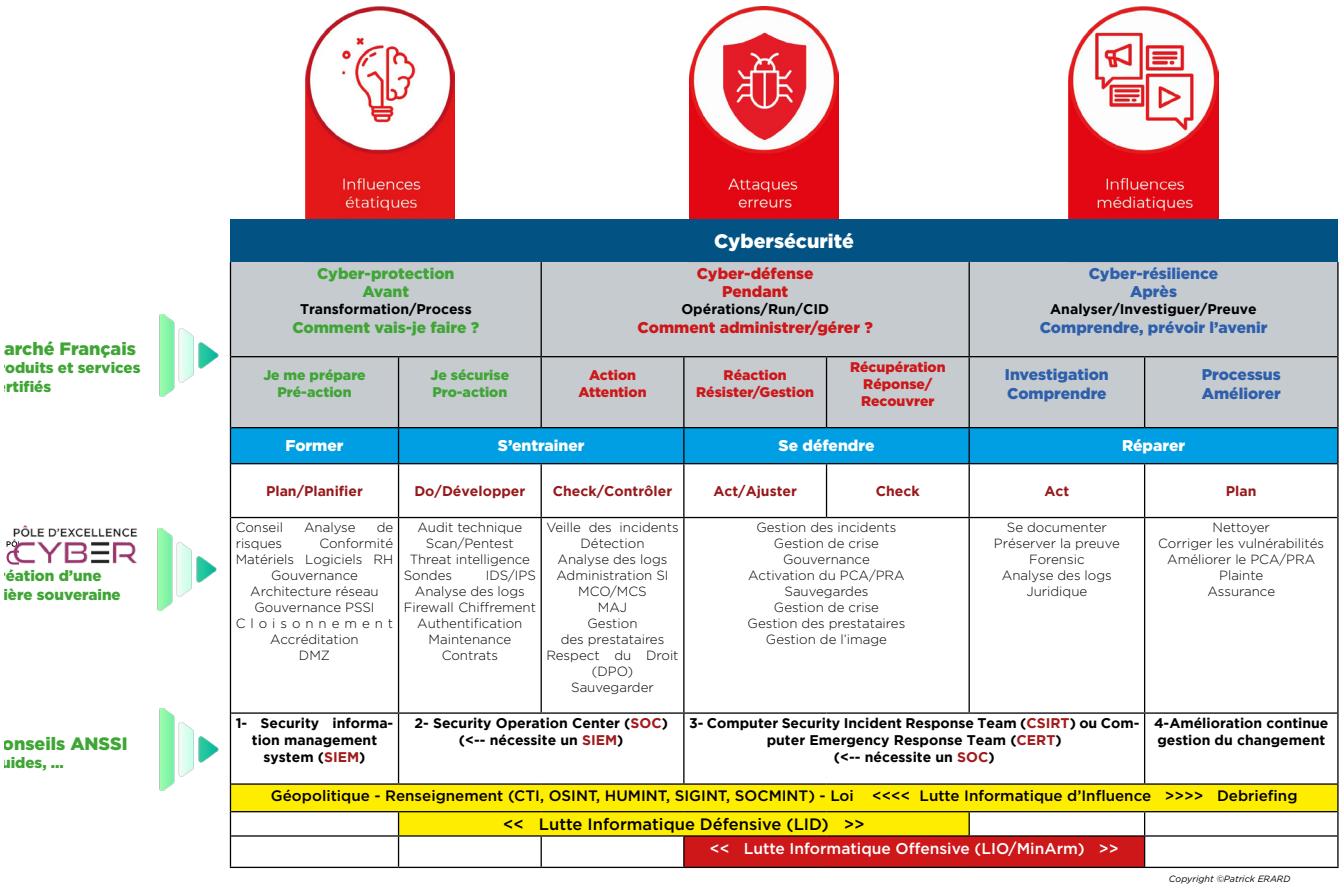
Source : Schémas : ConseilSI / Icônes : Komkrit Noenpoempisut, Abd Majd, ProSymbols de Noun Projet

Les IOV et OSE sont les premières organisations à avoir recruté des gens diplômés à BAC+5 pour assurer même des missions de techniciens, ils se sont donc aperçus très tôt de la nécessité de réhabiliter les métiers de techniciens à BAC+2/3. A cette époque, autour des années 2013, la cybersécurité n'était enseignée que comme spécialité de fin d'études dans les Universités ou Grandes Écoles, seules des formations continues comme certains Mastères spécialisés (validés par la Conférence des Grandes Ecoles, CGE) permettaient de monter véritablement en compétence sur ces métiers.

Dès 2013 l'ANSSI créait le label et l'association CyberEdu, des supports pédagogiques pour les enseignants d'informatique non spécialisés en cybersécurité, afin qu'ils tissent au sein de leurs cours existants les notions qui ont trait à leur discipline (composants, systèmes d'exploitation, développement, authentification, gestion d'identité). Dans la continuité, le Pôle d'excellence cyber a travaillé dès 2014 avec le Rectorat de Rennes afin de former les enseignants des filières Sciences et Technologies de l'Industrie et du Développement Durable, STI2D, puis Services Informatiques aux Organisations, SIO, à la cybersécurité. Un M@gistère cybersécurité a été créé pour les enseignants du Rectorat. L'ANSSI a récemment publié un panorama des métiers de la cybersécurité[1], mais aussi une liste des métiers cyber dans le cadre d'un groupe de travail, GT, du Campus Cyber[2].

Grâce au calcul haute performance (HPC, High Performance Computing) et bientôt à l'arrivée de l'ordinateur quantique, de nouveaux métiers émergent. Cette grande capacité de calcul rend possible l'utilisation des intelligences dites « artificielles », disons plutôt augmentées, et des algorithmes d'apprentissages sur les lacs de données et de métadonnées (*data lakes*), des intelligences qui vont devenir une formidable aide à la compréhension et à la décision, mais vont aussi encore un peu plus remplacer les humains (c'est déjà le cas pour ce qui est des développeurs, avec l'arrivée de Chat *GPT* et des autres outils de type *GPT*[3] (Bard de Google, copy.ai, YouChat, Rytr, Chatsonic, *GPT*-3 Playground ou Jasper, etc.) ou pour les traducteurs en ligne (tel Deepl), rendant du même pas les machines de plus en plus autonomes, et potentiellement indépendantes de leurs créateurs.

L'éthique doit revenir au centre des préoccupations, et il apparait que la morale devrait aussi être enseignée à ces intelligences, Chat *GPT*, par exemple, a ainsi été bridé. Comme pour les « *hackers* », pour les robots l'éthique revient aux centre des préoccupations. L'ordinateur qui tendra bientôt à concurrencer les réflexions et les décisions humaines doit-il être bridé par nos Lois ? N'oublions pas que nous avons créé ces matériels et ces logiciels pour qu'ils soient une aide aux productions humaines, pas pour que les hommes soient contraints par les machines. Pourtant, il apparait évident que l'addiction aux outils informatiques et aux informations qu'ils véhiculent nous guette tous.



1 https://www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf
2 https://campuscyber.fr/resources/referentiel-des-competences-des-metiers-de-la-cyber/
3 Generative Pre-Trained Transformer.

L'évolution des budgets de la cybersécurité

Comme nous l'avons évoqué, les budgets informatique et cybersécurité sont évidemment liés au secteur d'activité. Ainsi pour les entreprises de la base technologique de défense (BITD), les OIV & les OSE ou les entreprises très innovantes, ceux-ci sont plus élevés.

Gains de temps, de productivité, amélioration des processus, conservation des bases de données, ce que nous apportent l'utilisation de nos outils et de nos services informatiques au quotidien reste certes difficilement quantifiable. Cela est encore plus vrai pour ce qui concerne la cybersécurité, car celle-ci recouvre un nombre important de technologies très variées qui répondent toutes ou partie à un panel de besoins de sécurité. Quant à investir dans la sécurité c'est un peu comme étendre son portefeuille d'assurances, c'est obligatoire mais on ne sait jamais à l'avance à quoi cela servira.

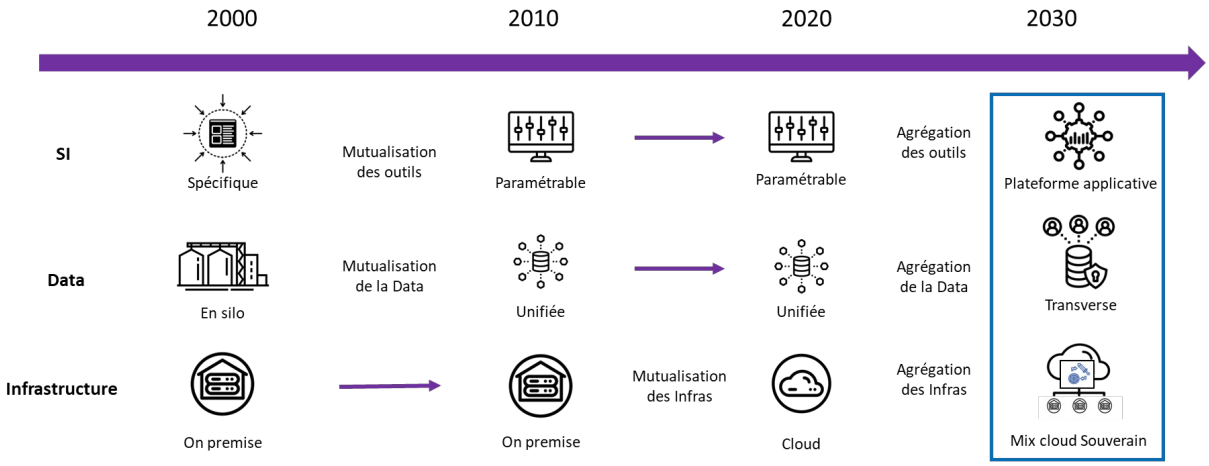
Depuis les années 2000, de nombreuses contraintes réglementaires et sécuritaires se sont imposées aux organisations, à leurs fournisseurs (qui doivent maintenant, par exemple, gérer RGPD[1] pour leurs clients), ainsi que des normes (ISO 27000, 22301, pour ne citer qu'elles, CEN, AFNOR), des certification aussi, pour les auditeurs et les consultants, quasiment toutes états-uniennes (de *l'ISC*[2] [2], *CISSP*[3] *et SSCP*[4] , *de l'ISACA, les CISA*[5] , *CISM*[6] , *CRISC*[7] , *CDPSE*[8] , *CGEIT*[9] *et CSX-P*[10] , de l'EC-Council, le *CEH*[11] , *du GIAC*[12] , *les GSEC*[13] , *GISF*[14] *& GCIH*[15] , ou du *CompTIA Security+, le CASP+*[16] , *de l'OSCP*[17] , ou du *PCI*[18] , etc.) et parfois imposée aux prestataires lorsqu'ils travaillent pour des multinationales ou des clients anglo-saxons, de nombreux modules de formations construits à partir du référentiel du *NIST*[19] par le *SANS Institute* qui avait été créé dès 1989, auxquels la plupart des organisations inscrivent leurs personnels. Citons aussi l'Agence Nationale de la Sécurité des Systèmes d'Information, l'ANSSI, en France qui propose des certifications de premier niveau aux entreprises (CSPN[20]), et de remarquables formations dans son centre de formation à la sécurité des systèmes d'information (CFSSI) aux personnels des administrations.

L'évolution de l'architecture dans les organisations : L'évolution du tout hébergé vers le tout externalisé

Les années 2000 connaissent l'avènement de l'ère de l'informatique industrielle, des systèmes relativement rudimentaires mais robustes basés sur la sûreté de fonctionnement. Des développements spécifiques, des adaptations dites « maison » sont réalisées pour chaque secteur d'activité, pour chaque organisation, selon les besoins des utilisateurs. Le but est alors que les chaines de production fonctionnent bien, les données sont traitées en silos, hébergées sur le site du client, sur ses machines (*on-premise* dit-on), souvent isolées dans une salle serveurs dédiée. Il existe parfois des interfaces entre plusieurs entités, des problèmes cyber apparaissent ça-et-là, mais cela n'arrive qu'aux autres... Dès 1999 le grand Progiciel de Gestion Intégré, PGI, ou *Enterprise Resource Planning* en anglais, *ERP, Salesforce* débutait son activité et proposait déjà ses services en mode logiciel en tant que service, *Software as a Service (SaaS).*

Autour de 2010, des outils spécifiques parfois développés au sein même des structures font place à des produits sur étagères, qui sont paramétrables et mis à jour, l'ère de la sous-traitance est née. Les bases de données permettent de mutualiser des données entre plusieurs utilisateurs issus de départements différents, qui utilisent des outils différents, l'interopérabilité arrive. Toutefois, malgré ces avancées, des matériels et des logiciels plus anciens et tout nouveaux cohabitent, ce qui accentue la dette technique. L'industrie devient alors une cible de choix, surtout pour les concurrents multinationaux souvent aidés par les États qui les portent.

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
2 *International Information Systems Security Certification Consortium.*
3 *Certified Information Systems Security Professional.*
4 *SSCP - Systems Security Certified Practitioner.*
5 *CISA - Certified Information Systems Auditor.*
6 *CISM Certified Information Security Manager.*
7 *CRISC Certified in Risk and Information Systems Control.*
8 *CDPSE Certified Data Privacy Solutions Engineer.*
9 *CGEIT Certified in Governance of Enterprise IT.*
10 *CSX Cybersecurity Practitioner (CSX-P) certification.*
11 *Certified Ethical Hacker.*
12 *Global Information Assurance Certification.*
13 *GIAC Security Essentials GSEC.*
14 *GIAC Information Security Fundamentals GISF.*
15 *GIAC Certified Incident Handler Certification GCIH.*
16 *CASP+ CompTIA Advanced Security Practitioner Certification Plus.*
17 *OSCP OffSec Certified Professional.*
18 *PCI Security Standards Council.*
19 *National Institute of Standards and Technology*, qui définit les standards aux États-Unis : https://www.nist.gov/cyberframework
20 Certification de sécurité de premier niveau.



Source : Schémas : ConseilSI / Icônes :@ WEBTECHOPS LLP, Kukuh Wachyu Bias, Laymik, Nithinan Tatah, Aficons, agus raharjo de Noun Projet

En 2010 les investissements pour le maintien en condition opérationnelle et de sécurité deviennent vraiment conséquents, ils deviennent un enjeu de continuité d'activité pour les organisations. Le métier d'architecte prend alors tout son sens, car les différents outils et services interfèrent entre eux via des plateformes, l'entreprise étendue n'est plus un mythe, une refonte des SI est maintenant nécessaire pour basculer tout ou partie de l'environnement dans l'univers *SaaS*, du *Cloud*. Moins d'investissement à faire, moins de machines à acheter et à gérer, donc de personnels à embaucher pour la maintenance, plus de flexibilité. Des solutions hybrides apparaissent (partie *on-premise* avec du *cloud* privé ou public), des données qui sont redondées dans des datacenters éloignés, parfois hors du pays dans lequel est l'entreprise ou l'administration, les clients réclament alors des formats de données réexploitables dans d'autres technologies.

C'est aussi le début du **AVEC**, pour Apportez Votre Équipement personnel de Communication, ***bring your own device*** en anglais (***BYOD***), qui oblige les organisations à surveiller chaque utilisateur en temps réel, les pares-feux ne sont plus suffisants, des systèmes de détection ou de prévention d'intrusion réseau (**Network-Based Intrusion Detection System, NIDS ou Intrusion Prevention Systems, NIPS**) sont alors installés sur le système d'information, elles alimentent des systèmes de systèmes de gestion de l'information des événements de sécurité (*SIEM*[1]), qui archivent, normalisent, agrègent, corrèlent de très nombreux logs, pour remonter des alertes à des agents des Centres des Opérations de Sécurité (*SOC*).

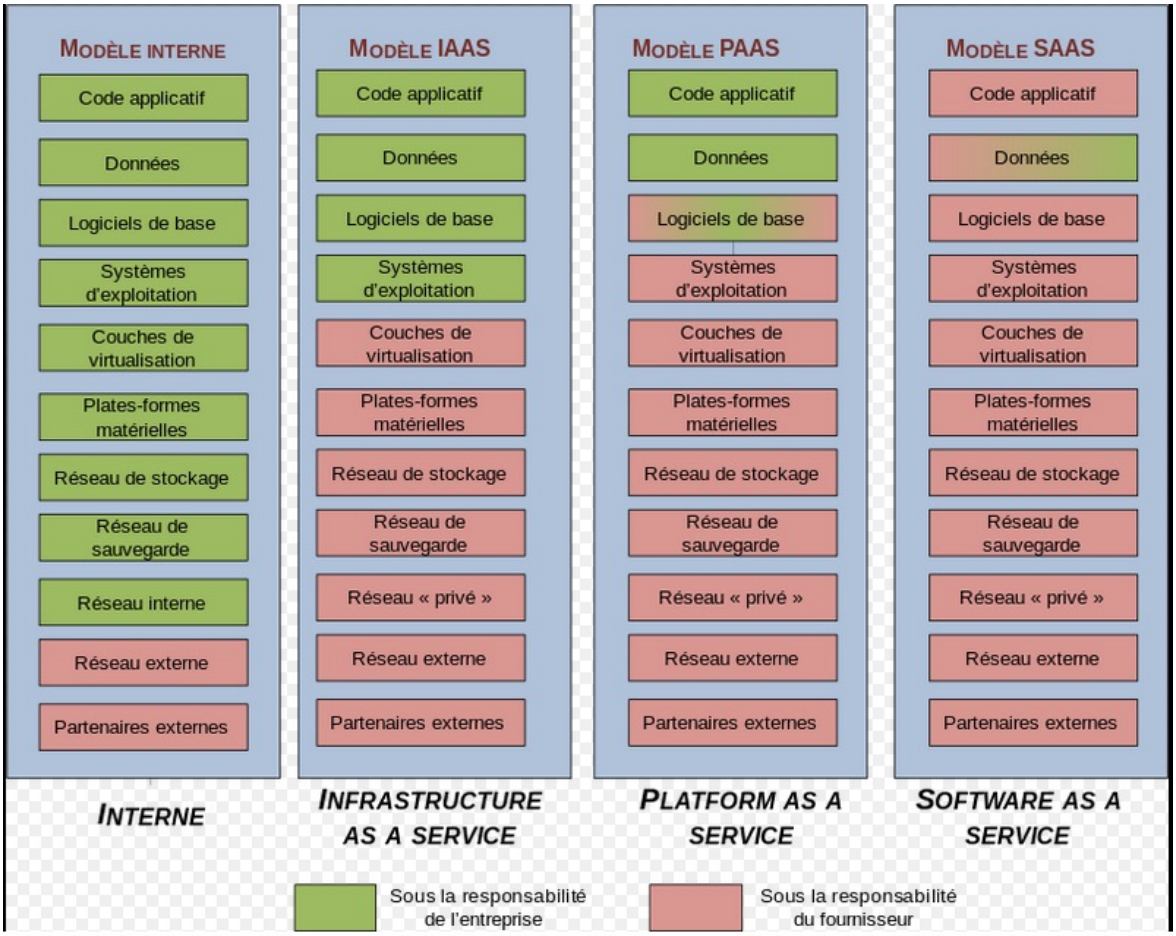
Ce sont les années où les flux réseaux sont chiffrés, même pour les particuliers (*WPA2*[2] , *https*[3] , etc.), et les antivirus classiques à partir de base de signatures virales (*EPP*[4]) sont complétés par des heuristiques poussées qui analyse en temps réel le comportement des machines et de leurs utilisateurs, surveillent la mémoire, vérifient les indicateurs de compromission (*IoC*[5]), les *EDR*[6] & *XDR*. L'arrivée de quantité d'objets connectés, souvent bien moins sécurisés que les classiques ordinateurs, souvent connectés de surcroit à l'Internet, augmente la surface d'attaque des SI classiques.

1 *Security information management system.*
2 *Wi-Fi Protected Access,* chiffrement CCMP pour plus de sécurité.
3 *Hyper Text Transfer Protocol Secure*, extension sécurisée du protocole HTTP, les données échangées avec le site Web sont chiffrées.
4 *Endpoint Protection Platform* en anglais, installé sur chaque poste utilisateur (*Endpoint*) et sur les serveurs de l'entreprise.
5 *Indicator of compromise* en anglais.
6 *Endpoint Detection and Response ou Extended Detection and Response*, pour étendue, qui protège les EPP déployés, supervise en temps réel de l'ensemble de l'activité et des flux du réseau informatique, assure la *Cyber Threat Intelligence*, la collecte d'informations sur les menaces ou les acteurs de la menace et une détection des comportements malveillants.

Dès 2013 la dynamique *Cloud* s'accélère et l'on passe d'offres *IaaS*[1] , au *PaaS*[2] , puis enfin à une infrastructure totalement dans le *Cloud* (Office 365 en est l'exemple, Microsoft Azure maintenant). Le risque majeur de ce phénomène, initié par les GAFAM et autres multinationales du numérique, c'est que les données des organisations soient hébergées sur des serveurs situés à l'étranger, et qui ne répondent pas aux lois sur la protection des données européennes.

Ce choix d'utiliser le *Cloud* reste souvent une solution de facilité pour des décideurs, aussi harcelés par les services mercatiques puissants de ces offreurs de solutions. Dirigeants et commerciaux ne comprennent pas toujours bien les enjeux de ces techniques, ils ne savent généralement pas, par exemple, que les formats des données archivées ne seront pas toujours récupérables dans d'autres technologies concurrentes, une volonté de certains éditeurs pour se rendre indispensables.

Aujourd'hui, nos ordinateurs (Apple, Asus, Compaq, Dell, Fujitsu, HP, Lenovo, MSI, Toshiba, etc.), téléphones (Android ou iOS), tablettes, montres connectées, nos systèmes d'exploitation (Windows, MacOS), nos logiciels, *ERP* ou *CRM*, nos messageries sont bien souvent des produits et services étrangers. Alors **il faut chiffrer nos données sur les réseaux ou dans nos bases de données** et éviter de les mettre dans des *Cloud* non maîtrisés lorsqu'elles sont importantes pour l'organisation. La France possède un haut niveau d'expertise en mathématique, qui s'avère essentiel dans ce domaine, ou celui de l'IA.



Source : https://fr.wikipedia.org/wiki/Cloud_computing

1 Infrastructure as a service.
2 *Plateform as a Service.*

Mieux maîtriser nos données et métadonnées personnelles

Peu à peu nous nous sommes habitués à ces matériels et outils qui sont en quelque sorte devenus le prolongement de nos sens, de notre pensée immédiate, nous sommes passés de *l'opt-in* (pour la publicité électronique par mail, SMS, MMS, automates d'appel ou fax, c'est obtenir le consentement du destinataire de la publicité : s'il n'a pas dit «oui», c'est «non», à défaut de s'opposer à recevoir des publicités, la personne pourra en recevoir), à *l'opt-out* (c'est lorsque le destinataire de la publicité ne s'est pas opposé : s'il n'a pas dit «non», c'est «oui»). Bien qu'autorisé en France s'il s'agit d'e-mailing concernant des activités commerciales entre entreprises (*BtoB*), *l'opt-out* est interdit pour les particulier et le *BtoC*, seul l'opt-in actif est légal dans le cadre d'e-mailing à destination de personnes physiques (particuliers)[1].

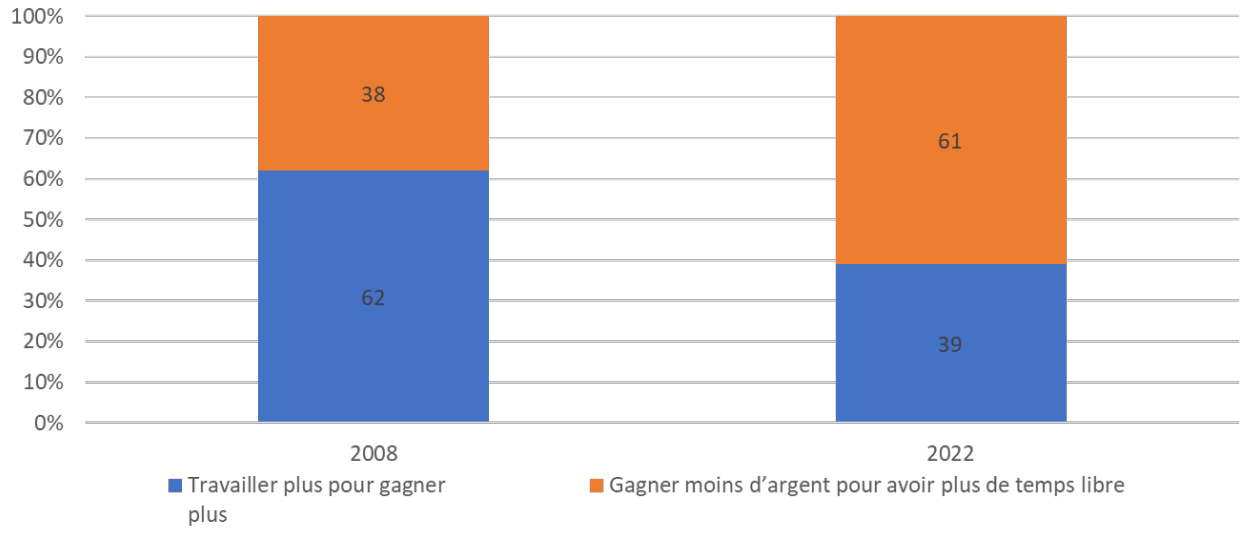
La sécurité des sites *Web* est aussi l'une des principales préoccupations de la CNIL quant à éviter que vos données personnelles soient volées et diffusées sur la toile[2]. Google avait commencé à tester la fiabilité des sites *Web* qu'il référence pour avertir les usagers de sites pas ou peu sécurisés[3].

LE CHANGEMENT DES MENTALITÉS

Depuis la période du COVID 19, différents facteurs ont évolués, dont les mentalités : travailler moins pour vivre mieux

Dans un monde plus anxiogène et après une longue période d'isolement subi consécutivement aux restrictions Covid19, les étudiants et les salariés se concentrent plus sur leur bien-être au travail, ils souhaitent pouvoir profiter d'au moins 2 journées de télétravail par semaine, ce qui est parfois difficile voire impossible dans des entreprises qui traitent des données sensibles ou classifiées par exemple. Les entreprises ont dû aussi rapidement s'adapter à cette main d'œuvre nouvelle, qui n'hésitera pas non plus à changer de poste ou à démissionner plutôt que de supporter trop de pression ou de contrainte de la part de l'employeur, la tension sur le recrutement dans la filière leur permettant de retrouver du travail quasi instantanément.

Souvenons-nous qu'au début du quinquennat du Président Sarkozy un des leitmotivs était de « travailler plus pour gagner plus », ce qui était souhaité alors par 62% des salariés, gagner plus d'argent, mais avoir moins de temps libre. 38% quant à eux désiraient « gagner moins d'argent pour avoir plus de temps libre ». Cette tendance s'est aujourd'hui inversée.



Sondage IFOP pour Solutions solidaires

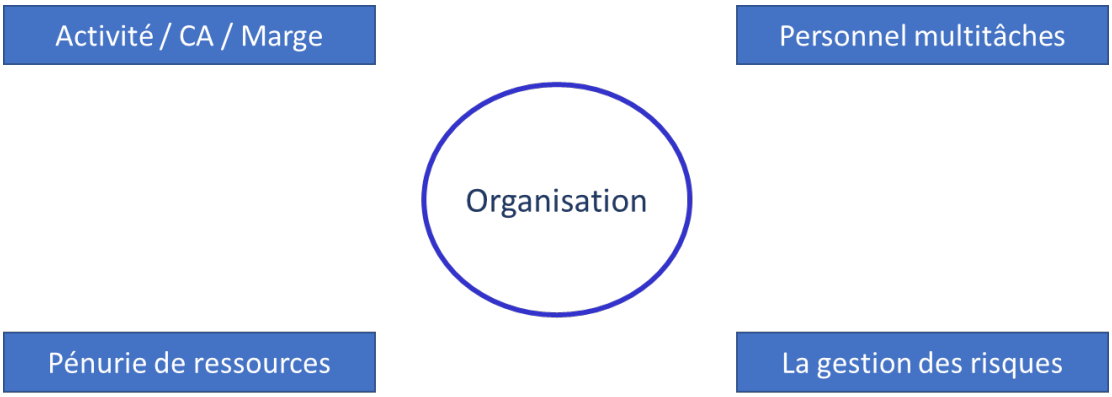
1 https://www.macg.co/aapl/2021/03/des-start-ups-francaises-portent-plainte-contre-apple-aupres-de-la-cnil-120113
https://www.nextinpact.com/article/49870/google-analytics-retour-sur-mise-en-demeure-cnil
2 https://www.cnil.fr/fr/cybersecurite-15-mises-en-demeure-lencontre-de-sites-web-insuffisamment-securises
3 https://www.blogdumoderateur.com/google-site-web-securise/

61% des salariés souhaiteraient désormais « gagner moins d'argent pour avoir plus de temps libre », contre seulement 39% qui préféreraient au contraire « gagner plus d'argent mais avoir moins de temps libre ».

Source : *Avant et post COVID, une inversion entre 2008 et 2022, fondation Jean Jaurès (GROSSE FATIGUE ET ÉPIDÉMIE DE FLEMME : QUAND UNE PARTIE DES FRANÇAIS A MIS LES POUCES Jérôme Fourquet, Jérémie Peltier 11/11/2022)*

Les contraintes du dirigeant

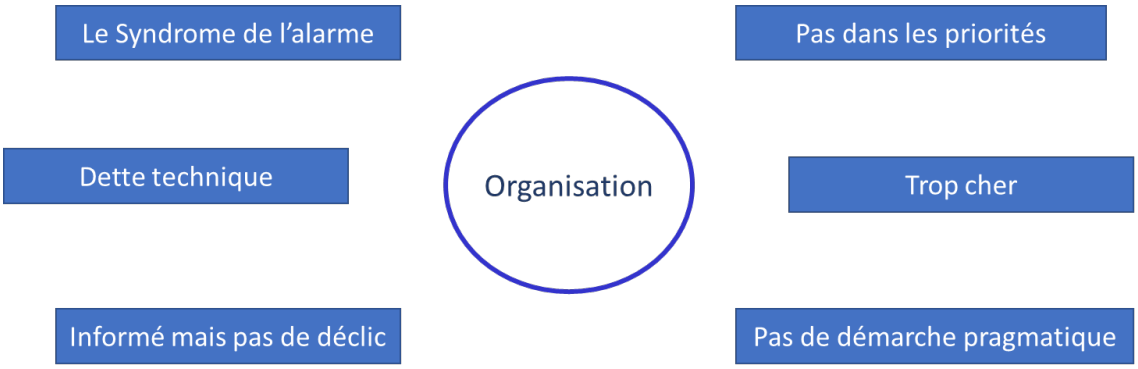
Le dirigeant est soumis en permanence à une bonne gestion des priorités pour son organisation. Si il possède une vision pragmatique de son métier, les moyens de mise en œuvre de sa stratégie et ses arbitrages sont parfois complexe, surtout dans ce contexte politique et géopolitique très instable, sachant aussi que plus la structure est petite, plus les ressources et le budget sont limitées.



Source : Pôle d'excellence cyber

Les freins du dirigeant

La gestion en conduite du dirigeant (priorités, coûts, absence de ressource capable de porter la cyber) ramène souvent celui-ci à mettre en proportion l'investissement fait (ROI) et ce qu'il est supposé rapporter.



Source : Pôle d'excellence cyber

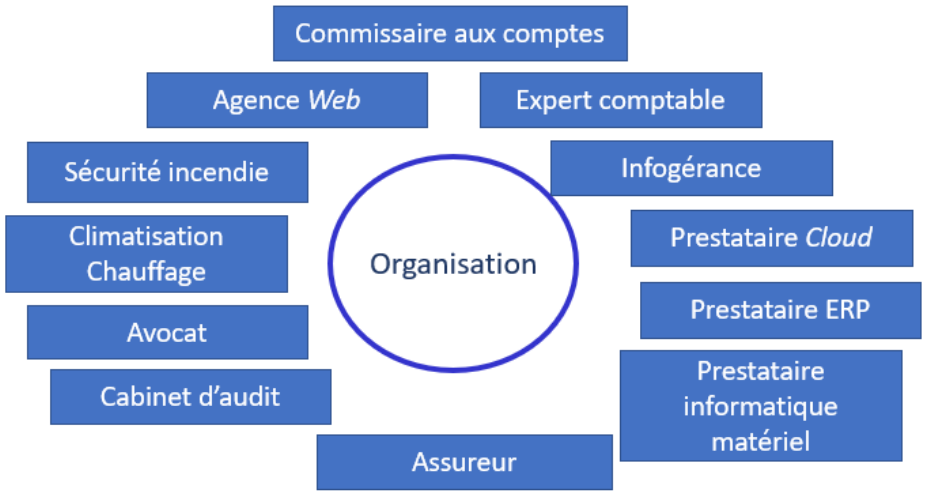
Tant qu'il n'a pas été confronté à une attaque, le chef d'entreprise, fort de son optimisme et de sa pensée positive, espère qu'il ne le lui arrivera rien… La plupart des chefs d'entreprises intègrent maintenant qu'il faille tenter de limiter au maximum le préjudice d'une potentielle attaque sur leur SI ou leur chaine de production.

La Cybersécurité fait maintenant partie intégrante du budget *IT* de la plupart des organisations, même si celui-ci est parfois encore trop faible surtout chez les plus petits. C'est en moyenne 2% du CA pour *l'IT* et 3% du budget de *l'IT* pour la cyber (source : *BoostAeroSpace* / *AirCyber*). L'ANSSI recommande de consacrer au moins 5 % du budget informatique à la cybersécurité, mais, selon une étude Stormshield, plus de 30 % des sociétés interrogées n'atteignent toujours pas ce palier.

Démarche pragmatique : les problématiques cyber et le vocabulaire parfois technique rebutent souvent les chefs d'entreprises qui ne dispose pas du temps nécessaire pour bien en évaluer les enjeux & les moyens à mettre en œuvre. Le Pôle d'excellence cyber aidé du MinArm et du MinInt, tout comme l'ANSSI et le SISSE, proposent des sensibilisations ciblées aux cadres et dirigeants des structures non cyber. Le Pôle a aussi sorti un Guide de sécurité numérique pour les collectivités, PME/PMI et petites organisations qui permettra à ces structures d'accélérer leur transition cyber. Ce Guide comprend 23 tutoriels explicites pour sécuriser son système Windows, son réseau et ses pratiques, qui existent aussi en vidéo sur notre chaine YouTube.

Les partenaires de contact

Parce qu'ils connaissent l'activité de l'organisation, son histoire, son métier, les partenaires de contact sont aussi à même d'accélérer l'intégration des problématiques cyber.



Les partenaires de contact sont en capacité d'apporter une aide en terme de bonnes pratiques.

Source : Pôle d'excellence cyber

Ces différents partenaires sont à même d'apporter un premier niveau de conseil et d'orienter le dirigeant vers des solutions (produits, services ou architectures) ou des acteurs (CyberLab) qui seront à mêmes de répondre aux différents besoins.

Les acteurs de proximité

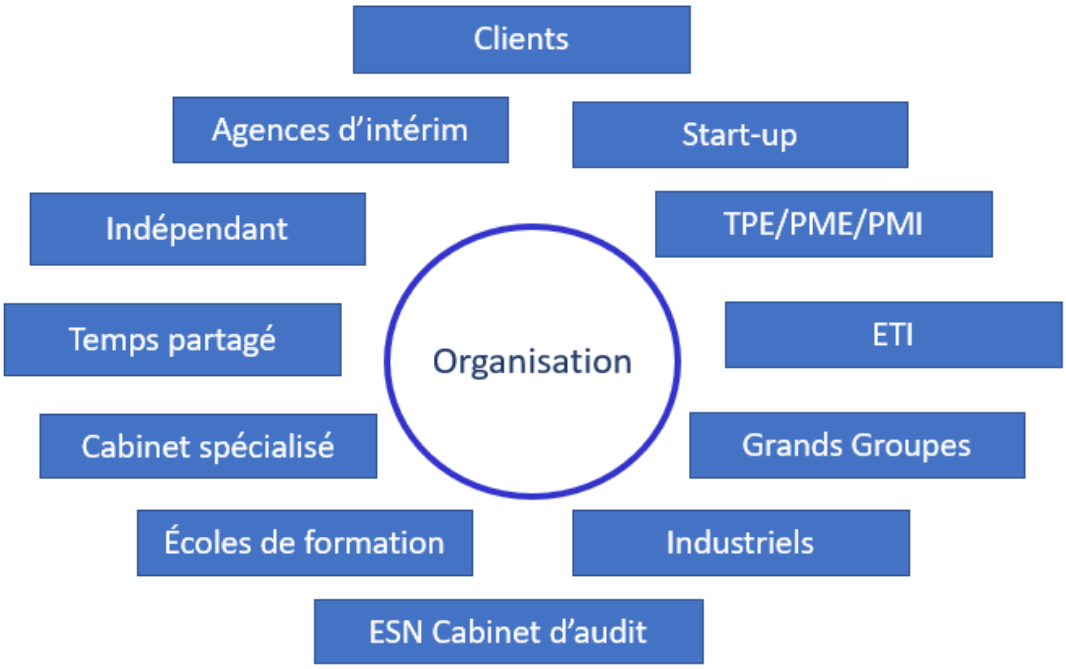
Les acteurs de proximité peuvent aussi jouer un rôle d'information et de formation en termes de bonnes pratiques, ils peuvent recommander des prestataires de confiance et parfois proposent des Diagnostics. Le Pôle d'excellence cyber propose son Diagnostic CARE dans la cadre du projet européen EDIH à toutes les entreprises bretonnes qui en feront la demande. CARE est aussi un accompagnement des structures par un consultant pour qu'elles évaluent leur niveau de maturité et qu'elles organisent leur transition vers la cybersécurité. 50% du coût du financement de ce diagnostic CARE est pris en charge par l'Europe.

Les acteurs de proximité, dont des services de l'État, sont en capacité d'apporter une aide en terme d'information, de référencement de partenaires, de bonnes pratiques autour du numérique.

Source : Pôle d'excellence cyber

Les autres acteurs du marché

Le Diagnostic CARE permettra à l'auditeur du Pôle de recommander des services, listés sur un catalogue de services auquel auront répondu les entreprises cyber françaises. Les services couverts par ce catalogue CyberLab vont de la formation du conseil, aux différents audits, réseaux et systèmes, en passant par la certification et le test. Toutes les entreprises listées sont françaises et reconnues comme d'excellents spécialistes dans leurs domaines d'intervention.



Source : Pôle d'excellence cyber

L'évolution des profils de la cybersécurité

Les profils se décomposent en deux niveaux :

- Puisque la France ayant décidée de vivre de ses brevets, la R&D prend une part très importante dans le développement de nos entreprises cyber.
- La conception et le déploiement d'outils et de systèmes, et de services à forte valeur ajoutée restent l'apanage d'ingénieurs et d'universitaires diplômés de Bac+5 à Bac+8, souvent des gens avec une formation initiale technique ou organisationnelle en informatique avec une spécialisation tout au long de la vie vers la cybersécurité, ou des plus jeunes qui possèdent une formation initiale cyber, les cursus prenant depuis 2013 mieux en compte ce besoin. Des initiatives comme CyberEdu ou SecNumEdu ont permises cette dynamique.

Toutefois, le déploiement et le paramétrage des outils, leur exploitation, la lecture des logs remontés par les systèmes de détection, systèmes de gestion de l'information des événements de sécurité (*SIEM*), le travail du Centre des Opérations de Sécurité (*SOC*) sont des tâches dédiées majoritairement à des techniciens de niveau Bac +2/4 :

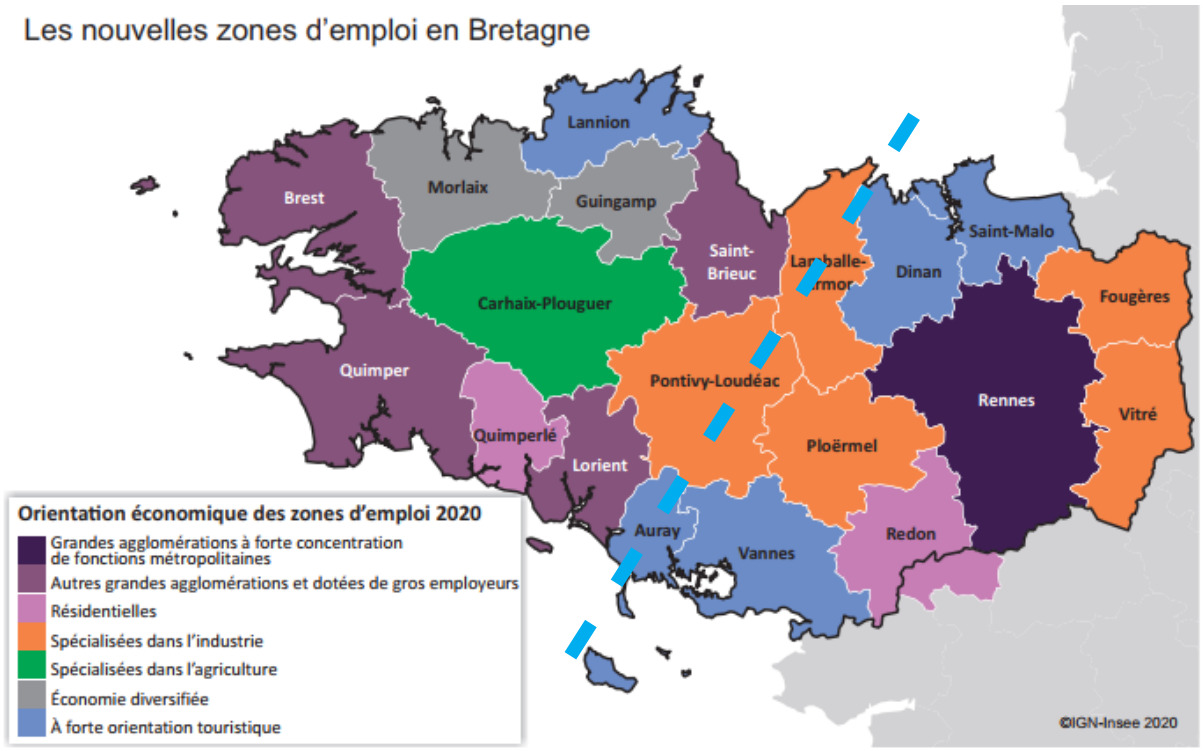
- Des gens possédant un BTS ou un DUT avec une option cyber ;
- Des certifications métier : produit ou service ;
- Des compétences techniques en termes de MCO/MCS[1] , de développement, d'administration système ou réseau ;
- Et bien souvent de bonnes notions d'investigation et de gestion de crise.

FOCUS SUR LA BRETAGNE

Les zones d'emploi bretonnes et les Bretons

Les vingt zones d'emploi bretonnes sont bien diversifiées, la Bretagne est l'une des rares régions françaises qui couvre les sept catégories.

1 Maintient en condition opérationnelle, ou maintient en condition de sécurité.

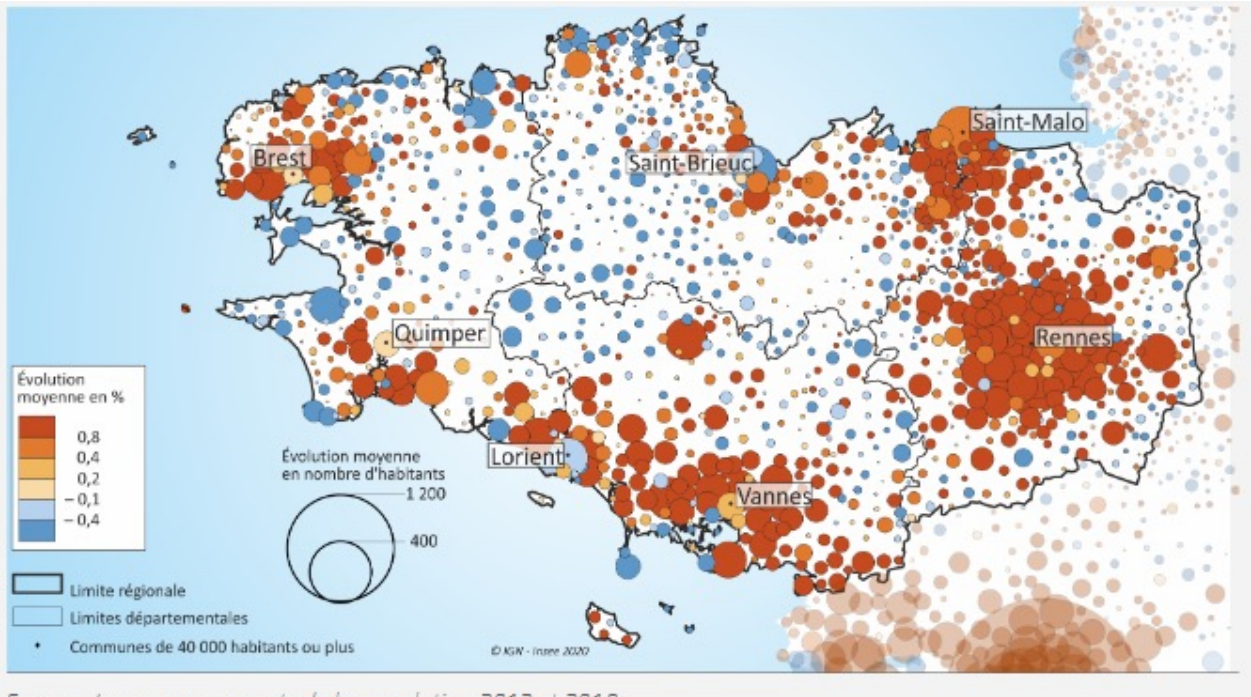


Source : Insee, recensements de la population 2016 et 2017, Clap 2015, enquêtes de fréquentation touristique 2019.

La Bretagne peut être scindée en deux territoires différenciés :

- L'Ouest de la Bretagne, qui dispose de quatre grandes agglomérations à chaque extrémité (Brest, Quimper, Saint Brieuc et Lorient) et en son centre un bassin agricole ;
- L'Est de la Bretagne, qui gravite autour du pôle d'attraction Rennais du fait de sa situation de capitale administrative et son tissu industriel et tertiaire.

Évolution de la population des communes entre 2013 et 2018 en Bretagne



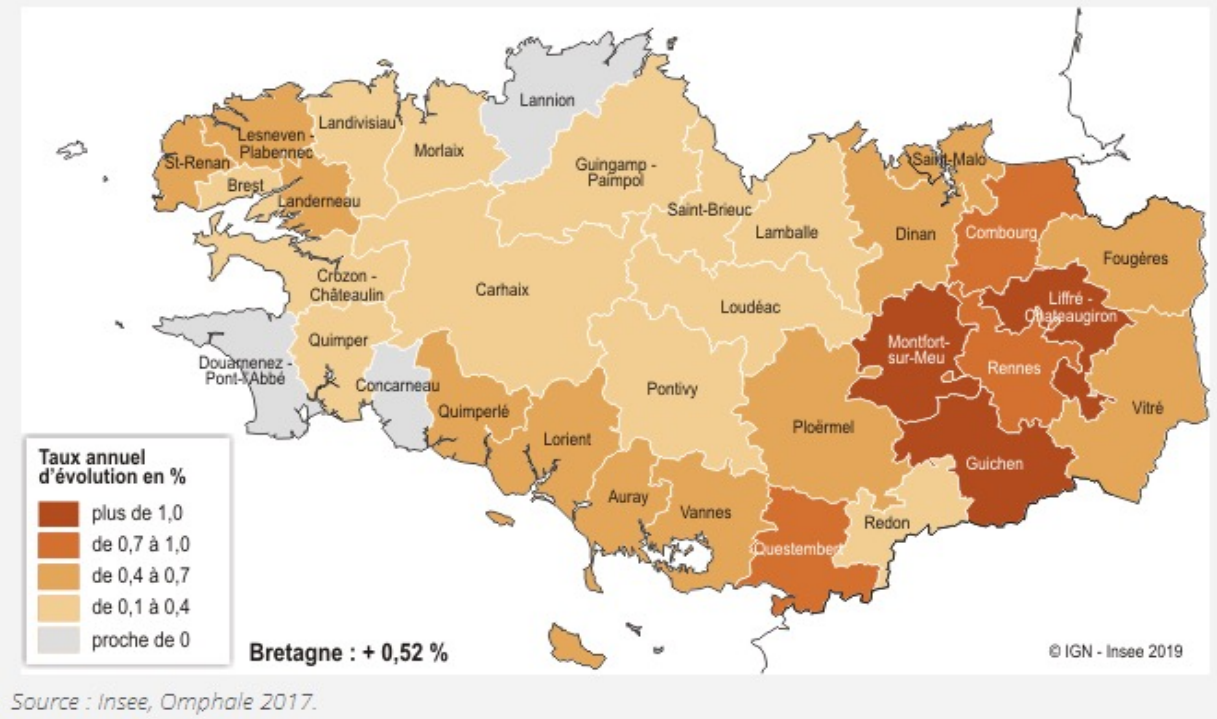
Source : Insee, recensements de la population 2013 et 2018.

Cette carte montre bien où se concentre l'attractivité du territoire Breton, majoritairement autour des grandes agglomérations et sur la côte par l'attrait du littoral, en particulier au Sud pour la partie Ouest, et autour de Saint-Brieuc et Saint-Malo pour l'Est.

La période Covid a motivé nombre de Parisiens à s'exiler vers le territoire Breton. Si ces classes CSP+ ont le plus souvent les moyens de s'acheter des biens en centre Rennes ou Brest ou sur la petite ceinture, ou sur le bord de mer, toutefois le prix des biens et des loyers autour des centres villes des deux grandes métropoles bretonnes ou en bordure de rivage contraint les jeunes et les nouveaux arrivants à rechercher un logement entre 20 ou 30 km plus loin.

Notons que la population du centre Bretagne a tendance à décroitre.

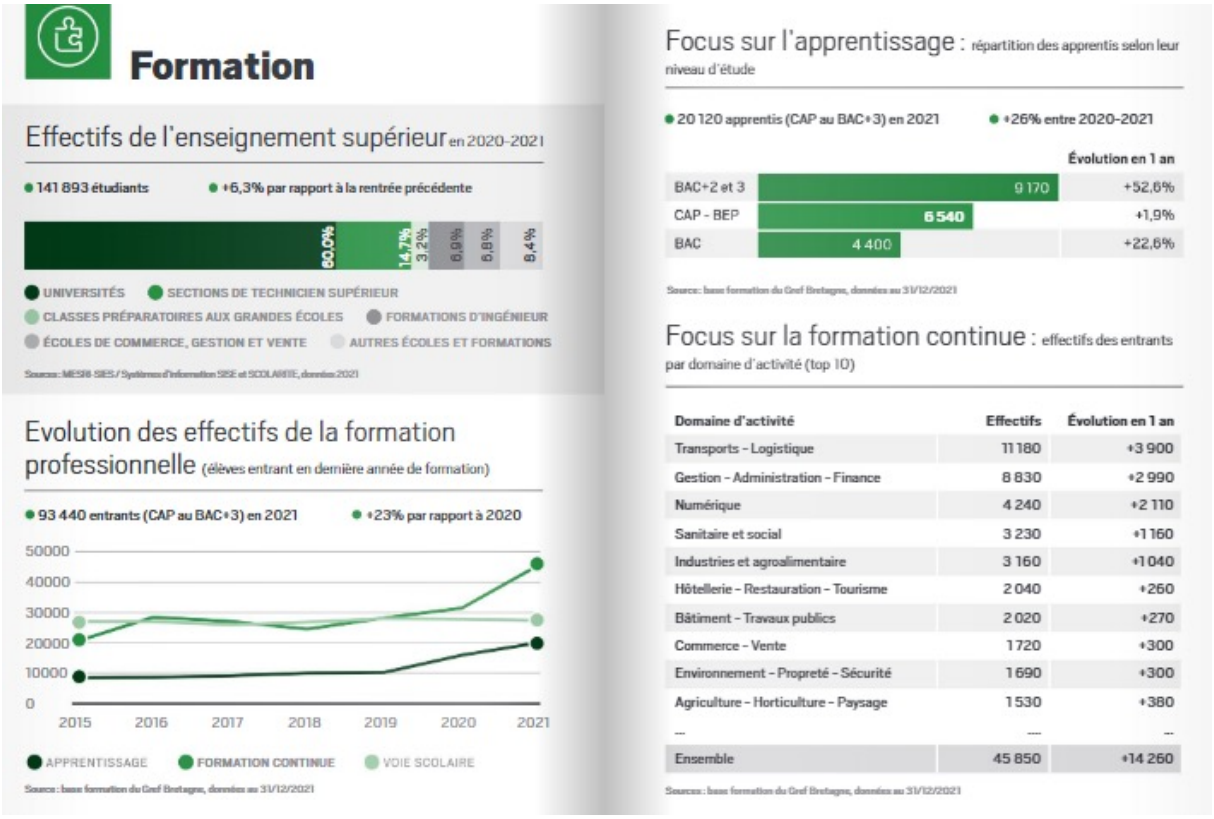
Projection de l'évolution de population entre 2018 et 2040 (scénario central)



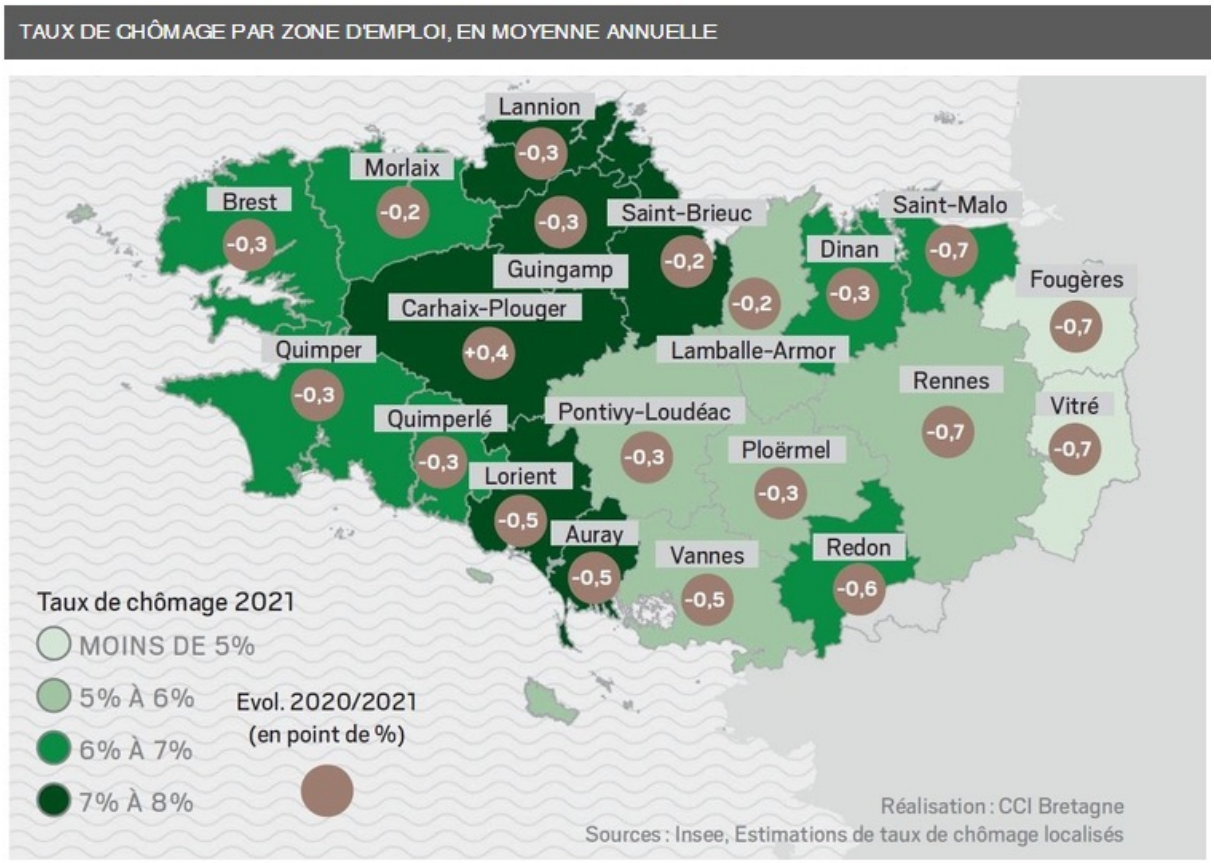
Source : Insee, Omphale 2017.

Si l'on prévoit que la population bretonne va augmenter de plus de 400 000 habitants d'ici 2040, l'évolution la plus forte sera tout de même bien localisée surtout à l'Est autour de Rennes, mais aussi à l'Ouest autour de Brest.

Effectifs de la formation



Taux de chômage par zone d'emploi, moyenne annuelle



L'ACTIVITÉ BRETONNE

Le grand ouest attractif

Les métropoles du Grand-Ouest sont les plus attractives de l'Hexagone : enquête NHU Bretagne réalisé en ligne entre le 11 Octobre et le 09 Novembre 2020 auprès de 3454 actifs vivant dans les vingt principales métropoles de l'Hexagone, publiée le 17 décembre 2020, mise à jour le 12 mars 2023.

Il s'agit ici de la perception des habitants eux-mêmes face à ces critères selon 7 critères. Dans l'Hexagone, ce sont Nantes, Brest et Rennes, qui tiennent les meilleures places, selon une récente étude de HelloWork, une plateforme de recrutement, auprès d'un panel d'actifs des vingt plus importantes métropoles de l'Hexagone.

L'étude retient sept critères.

Pour l'ensemble des critères, c'est Rennes, la capitale administrative actuelle de la Bretagne, qui se place sur la plus haute marche du podium. Rennes a déjà été par le passé sur les plus hautes marches d'autres études européennes. Puis Nantes, la plus grande ville de Bretagne, est en second. Enfin, Strasbourg l'Alsacienne sur la troisième marche. Brest est cinquième, juste derrière Lyon. Les trois métropoles bretonnes se placent donc dans le Top5 des villes les plus attractives de l'Hexagone. Paris, l'auto-proclamée « ville lumière » s'éteint à la dix-huitième place.

- La qualité de la vie : Rennes et Brest respectivement premier et deuxième, devant Tours.
- Le coût de la vie : Brest sur la deuxième marche, entre Saint Étienne et Toulouse
- Le dynanisme économique : Nantes et Rennes dans cet ordre sur les deux premières marches, Lyon en troisième place.
- L'état du marché du travail : Paris sombre depuis plusieurs années dans les profondeurs du classement général mais est encore en tête du palmarès, puis Nantes et Rennes.
- Les équipements liés à la mobilité dite douce : la métropole alsacienne de Strasbourg devance la bretonne de Rennes, avant Grenoble.
- La qualité des infrastructures : la métropole alsacienne de Strasbourg en tête du classement, puis à nouveau Rennes deuxième métropole la plus attirante de l'Hexagone, Dijon 3ième..
- La qualité des loisirs, de la culture et de l'environnement : pour ces critères de vie importants, à nouveau les métropoles de Nantes plus au Sud, puis Rennes. Grenoble obtient la troisième place.

Critères	1er	2ième	3ième
Les métropoles qui attirent	Nantes	Rennes	Strasbourg
Qualité de la vie	Rennes	Brest	Tours
Coût de la vie	Saint Étienne	Brest	Toulouse
Dynamisme économique	Nantes	Rennes	Lyon
Marché du travail	Paris	Nantes	Rennes
Équipements liés à la mobilité douce	Strasbourg	Rennes	Grenoble
Qualité des infrastuctures	Strasbourg	Rennes	Dijon
Qualité des loisirs, culture et environnement	Nantes	Rennes	Grenoble

https://www.nhu.bzh/metropoles-bretonnes-attractives/

La Bretagne attractive

Notons que presque la moitié des cadres qui résident en Bretagne sont nés dans une autre région ou à l'étranger, ce qui montre l'attractivité de ce territoire. En 2016, la Bretagne comptait 970 500 habitants nés dans une autre région ou à l'étranger, soit un peu moins du tiers de sa population. Parmi eux, 27 % sont franciliens de naissance, 17 % sont nés à l'étranger et 14 % sont natifs des Pays de la Loire.

La majorité des habitants nés hors de la région fait partie de la population active (53 %) et la part des retraités est équivalente à celle qui est observée chez les natifs de Bretagne.

Le secteur public en Bretagne

La région Bretagne compte de nombreuses collectivités et établissements public territoriaux :

- Le Conseil Général de Bretagne ;
- 4 départements ;
- 1208 communes ;
- 9 EPCI à fiscalité propre ;
- 296 syndicats.

La Bretagne compte plus de 285 000 fonctionnaires, tous statuts confondus, dans trois fonctions :

- La fonction publique d'Etat (FPE) : 45 % soit 128 500 agents ;
- La fonction publique territoriale (FPT) : 33 % soit 95 000 agents ;
- La fonction publique hospitalière (FPH) : 22 % soit 62 700 agents.

Les agents de la fonction publique représentent 25 % de l'emploi salarié régional.

Le secteur privé en Bretagne hors agriculture

La Bretagne compte plus de 684 200 salariés des secteurs marchands avec plus de 95 000 entreprises.

- Micro Entreprise : 18 % des salariés des secteurs marchands, 126 900 salariés en 2017 ;
- PME : 33 % des salariés des secteurs marchands, soit 227 100 salariés en 2017 ;
- ETI : 27 % des salariés des secteurs marchands, soit 187 600 salariés en 2017 ;
- Grandes entreprises : 22 % des salariés des secteurs marchands, soit 142 600 salariés en 2017.

Source : INSEE flash Bretagne n°68.

L'agriculture en Bretagne

La Bretagne compte plus de 67 500 actifs (exploitants, collaborateurs et salariés) travaillant dans les exploitations agricoles, 42 % sont des salariés soit 3,7 % des emplois bretons : 25 006 exploitations agricoles en Bretagne en 2021 selon la MSA[1].

L'emploi breton dépend de l'agriculture :

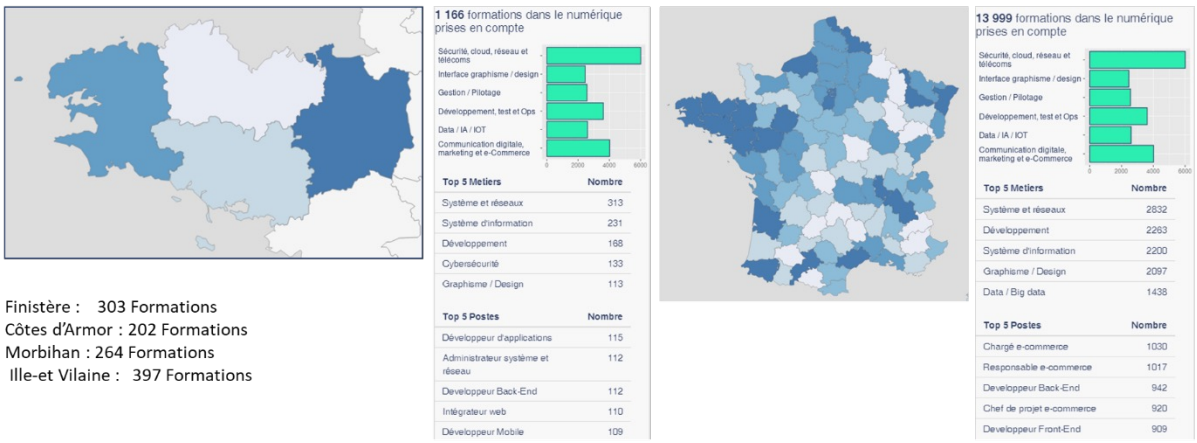
- Plus de 40 % des emplois industriels sont dans le secteur agroalimentaire, qui utilise des chaines de production et de nombreux automates industriels ;
- Cela représente près de 9 milliards d'euros de productions agricoles, les exploitants ayant dû fortement s'industrialiser ces dernières années ;
- Près de 20 milliards d'euros de chiffre d'affaires générés par l'agroalimentaire breton, dont 42 % dans l'industrie de la viande ;
- Les exportations agricoles et agroalimentaires comptabilisent plus de 4 milliards d'euros de ventes.

Source : CAB ABC 2022.

Vision du marché du Numérique en Bretagne versus la France

Dans tous les projets et métiers du numérique la cybersécurité devient essentielle. Une vision de ce qui se passe sur le territoire peut aussi permettre de comprendre les enjeux en termes de formation et de recrutement.

Les Formation numériques



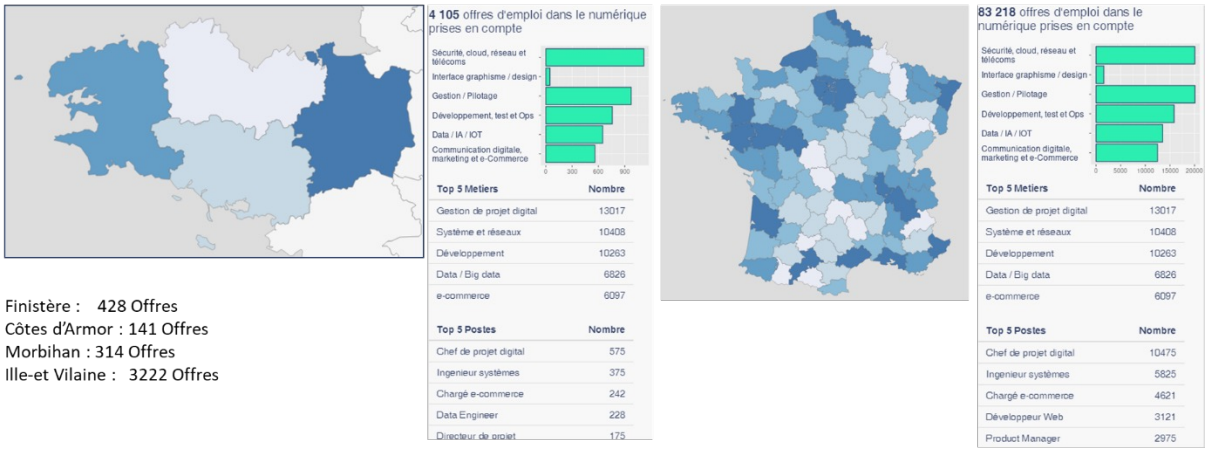
Finistère : 303 Formations
Côtes d'Armor : 202 Formations
Morbihan : 264 Formations
Ille-et Vilaine : 397 Formations

Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

L'offre de formation est principalement localisée en Ille-et-Vilaine ainsi que dans le Finistère, majoritairement à Brest, elle représente plus de 60 % des formations.

1 Sécurité sociale agricole

Les offres d'emploi dans le numérique

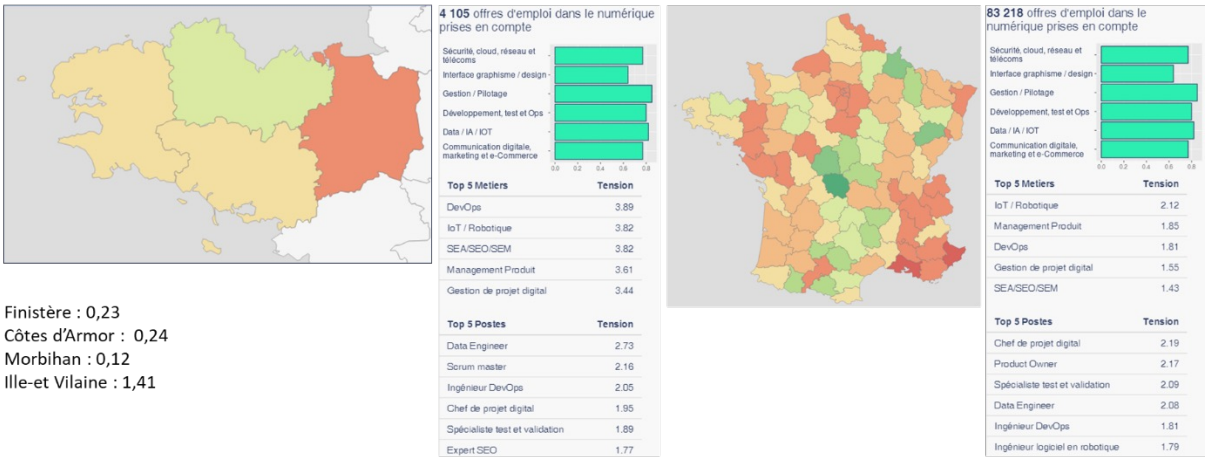


Finistère : 428 Offres
Côtes d'Armor : 141 Offres
Morbihan : 314 Offres
Ille-et Vilaine : 3222 Offres

Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

Les offres d'emplois sont principalement localisées en Ille-et-Vilaine, elles représentent plus de 78 % des offres.

L'indice de tension dans le numérique



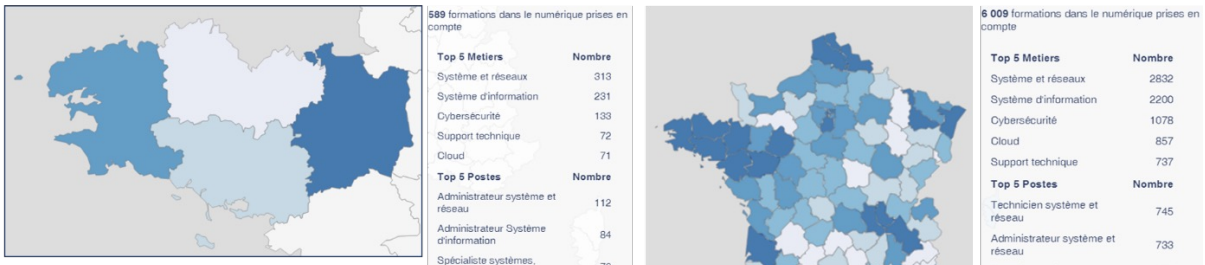
Finistère : 0,23
Côtes d'Armor : 0,24
Morbihan : 0,12
Ille-et Vilaine : 1,41

Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

L'indice de tension est fort en Ille-et-Vilaine, il ne cesse de croitre. C'est aussi le cas de la Région Pays-de-la-Loire, PACA et Île-de-France. On retrouve les métiers en tension, DevOps, les métiers de l'industrie (*IoT*/Robotique), de bons gestionnaires de projets, tous les métiers liés à l'IA et aux Data, des ingénieurs commerciaux et des spécialistes du référencement *Web*.

La vision Sécurité, cloud, réseaux et télécom de la Bretagne versus la France

Les formation Sécurité, cloud, réseaux et télécom

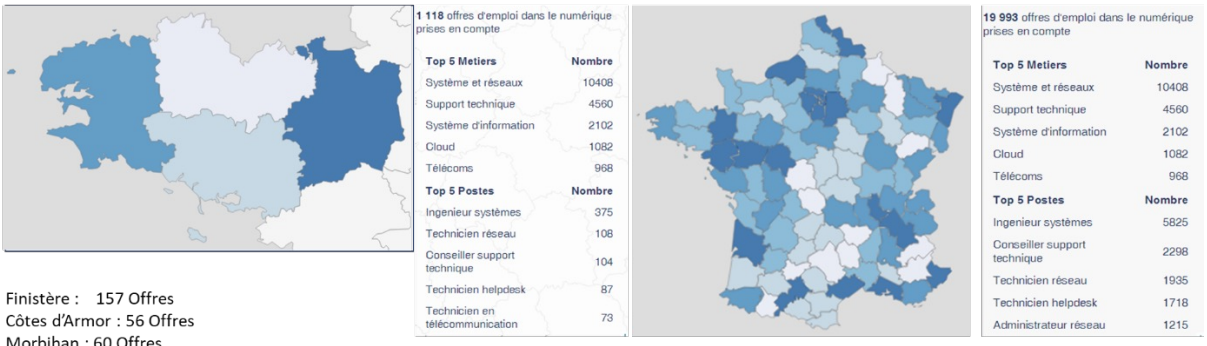


Finistère : 163 Formations
Côtes d'Armor : 117 Formations
Morbihan : 132 Formations
Ille-et Vilaine : 177 Formations

Source : https://grandeecolenumerique.fr/

L'offre de formation est principalement localisée en Ille-et-Vilaine ainsi que dans le Finistère, cela représente plus de 57 % des formations.

Les offres d'emploi dans la Sécurité, cloud, réseaux et télécom

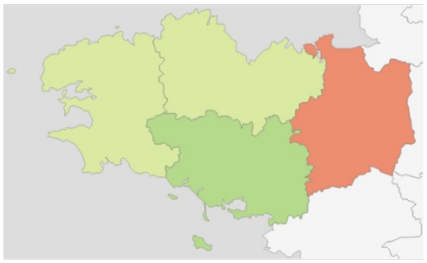


Finistère : 157 Offres
Côtes d'Armor : 56 Offres
Morbihan : 60 Offres
Ille-et Vilaine : 845 Offres

Source : https://grandeecolenumerique.fr/

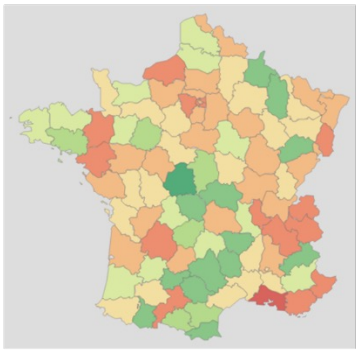
Les offres d'emploi sont elles aussi, principalement localisées en Ille-et-Vilaine (75 %) ainsi que dans le Finistère, dans une moindre mesure (15%).

L'indice de tension dans la Sécurité, cloud, réseaux et télécom



1 118 offres d'emploi dans le numérique prises en compte

Top 5 Metiers	Tension
Support technique	2.79
Télécoms	2.66
Système et réseaux	2.37
Cloud	1.83
Système d'information	1.49
Top 5 Postes	**Tension**
Ingenieur systèmes	1.19
Ingénieur Cloud computing	1.13
Conseiller support technique	0.97
Technicien helpdesk	0.94
Technicien en télécommunication	0.92
Expert Sécurité IT	0.19



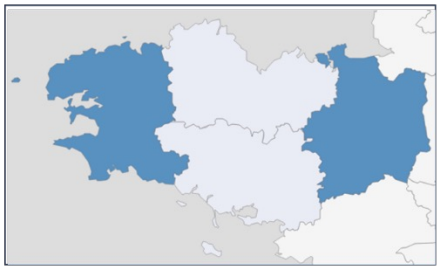
19 993 offres d'emploi dans le numérique prises en compte

Top 5 Metiers	Tension
Support technique	1.23
Système et réseaux	0.88
Télécoms	0.72
Cloud	0.16
Système d'information	-0.03
Top 5 Postes	**Tension**
Technicien helpdesk	1.73
Ingenieur systèmes	1.69
Conseiller support technique	1.46
Expert Sécurité IT	1.11
Ingénieur Cloud computing	0.90
Technicien en télécommunication	0.82

Finistère : - 0,03
Côtes d'Armor : - 0,49
Morbihan : : - 0,53
Ille-et Vilaine : 1,05

Source : https://grandeecolenumerique.fr/

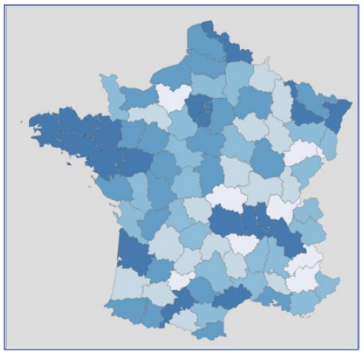
Formation de Cybersécurité



Finistère : 36 Formations
Côtes d'Armor : 30 Formations
Morbihan : 30 Formations
Ille-et Vilaine : 37 Formations

133 formations dans le numérique prises en compte

Top 5 Postes	Nombre
Analyste SOC	61
Analyste cybersécurité	54
Technicien cybersécurité	42
Pen testeur	21



1 078 formations dans le numérique prises en compte

Top 5 Postes	Nombre
Analyste SOC	496
Analyste cybersécurité	388
Pen testeur	268
Technicien cybersécurité	186

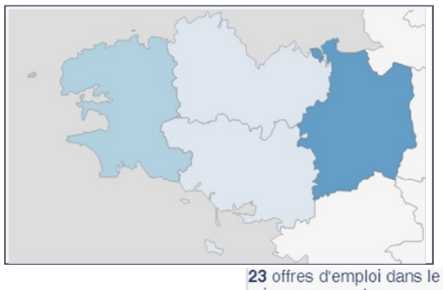
Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

L'Ille-et-Vilaine et la Région de Nantes sont en forte tension au niveau de l'emploi.

La vision Cyber de la Bretagne versus la France

L'offre de formation est principalement localisée en Ille-et-Vilaine ainsi que dans le Finistère, cela représente plus de 54 % des formations. Notons que les formations cyber sont riches dans l'Ouest de la France.

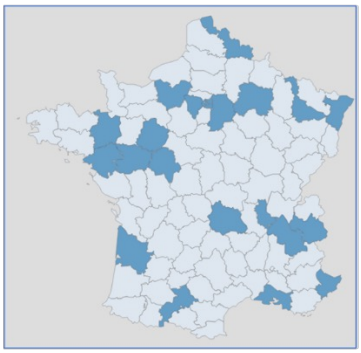
Les offres d'emploi de Cybersécurité



Finistère : 2 Offres
Côtes d'Armor : 0 Offres
Morbihan : 0 Offres
Ille-et Vilaine : 21 Offres

23 offres d'emploi dans le numérique prises en compte

Top 5 Postes	Nombre
Analyste cybersécurité	10
Analyste SOC	8
Technicien cybersécurité	5



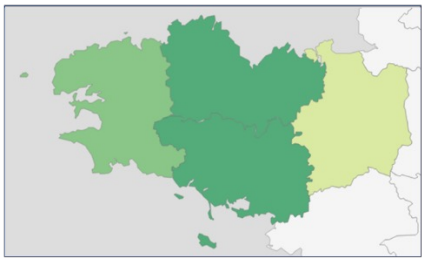
418 offres d'emploi dans le numérique prises en compte

Top 5 Postes	Nombre
Analyste SOC	204
Analyste cybersécurité	180
Technicien cybersécurité	40

Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

Les offres d'emploi ne sont pas représentatives de la dynamique de la filière cyber, cela étant dû au fait que la plupart des nombreuses embauches se font sur un marché caché, les services RH des entreprises et administrations qui recrutent font une chasse permanente aux bons profils. Cela provoque aussi un fort taux de *turn over* dans la filière et un souci de surenchère au niveau des salaires qui pose surtout des problèmes aux PME/PMI.

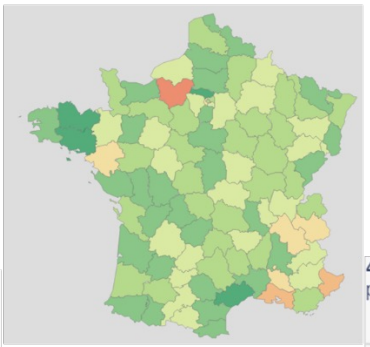
L'indice de tension dans la Cybersécurité



Finistère : - 1,7
Côtes d'Armor : - 2,32
Morbihan : : - 2,32
Ille-et Vilaine : - 0,37

23 offres d'emploi dans le numérique prises en compte

Top 5 Postes	Tension
Analyste cybersécurité	-1.09
Analyste SOC	-1.30
Technicien cybersécurité	-1.33



418 offres d'emploi dans le numérique prises en compte

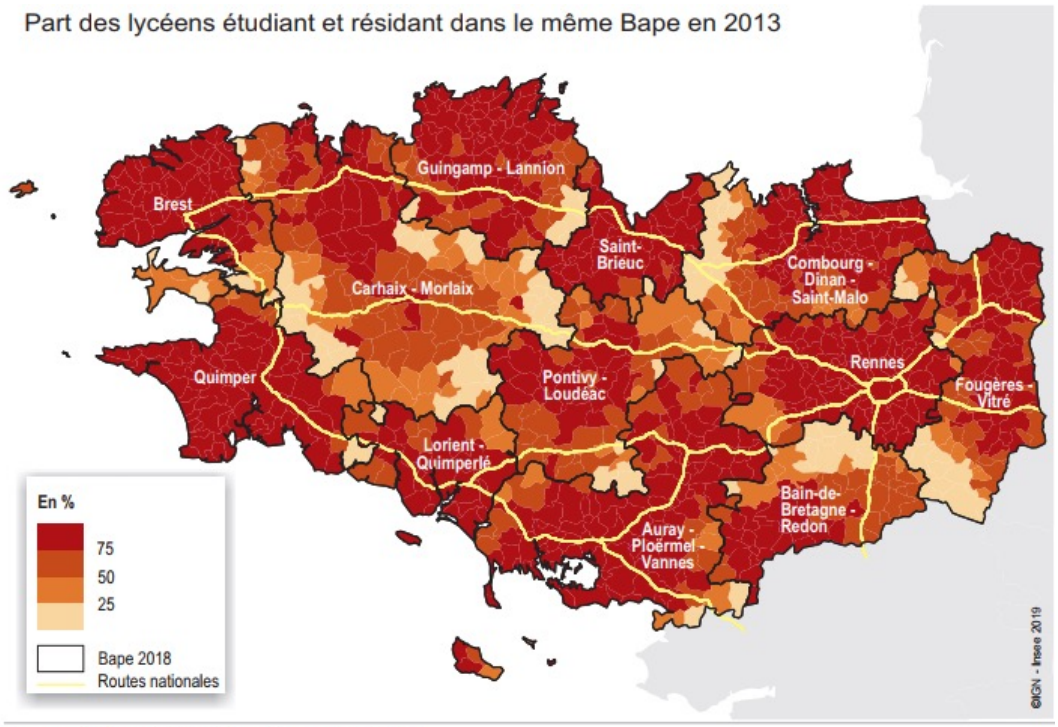
Top 5 Postes	Tension
Analyste cybersécurité	-0.52
Analyste SOC	-0.60
Technicien cybersécurité	-1.03

Source : https://www.grandeecolenumerique.fr/gen_scan/cartographie

De la formation en Bretagne à la vie professionnelle

Plus de 80 % des lycéens bretons résident et étudient dans le même BAPE (Bassin d'animation de la politique éducative), seules les zones très rurales les obligent à rechercher un établissement dans un autre bassin. Cela est encore plus vrai pour les trois BAPE de Rennes, Brest et Saint-Brieuc, où cette proportion dépasse les 90 %. Cela s'explique par des densités relativement élevées de population dans ces zones qui proposent donc aussi une offre d'enseignements plus importante.

Toutefois, plus l'étudiant monte en niveau d'étude et plus sa scolarité est brillante plus il aura tendance à être mobile, surtout au-delà du Bac+2/3.

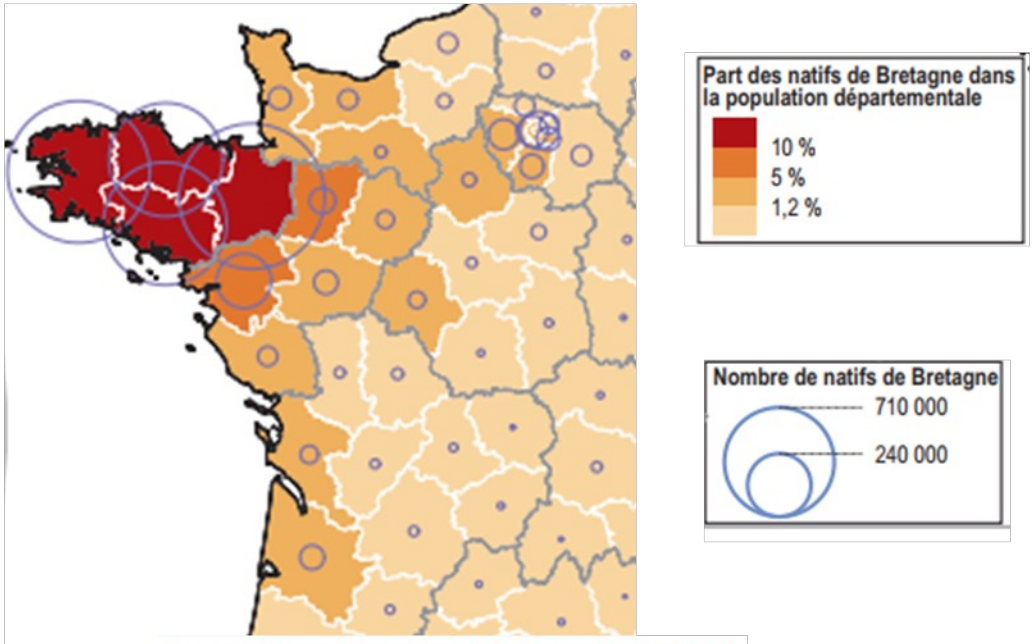


Source : Rectorat, DEPP, Base élèves au 31/12/2012.

Après le lycée : on reste dans l'Ouest

En 2016, un quart des personnes nées en Bretagne vivaient dans une autre région de France. Parmi ces 688 600 natifs de Bretagne, la moitié résidait en Île-de-France (186 600) et dans les Pays de la Loire (164 500).

Nombre de natifs de Bretagne dans les départements français (hors Mayotte) et part dans la population départementale

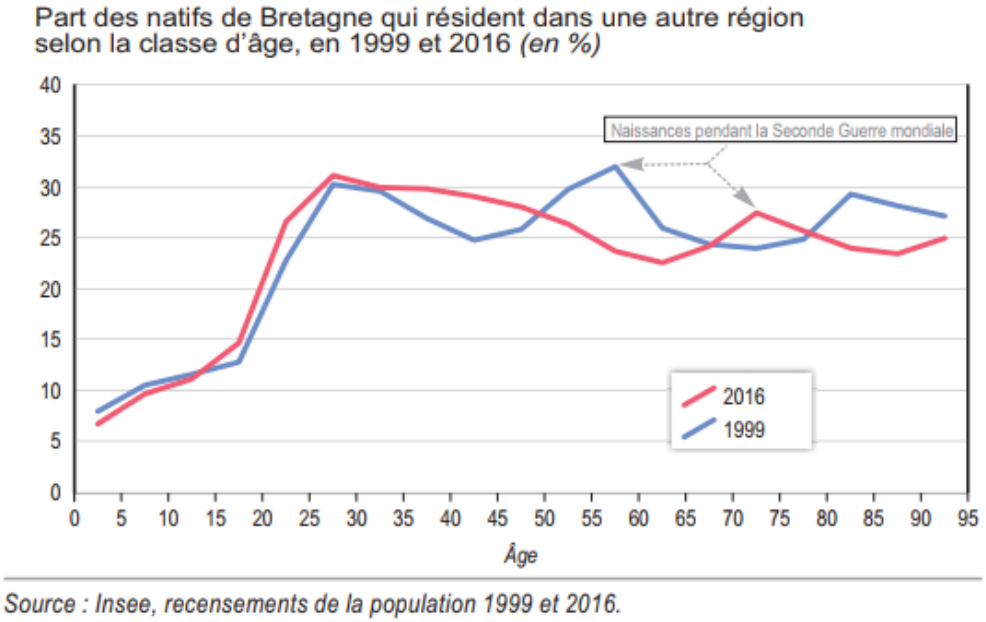


Source : Insee, recensement de la population 2016.

Les études supérieures ou la recherche d'un premier emploi motivent la plupart du temps un départ de sa Région natale. Cela est encore plus vrai pour les plus diplômés ou les travailleurs les plus qualifiés, qui migrent davantage. Toutefois, les Bretons privilégient le Grand-Ouest ou la région parisienne, et ceux qui sont partis reviendront pour la plupart un jour en Bretagne.

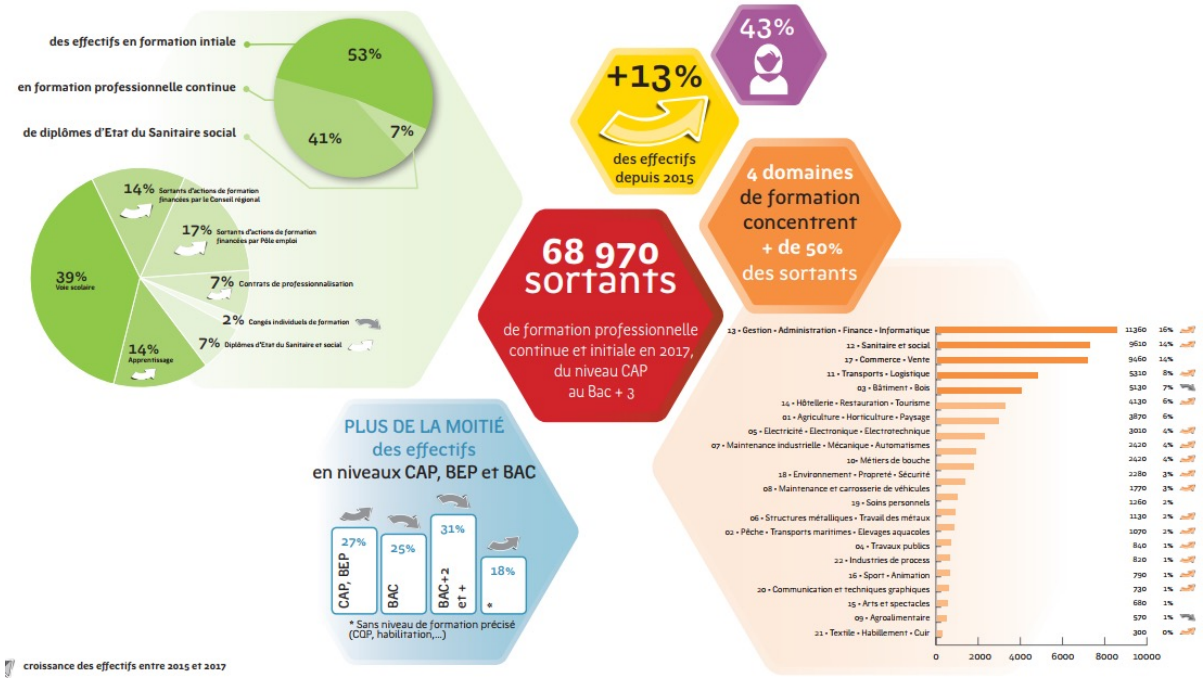
A 30 ans : toujours dans l'Ouest

Ainsi, à 30 ans, près d'un natif de Bretagne sur trois a quitté la région.



Source : Insee, recensements de la population 1999 et 2016.

Parmi les natifs de Bretagne, les plus diplômés et les plus qualifiés ont le plus souvent quitté la région : 40 % des Bretons de naissance diplômés du supérieur résident dans une autre région (contre un tiers au niveau national) ; ils occupent des emplois plus qualifiés que ceux qui sont restés en Bretagne.



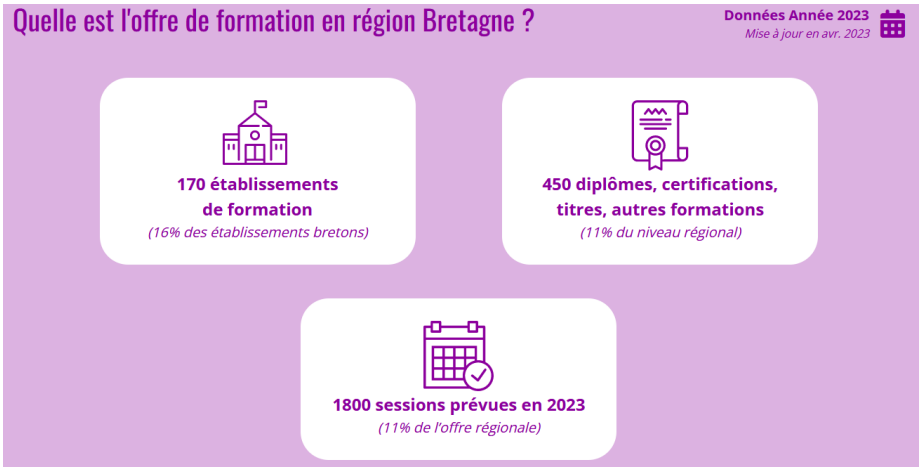
Source : GREF Bretagne

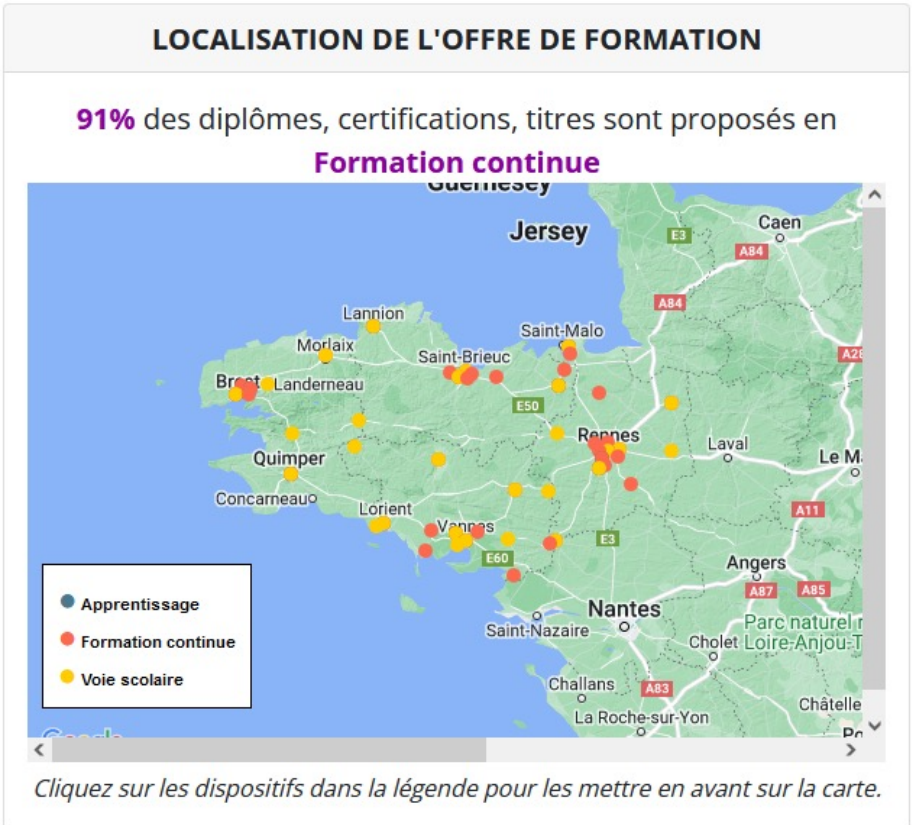
Dans les 4 domaines de formation qui concentrent 50 % des sortants, le premier et « Gestion, Administration, Finance, Informatique », qui représente à lui seul 16 % de la formation professionnelle, ainsi que le commerce et la vente de produits ou services, dont le domaine du numérique.

Notons enfin, qu'entre 2015 et 2017, une évolution de 34 % des sortants d'une formation « Gestion, Administration, Finance, Informatique », dont les BTS SIO très nombreux sur le territoire, ou les SN devenus CIEL, avec une forte proportion de formations continues professionnalisantes.

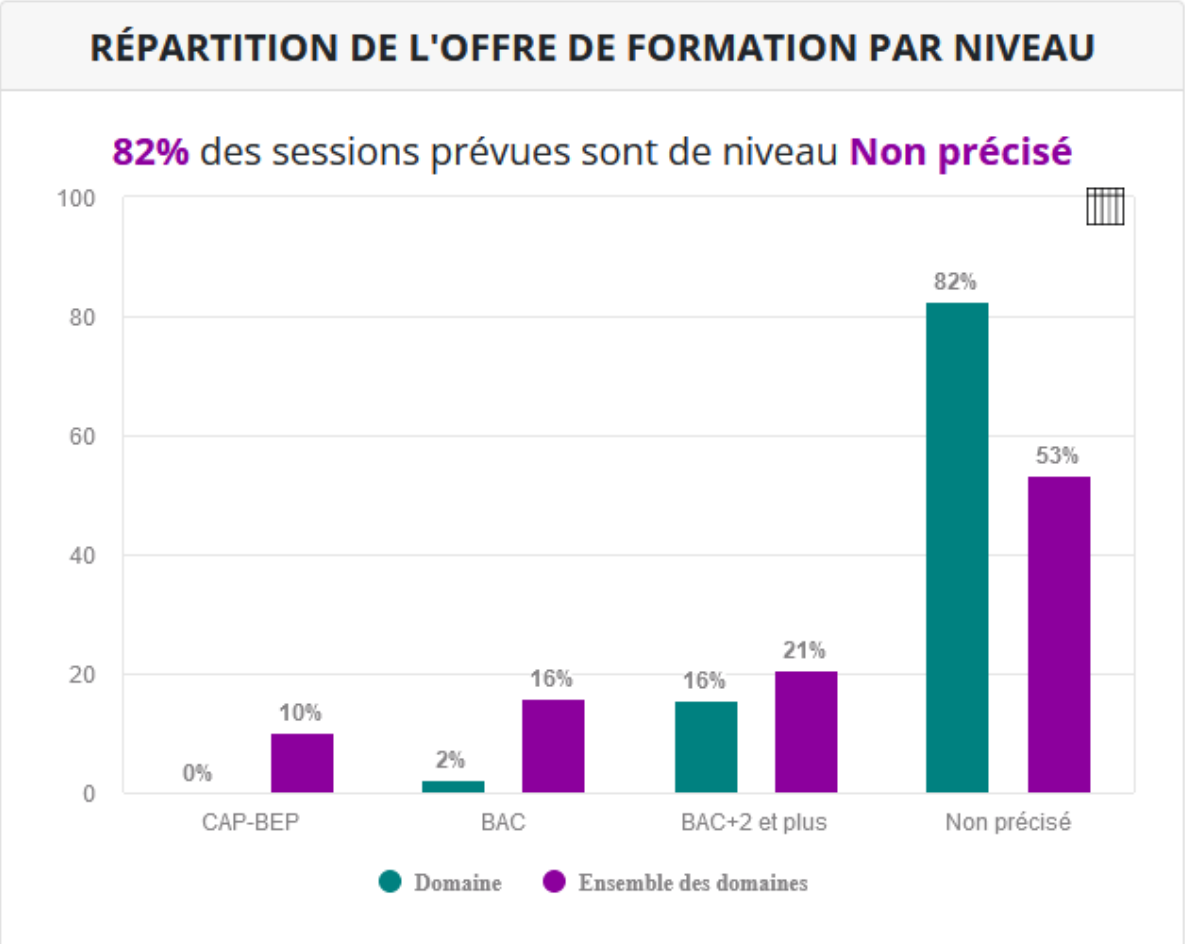
Une offre de formation bretonne riche.

La Bretagne est aussi un territoire renommé pour la qualité de ses Grandes Écoles et Universités qui forment des étudiants compétents dans de nombreux domaines. La base OFELI du Gref Bretagne et l'ONISEP nous proposent cette infographie pour 2023 : formations dans le secteur du numérique.





Offre de formation dans le domaine du numérique par niveau



https://focus-emploi-formation-bretagne.bzh/offre-de-formation/tous-dispositifs/13

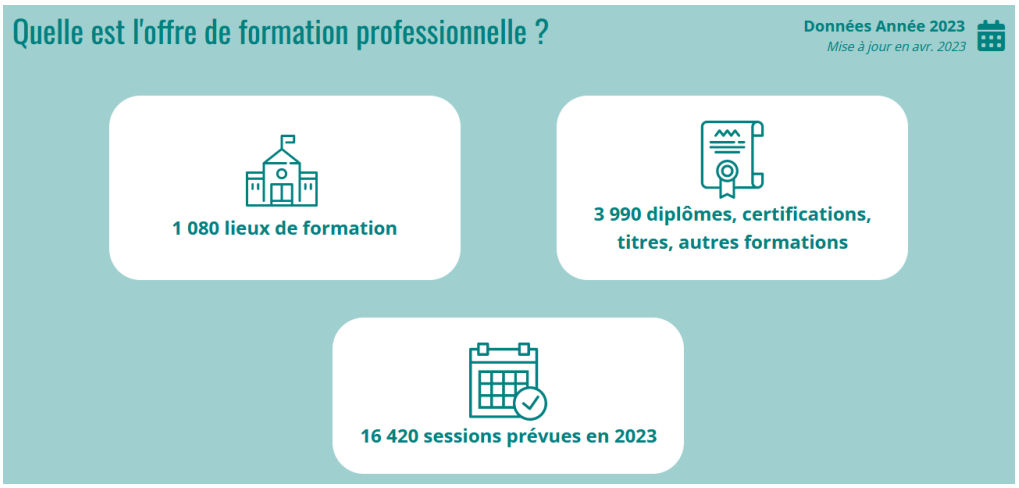
Le numérique demande souvent un niveau de formation supérieur au BAC, a minima BAC+2/3 (deux tiers des étudiants bretons du numérique sortent des diplômes de BTS[1] ou de Licence pro), et 84% des diplômes proposés sur le territoire sont de ce niveau. Notons qu'avec la mise en place du référentiel Licence/Master/Doctorat (L/M/D) au niveau européen, nombreux sont les étudiants à Bac+2 des BTS et IUT[2] qui souhaitent continuer jusqu'à la licence au moins, surtout dans les IUT. L'administration réseaux et systèmes, le développement et les métiers du Web sont les principaux choix des étudiants, l'intelligence artificielle et la gestion des données sont des domaines en forte émergence.

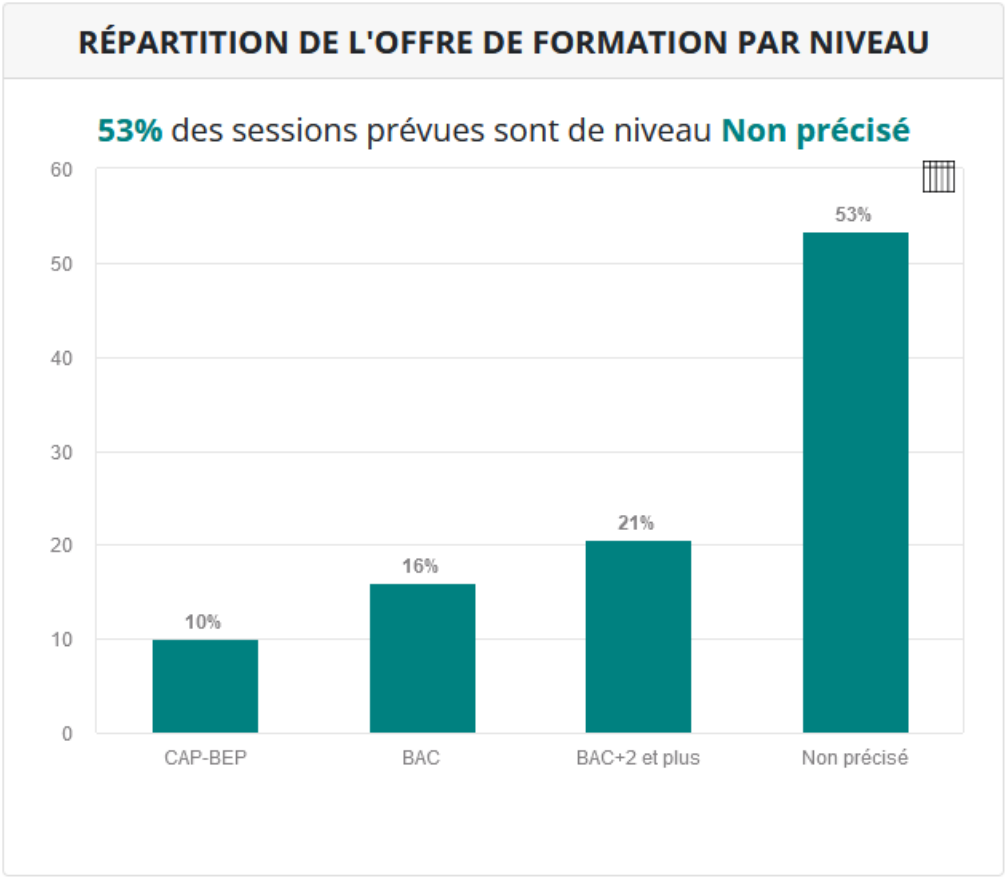
Il existe une forte demande de diplômes spécialisés de premier niveau vers des domaines comme le développement Web, le design, et l'administration réseau. De nouvelles écoles, telle l'école 42, Simplon, et d'autres, se sont ouvertes sur ce modèle proche des certifications métiers. Cette manne pour ces écoles est importante, car 47% des apprenants en Bretagne entrent dans les métiers du numérique par la formation continue, contre 38% par la voie scolaire et 15% par apprentissage, filière qui ne cesse d'augmenter depuis 2020. Une fois formé aux bases d'un métier, l'étudiant est mis en immersion dans l'entreprise pour consolider ses savoir-faire.

Toutefois, certaines formations trop courtes ou trop ambitieuses au regard des prérequis nécessaires affichent malheureusement un fort taux d'échec. Le terme de « non précisé » dans le schéma signifie qu'il s'agit de sans niveau reconnu par un référentiel (RNCP[3] , éducation Nationale, etc.).

1 Brevet de technicien supérieur.
2 Institut universitaire de technologie.
3 Répertoire national des certifications professionnelles.

Offre de formation professionnelle globale par niveau

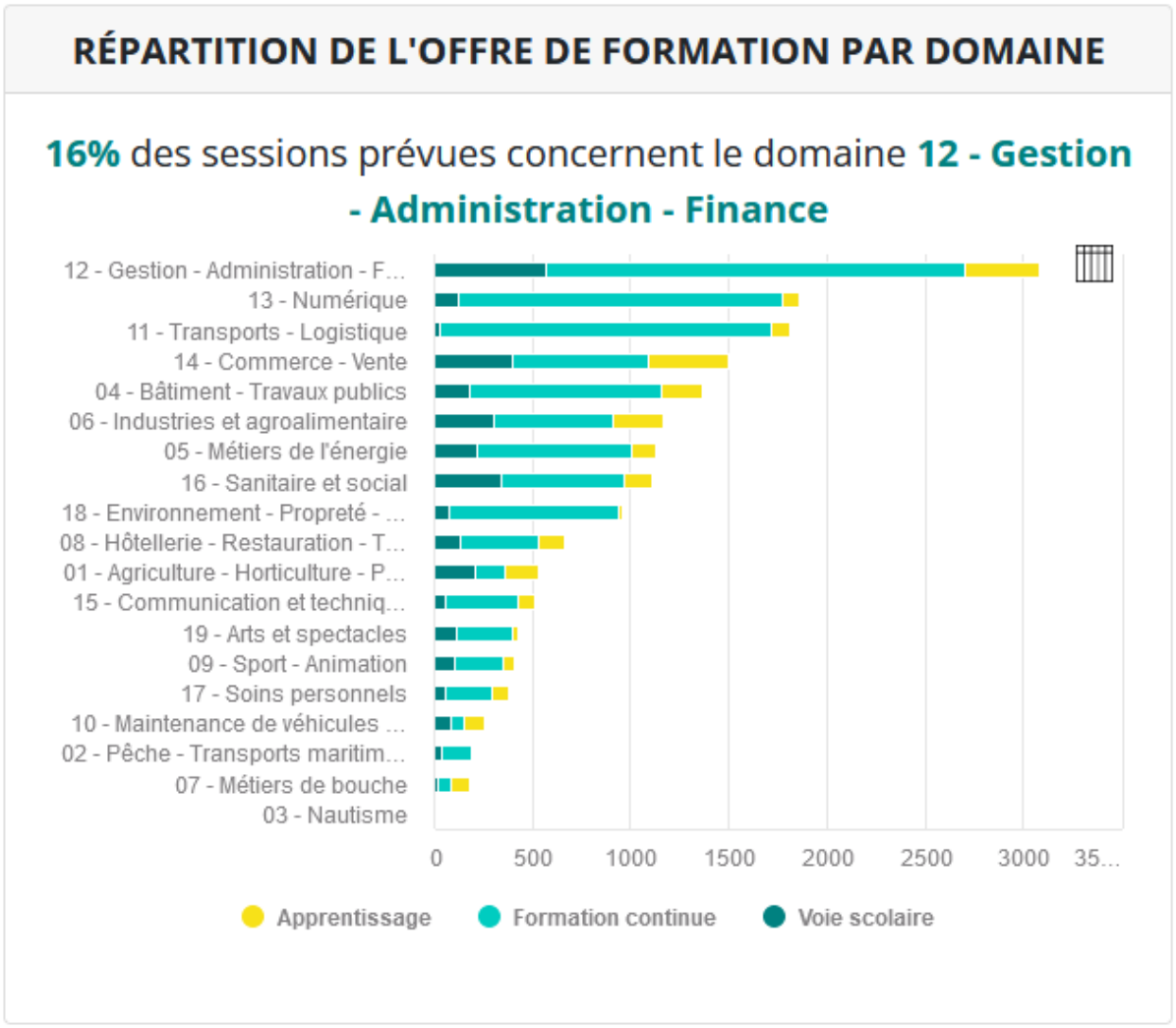




Ce schéma nous montre que les jeunes et moins jeunes recherchent tout de même un diplôme, un niveau reconnu au RNCP ou par l'éducation Nationale. Le numérique arrive en seconde place tous domaines confondus, domaine qui se prête aussi bien à des études en distanciel et à l'autoformation. La voie scolaire pourrait être encore développée, elle donne de bons résultats, mais l'engagement financier pour des études dites longues est parfois compliqué pour des gens qui raisonnent année par année et qui optent alors parfois pour l'apprentissage où le taux d'insertion est aussi meilleur en sortie.

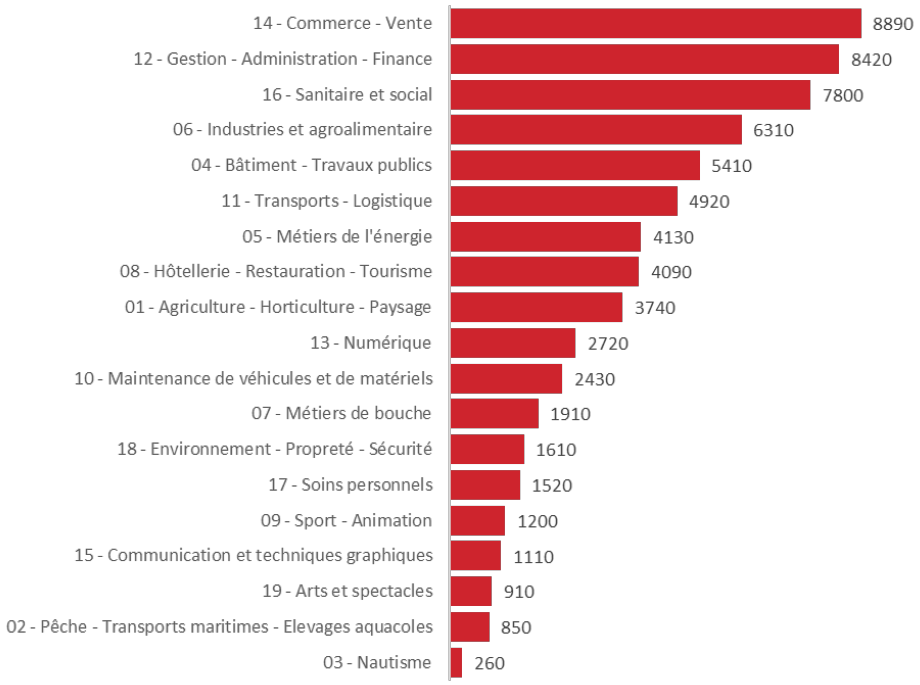
Se projeter sur des études longues lorsque l'on reprend un cursus venant d'un autre métier n'est pas chose aisée. Un accompagnement fort des structures d'accueil doit être privilégié. Les femmes bretonnes sont attirées par le numérique, avec une croissance de 46% contre 23% tous domaines confondus, une croissance qui reste en deçà de celle de leurs homologues masculins.

Il serait bon d'avoir un observatoire qui analyse les besoins en emploi des différents BAPE bretons, hors des grandes métropoles où les offres sont plus nombreuses, cela pour y proposer des modules de formations jusqu'au Bac+3 qui correspondent effectivement aux besoins du territoire. Enfin, toute formation aux métiers du numérique devrait comporter les notions de cybersécurité associées aux compétences en sortie, et cela est d'autant plus vrai pour des métiers comme le *Web* ou la communication numérique qui sont les cibles d'attaques simples et nombreuses.



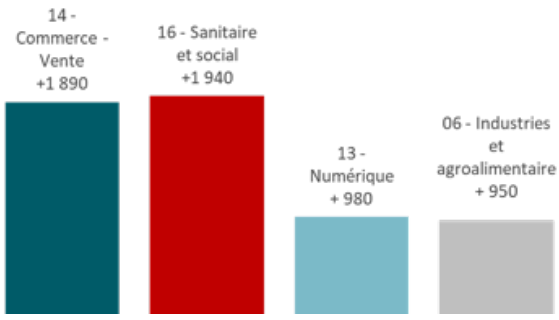
https://focus-emploi-formation-bretagne.bzh/formation/offre-de-formation/tous-dispositifs/region/53

« Note de lecture : La session de formation correspond à une classe ou une action de formation sur un site et pour une date définie. La notion de lieux de formation comprend les sites de formation liés aux établissements scolaires, organismes de formation professionnelle continue et/ou par apprentissage. Les données concernent l'offre de formation professionnelle, prévisionnelle, déclarée par les établissements pour la formation initiale (source : ONISEP), la formation continue et l'apprentissage (Source : Base OFELI – GREF Bretagne). Ces sessions doivent débuter dans l'année en cours. »



Source : Base OFELI du GREF Bretagne, ONISEP.

54% des sortants 2021 hors CPF sont concentrés sur les 5 premiers domaines de formation, le numérique n'arrivant qu'en 10ième position.



Source : Base OFELI du GREF Bretagne, ONISEP.

Le numérique fait partie des plus fortes croissances pour l'entrée en formation, et l'apprentissage est l'un des facteur porteur dans cette filière.

Offre de formation professionnelle globale par niveau : GRETA/AFPA

Métiers du Numérique– Réseau des GRETA-CFA de Bretagne

Chaque année, ce sont plus de 400 personnes formées aux métiers du Numérique dans les GRETA-CFA Bretons.

Nos équipes accompagnent les publics :

Sur la connaissance de la filière et des métiers numérique :
- Réalisation de modules de découverte de 2 jours aux métiers du numérique ;
- Mise en œuvre d'action de préqualificaion aux métiers du numérique à St Malo, Redon, Lannion et Loudéac ;
- Actions de communication ciblées sur l'ensemble du territoire (Safari du Numérique ADN Ouest, semaine du numérique à Pole Emploi, Femmes et Numérique à Quimper, Estim Numérique, Dispositif wi filles / FACE, action girls & coding dans les collèges…). Le réseau des GRETA-CFA a notamment développé un espace game permettant de valoriser l'attractivité de la filière, utilisé régulièrement sur les salons, portes ouvertes il permet de favoriser les parcours d'accès à la qualification et de reconversion.

Sur la montée en compétence et la qualification au travers la mise en œuvre de formations certifiantes :

- BTS Services informatiques aux organisations (niveau 5), Option SLAM à St Malo, St Brieuc, Vannes, Quimper et option SISR à Morlaix ;
- Titre Technicien d'Assistance Informatique (niveau 4) sur Fougères et Morlaix ;
- Titre Concepteur Designer UI (niveau 6) à Rennes, Vannes et Brest ;
- Titre Concepteur développeur d'application (niveau 6) et Développeur web full stack (formation labellisée Grande Ecole du Numérique) à Vannes.

En 2023/2024 afin de répondre aux forts besoins de compétences cyber en Bretagne, notamment sur le niveau technicien, le réseau des GRETA-CFA va mettre en œuvre une nouvelle formation en partenariat avec le Ministère des Armées et financée par la Région Bretagne : technicien veilleur de cyber sécurité (niveau 5) en partenariat avec le Ministère des Armées à Rennes, Vannes, Lannion et Morlaix

Notre réseau, partenaire également du projet CMA CyberSkills4All va accompagner la montée en compétences des équipes et des publics sur la cybersécurité et les usages sécurisés : coloration des formations existantes, modules dédiés transversaux ou techniques, accompagnement des enseignants et formateurs, création de ressources et de référentiels de certification…

Adresse site internet Réseau des GRETA-CFA : https://greta-bretagne.ac-rennes.fr/portail/web

Contacts :
- GRETA-CFA Est-Bretagne
02 99 22 63 64
greta.agrennes@ac-rennes.fr
- GRETA-CFA Bretagne Sud
02 97 87 15 60
greta.aglorient@ac-rennes.fr
- GRETA-CFA de Bretagne Occidentale
02 98 90 15 18
greta.agquimper@ac-rennes.fr
- GRETA-CFA des Côtes d'Armor
02 96 61 48 54
greta.cotesarmor@ac-rennes.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RÉSEAU greta
GRETA-CFA BRETAGNE

La CyberSchool de Rennes

L'école Universitaire de recherche en cybersécurité, la Cyber School de Rennes, rassemble 19 formations universitaires et des formations d'ingénieurs et grandes écoles en cybersécurité dispensées par un consortium de 10 établissements bretons. Ces formations forment des spécialistes, ingénieurs et scientifiques dans les domaines clés de la cybersécurité. Cela va du BUT et master, en passant par des formations d'ingénieurs et des grandes écoles, accessibles à partir du baccalauréat jusqu'à bac+6. La Cyber School lancera dès la rentrée 2023, un parcours doctoral qui permettra aux doctorants en cybersécurité d'enrichir leur expérience de thèse en donnant accès à un éventail d'activités de soutien scientifique, de formation et de développement de réseau professionnel dans le domaine de la cybersécurité.. Rennes Métropole finance l'école dont le Pôle est l'un des partenaires.

L'ÉVOLUTION DES BESOINS

Les besoins ne cessent de croitre, et les nouvelles normes & contraintes réglementaires, la montée en puissance des administrations (ANSSI, ministère des Armées, de l'Intérieur, les centres d'alerte et de réaction aux attaques informatiques (*CSIRT*) Régionaux financés pour partie par l'ANSSI, etc.) et des entreprises vient encore accroitre les besoins en personnels qualifiés, techniciens, ingénieurs et gestionnaires de projets.

Les opportunités d'emploi ont augmentées depuis la dernière étude entre 1,5 et 2,5 en fonction des familles de métier :

- Compris entre 2 et 2,5 : Gestion des incidents, audit et expertise et Marketing commercial ;
- Compris entre 1,5 et 2 : *Build & run*, GRC, Généraliste.

Les dirigeants prennent de plus en plus conscience de la nécessité de se protéger des potentielles attaques et bugs qu'ils pourraient subir, ils mettent en place des stratégies de défense ; la question qu'ils se posent n'est plus « qui va être attaqué ? » mais « quand va-t-on être attaqué ? », et cela devient une réalité, quelques soient les activités ou la taille de l'organisation.

2013-2022 pénurie de ressources et des salaires qui flambent

Le manque de RH dans certains métiers de la cyber (architecte, RSSI, consultant, gestionnaire de crise, etc.) a provoqué une inflation des salaires à l'initiative des Grands Groupes et des grandes société multinationales (GAFAM en tête), et, au regard de l'UE, cela fut surtout vrai en France, avec des rétributions deux fois plus importantes que dans les autres pays de l'OCDE, mais bien inférieures à ce qui est pratiqué dans les pays anglo-saxons dans lesquels de nombreuses ressources de haut niveau se sont exilés.

Un autre phénomène est l'impact qu'a la validation d'une formation diplômante sur la carrière. En effet, une personne qui se fait financer un titre universitaire ou un diplôme d'ingénieur par son entreprise, ou valide une valorisation des acquis de l'expérience (VAE) change souvent à la suite de structure rapidement, une fois le diplôme obtenu, faisant à cette occasion un bond conséquent quant au salaire.

Cette valorisation des salaires dans le secteur privé attire non seulement les ressources humaines évoluant dans la cyber issues du secteur public, mais freine aussi le secteur public dans ses recrutement, celui-ci ne pouvant rivaliser avec les niveaux de salaires proposés. Cela empêche les organisations de capitaliser sur des équipes pérennes et peut aller jusqu'à les mettre en péril. Cela favorise aussi la mobilité des ressources qui provoque des déséquilibres d'une région à l'autre, car l'enfermement dans les grosses métropoles durant la période Covid19 a motivé nombre de personnes à s'installer dans les régions de la côté Atlantique et en PACA, y compris pour ceux qui ont gardé leur poste dans la grande ville (surtout Paris).

Ainsi, pour garder la ressource cyber certaines administrations centrales ont parfois pu réhausser les salaires grâce à la circulaire Cazeneuve, certains départements ont aussi réussi à offrir des primes à leurs salariés, mais ce n'est jusqu'ici pas le cas des Régions. De plus, les entreprises du privé proposent de nombreux aménagements, tout comme certaines entreprises anglo-saxonnes qui autorisent le full télétravail en portage salarial à des salaires très élevés.

Grâce à la dynamique du territoire Breton depuis la création du Pôle d'excellence cyber, la plupart des Grandes Entreprises et des services de l'état ont conduit une décentralisation de leurs organisations sur des territoires métropolitains, tel que Rennes Métropole ou Brest Métropole, pour séduire ces gens qui fuyaient les grandes agglomérations. Les Grands Groupes, tels Airbus, Thales, Sopra-Steria, Capgemini, ont ainsi consolidé leur présence sur le territoire, proposant de surcroit des salaires intéressant. Cela augmente aussi la tension en termes de recrutement RH pour les PME/PMI et administrations. Nul doute que ces organisations, qui ont su investir de nouveaux territoires qui correspondent mieux aux attentes de vie de salariés exigeants, renforceront ainsi leur lien avec l'organisation et seront donc gagnants sur le long terme.

Évolution entre l'étude 2017 et celle de 2023 - Tableau comparatif

Le classement des régions en fonction des annonces de l'Agence Pour l'Emploi des Cadres	
2017 : Île-de-France, Bretagne.	2023 : Île-de-France, Auvergne Rhône Alpes, Occitanie, PACA, Bretagne.
Les établissements de formations cyber en Bretagne	
2017 : 10 + les filières STI2D. Pour ce qui est des certifications, elles sont majoritairement états-uniennes et leur coût est élevé. Des *MOOC*[1] commencent à apparaître.	2023 : 15 + les filières SN, SIO et CIEL. Des certifications sont faites au sein des cursus bretons, le Pôle a pour projet de mettre en place un GT certification pour en construire et les porter à l'Europe.
Les entreprises Cyber en Bretagne (sécurisants)	
2017 : 130.	2023 : 160 dont les start ups de la *CyberFactory*, *CyberBooster* ou du *Startup Studio*.
Répondre à la pénurie et fidéliser les personnels	
2017 : couvrir les besoins de la Loi de Programmation Militaire (LPM), et faire en sorte que les étudiants se dirigent vers la filière cyber dès le BAC+2, hormis certaines écoles (ENSIBS[2], EPITA[3], ESIEA[4]) la spécialité se fait généralement au dernier semestre du cursus ingénieur ou par le biais de Mastère spécialisés (accréditées par la CGE[5]).	2023 : former tous les utilisateurs, miser sur les compétences internes de l'administration ou de l'entreprise et la motivation pour éviter le turn over, enseigner les bonnes pratiques et les notions de cybersécurité dès la 3ème et jusqu'au BAC, consolider les parcours de technicien cyber dès le BAC.
Profils recherchés (sécurisants et sécurisés)	
2017 : former les informaticiens à BAC+5 pour assurer les Grands Groupes et Opérateurs d'Importance Vitale (LPM). Besoin de techniciens *SIEM*[6], *SOC*[7], *CSIRT*[8], d'architectes et de gestionnaires de crises. Le commandement de la cyberdéfense (COMCYBER[9]) est créé le 1er janvier.	2023 : former des techniciens aux principaux outils cyber du marché, besoin de spécialisation, des techniciens et ingénieurs possédant des *soft skills* et des gens souhaitant s'investir dans la durée. Les consultants spécialisés dans la vente de produits et services de sécurité, les spécialistes en développement sécurisé (*DevSecOps*[10]), de plan de continuité d'activité (PCA) ou de retour d'activité (PRA) sont très demandés, les analystes (*CTI*[11]) et les *DPO*[12] sont des profils très recherchés, public et privé manquant de personnels techniques.
Cible de la menace	
2017 : les attaques se concentrent sur les grands acteurs, les Grands Groupes, les administrations centrales, les OIV	2023 : vers tous les acteurs, elle est organisationnelle, réglementaire, environnementale, informatique et humaine, visant surtout les PME/PMI, les sous traitants & les individus. Le périmètre de la Loi *European Network and Information System Security NISv2*) s'élargit aux Opérateur de Services Essentiels (OSE), collectivités. La taille critique n'est plus un critère pour se doter de ressources cyber, les ingérences étrangères sont

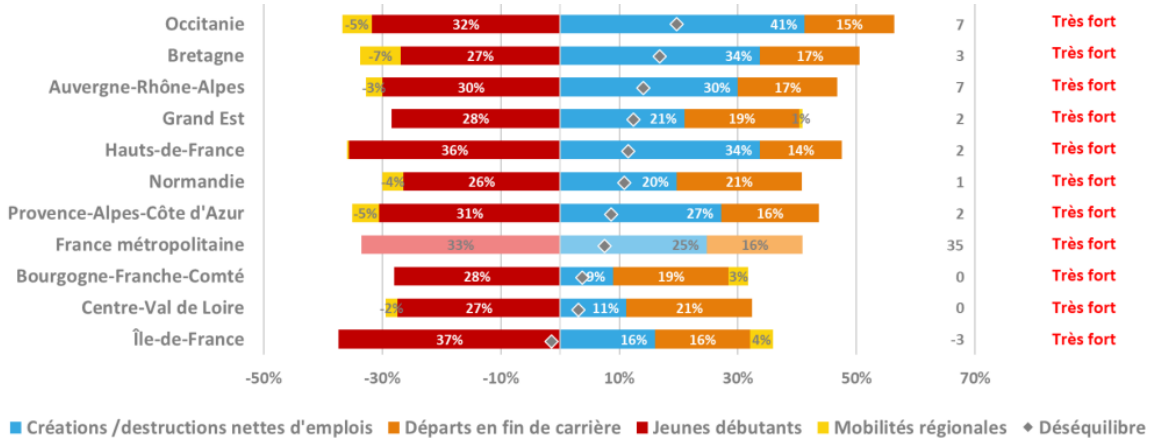
1 *Massive open online course*, cours en ligne généralement gratuit donnant lieu à un certification d'école généralement ou de l'ANSSI.
2 École nationale supérieure d'ingénieurs de Bretagne Sud. École pour l'informatique et les techniques avancées.
3 École supérieure d'informatique électronique automatique.
4 Conférence des Grandes Écoles.
5 Gestion des évènements de sécurité du système d'information ou *Security Information Event Management (SIEM).*
6 Centre des Opérations de Sécurité, *Security operations center* en anglais.
7 Centre d'alerte et de réaction aux attaques informatiques, *Computer Security Incident Response Team (CSIRT)* ou *Computer Emergency 8 Response Team (CERT)* en anglais.
9 Placé sous l'autorité directe du chef d'état-major des armées, le COMCYBER est un commandement opérationnel qui rassemble l'ensemble des forces de cyberdéfense du ministère des Armées sous une autorité interarmées.
10 *Development, Security, Operations* approche qui désigne à la fois le développement, la sécurité et l'exploitation, et qui permet d'intégrer la sécurité des données dès le début d'un projet.
11 *Cyber Threat Intelligence*, la collecte d'informations sur les menaces ou les acteurs de la menace.
12 Délégué à la protection des données (DPD), *pour Data Protection Officer.*

(on passe de l'*IT*[13] vers l'*OT*[14]) la BITD[15], les technologies innovantes, et les médias. Elles reflètent les capacités techniques des grands pays cyber (USA/Israël, Chine, Russie) qui se font une guerre économique & d'influence.	permanentes & multiformes, la cyber devient guerrière, utilise les objets connectés (téléphones, drones, véhicules, etc.) et l'IA (reconnaissance faciale, *OSINT*[16], CTI), sous fond de guerre aux portes de l'Europe.
Mutualisation des forces	
2017 : les acteurs malveillants sont spécialisés par secteur, les attaques sont ciblées et souvent unitaires, le *Deep Web*[17] se structure, les *hackers* sont des stars, les défenseurs sont rares et trop peu nombreux, les pare-feux ne suffisent plus, des sondes sont développées, le travail de détection en temps réel est nécessaire (les *SOC* se développent), les *CISRT* deviennent essentiels, les universitaires, entreprises cyber et les Armées collaborent à l'effort de défense.	2023 : les acteurs malveillants touchent tous les secteurs de l'économie, les attaques sont plus complexes et souvent dissimulées derrière les premières actions détectées, de nombreuses données volées sont vendues sur le *Deep Web*, les attaquants ne se refusent aucune cible (hôpitaux, appareils médicaux, stimulateurs cardiaques, etc.), les défenseurs doivent unir leurs forces pour faire face à la menace toujours croissante, la puissance des machines (*HPC*[18]) qui travaillent jour et nuit, permet l'avènement d'intelligences artificielles (IA) et l'utilisation des algorithmes d'apprentissage automatique (*Machine Learning*) qui tentent de remplacer le raisonnement et les comportements humains, États et scientifiques souhaitent garder le contrôle de ces innovations.
Évolution des mentalités	
2017 : les victimes (les sécurisés) se « défendent » souvent seules contre les attaques, parfois sans autre alternative que de payer des rançons (si pas de sauvegarde, ni de PCA/PRA), les dirigeants continuent de penser que ce n'arrive qu'aux autres.	2023 : les organisations s'unissent pour se défendre, mutualisent les moyens techniques et humains et s'équipent en outils de prévention, d'analyse et de défense. Les dirigeants savent qu'ils seront attaqués. Volonté de créer une filière cyber souveraine européenne.
Définition des fonctions recherchées dans la filière	
2017 : 4 fonctions, conception, administration, recherche, conseil.	2023 : 6 fonctions, gestion de la relation client, *Build* & *Run*[19], gestion et réponse à incidents, audit et expertise, ingénierie généraliste en cybersécurité, commercial et marketing.

13 *Internet Technology*.
14 *Operational Technology*, la technologie d'exploitation qui comprend les systèmes de contrôle/commande industriels ou *Industrial Control Systems (ICS)*, les Automates Programmable Industriels (API) ou *Programmable Logic Controller (PLC)*, les Contrôles dynamique de la puissance ou *Dynamic Power Control (DPC)* & les systèmes de contrôle et d'acquisition de données en temps réel ou *Supervisory Control And Data Acquisition (SCADA)*.
15 Base Industrielle et Technologique de Défense, l'ensemble des industries nationales d'un pays prenant part aux activités de défense, l'industrie de défense ou l'industrie de souveraineté.
16 Renseignement de sources ouvertes ou renseignement d'origine sources ouvertes (ROSO), pour *Open Source Intelligence*, obtenu par une source d'information publique.
17 Le *Deep Web* est l'Internet qui n'est pas indexé par les moteurs de recherche (sites payants, protégés par un mot de passe, messagerie électronique, etc.). Le *Dark Web*, fait partie du *Deep Web*, mais utilise le chiffrement pour renforcer sa sécurité.
18 *High performance computing* pour calcul haute performance ou calculs intensifs, les superordinateurs dont l'ordinateur quantique.
19 Concept défini par les méthodes agiles & l'amélioration continue, la Production, le Build, définit des fonctionnements en mode projet pour proposer de nouvelles solutions, et l'Exploitation, le Run, les pratiques de productions qui visent à délivrer un bien ou service de qualité.

L'ÉVOLUTION VERS 2030

Le déséquilibre en pourcentage pour les ingénieurs en informatique dans chaque région (2019-2030) et leur niveau de tension en 2019.

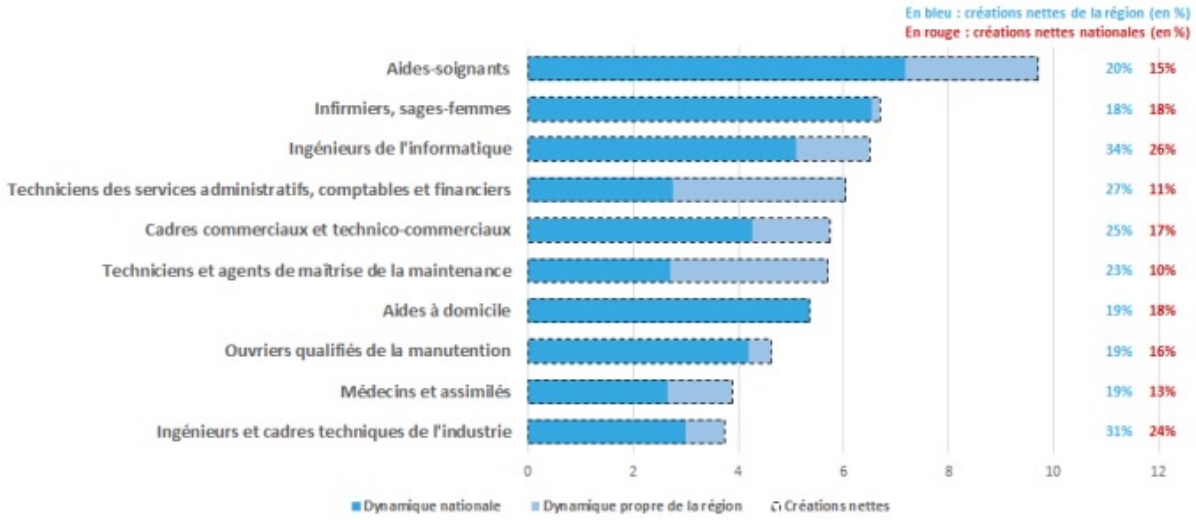


Sources : projections France Stratégie/Dares

La Bretagne est confrontée à la concurrence des autres régions de l'arc Atlantique, elle doit donc se démarquer pour rivaliser avec ces autres endroits attractifs. Le Pôle d'excellence cyber a attiré nombre d'entreprises de la base industrielle et technologique de défense (BITD) mais aussi celles utilisatrices de la cyber (telles EDF, La Poste, Orange, etc.) Nombreux sont les ingénieurs et techniciens qualifiés qui sont venus s'installer sur le territoire Breton, aussi des enseignants et chercheurs au sein des laboratoires. Le Groupement cyber des Armées (GCA) à lui seul va recruter 1000 personnes ces 5 prochaines années, il est venu accélérer encore cette dynamique qui avait été initiée. Aussi, d'autres services du ministère des Armées et de l'État ont décidé de renforcer leur présence en Bretagne : c'est par exemple le cas du ministère de l'Intérieur et de l'ANSSI.

Le Pôle d'excellence cyber a aussi créé l'*European Cyber Week*, l'un des trois grands évènements français aujourd'hui, seul évènement cyber souverain européen, dédié aussi bien à la formation (initiale et continue, avec un grand forum recrutement et une agora sur les orientations en terme de formation dès les collèges et lycées), à la recherche (avec une majorité de conférences scientifiques sur la cybersécurité et les domaines connexes : intelligence artificielle, ordinateur quantique, cryptographie, etc.) qu'à l'innovation et au développement industriel et économique, au profit des pure players mais aussi des utilisateurs. Le Pôle d'excellence cyber a été créé dans une logique de décloisonnement des silos universitaires & industriels d'une part et administratifs & militaires d'autre part. La dualité civilo-militaire du Pôle en fait un creuset riche d'idées et de pratiques nouvelles qui pousse nombre de recruteurs à innover. Le Pôle participe aussi à la formation des jeunes et moins jeunes par l'organisation de challenges, la construction de parcours pour les enseignants du Rectorat ou pour les étudiants post Bac.

Décomposition de la création nette pour les dix métiers les plus créateurs d'emplois en Bretagne entre 2019 et 2030 (en milliers)



Source : projections France Stratégie/Dares

Le vivier de la cybersécurité est alimenté principalement par les ingénieurs de l'informatique, qui arrivent tout de suite derrière les aides-soignants, infirmiers et sage-femmes sur ce schéma, des métiers aussi en grande tension, surtout après la période Covid19. L'informatique est entrée dans tous les domaines métiers, et surtout au sein des chaines industrielles (on parle d'OT^1), car la robotique et les systèmes industriels de contrôle/commande se sont généralisés au sein des entreprises, faisant à fortiori évoluer fortement les métiers. Le besoin en techniciens de maintenance informatique augmente aussi, pour le maintien en condition opérationnelle ou de sécurité, ainsi que pour l'analyse des logs produits par les matériels et logiciels, des métadonnées, des évènements.

PLAN D'ACTION

Une filière scientifique et technique fragilisée

La pénurie d'enseignants de mathématiques dans l'Éducation Nationale, la baisse année après année du niveau en mathématiques dans les différents cursus, jusqu'à proposer de faire de cette matière essentielle à la structuration des esprits une discipline optionnelle, tout cela n'aura certes pas motivé les élèves des collèges et lycées à faire des études scientifiques et techniques. La forte réduction du volume de candidats potentiels aux métiers de la cybersécurité, et en particulier des filles, doit accélérer la dynamique de partenariat entre le Pôle d'excellence cyber et le Rectorat de Rennes quant à former les enseignants volontaires à la cybersécurité grâce au M@gistère créé. L'association CyberEdu, qui propose en ligne aussi des supports pédagogiques divers aux enseignants des filières post BAC, doit programmer des colloques sur tout le territoire français pour expliciter la méthode pédagogique à des enseignants d'informatique de plus en plus volontaires : tisser les notions de cybersécurité au sein de leurs cours existants.

Les formations scientifiques peinent aujourd'hui à former un nombre d'élèves suffisant pour permettre aux différents secteurs d'activités de recruter des ressources spécialisées.

La ressource étant déjà limitée actuellement, une réponse à cette nouvelle norme doit être apporté rapidement et plusieurs vagues pour y pallier : Enseigner / Former.

Actions à court terme :

- **Former des enseignants dans les différents domaines de la cybersécurité :** le Pôle d'excellence cyber a créé dès 2017 le Parcours d'excellence cyber en STI2D/SIO avec le Rectorat de Rennes, de nombreux enseignants volontaires ont alors été formés et un M@gsitère avait été produit. Cette initiative est en cours de réamorçage avec la rénovation de la filière systèmes numériques transformée en BTS Cybersécurité, Informatique et réseaux, Électronique (CIEL) sous l'impulsion de Monsieur le Recteur et de l'Inspecteur d'Académie (IA) & Inspecteur Pédagogique Régional (IPR) pour les Sciences et Techniques Industrielles, Dominique PRIGENT. Il y a aussi un fort besoin de professeurs dans les Universités et Grandes Écoles, capables de former au dernier cri des tendances cyber : le développement sécurisé, les systèmes d'exploitation récents (MacOS Ventura, Windows 11, Ubuntu 22.04 LTS, etc.), la gestion d'identité, la cryptographie, etc. La charge de travail des rares enseignants spécialisés est aujourd'hui peu tenable, et dans les BTS/BUT/licences professionnelles jusqu'aux Grandes Écoles ce sont les étudiants qui en font les frais. Il faut proposer aux enseignants d'informatique d'actualiser régulièrement leurs formations ou de se convertir à l'enseignement de la cybersécurité, et à des professionnels de la cybersécurité, qui interviennent souvent comme prestataires de service au sein des établissements, des formations pour être mieux formés à la pédagogie. Le Pôle d'excellence cyber travaille avec plusieurs établissements à l'élaboration de certifications.

- **Former les jeunes dès le collège aux problématiques numériques**, en les intéressant au fonctionnement de leurs outils, leur faire faire pour leur système Windows, par exemple, le Guide de sécurité numérique produit par le Pôle d'excellence cyber [1] et les 15 tutoriels vidéo associés sur notre chaine YouTube[2] . Compléter leurs compétences dès la seconde et jusqu'à la terminale en leur apprenant à protéger & défendre, s'inspirer de leurs retours d'expériences numériques, surtout sur les réseaux sociaux, grâce aux compétences acquises par les enseignants formés à la cyber par le Rectorat de Rennes. Des outils pédagogiques seront d'ailleurs mis en ligne afin que ceux-ci puissent trouver des contenus adaptés à leurs compétences. Par contre nous déconseillons d'apprendre aux plus jeunes élèves les techniques d'attaque, l'enseignement des attaques ne devant commencer à s'enseigner qu'au terme du BAC+2, âge auquel la plupart des individus ont déjà développé un sens éthique.

- **Revaloriser les formations de techniciens informatiques colorées cyber :** permettre à ces profils d'être mieux rémunérés, et d'avoir des perspectives de carrières ou de continuité d'études (certification ou diplôme) tout au long de la vie facilitées. Pour cela faire connaître aux chefs d'entreprises quelles sont les formations qui garantissent un niveau minimal en cyber (grâce aux Label CyberEdu[3] et SecNumEdu[4]).

1 https://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/GuideSecurite_organisations-V1-1_WEB1.pdf
2 https://youtube.com/playlist?list=PLzQd6dPwHSN3AAL5TLPaHSR9hW6bymkDn
3 Label qui valide la prise en compte de la cybersécurité dans l'ensemble des formations supérieures françaises en informatique.
4 Label de formations initiales ou continues (SecNumEdu-FC) en cybersécurité de l'enseignement supérieur.

- **Permettre à certains cursus d'études d'intégrer des modules cyber ou de se scinder en double-cursus :** apprendre un domaine métier, en y intégrant des cours de cybersécurité, les filières STAPS en sont un bon exemple. Compte-tenu des débouchés de sortie, ces filières pourraient être un laboratoire d'expérimentation du double cursus, d'autant plus que nombre d'élèves sortent des filières scientifiques. De plus, au regard du nombre d'étudiants qui s'y inscrivent, c'est aussi un vivier important pour les administrations, en particulier le ministère des Armées. Le CNAM Bretagne pourrait, avec le Rectorat de Rennes, expérimenter ce modèle à Saint-Brieuc, qui pourrait être ensuite proposé au National.

- **Former tout utilisateur de produits numériques :** Toutes les ressources humaines de l'organisation, y compris les administratifs, les fournisseurs, doivent être formés a minima à l'hygiène de base et aux bonnes pratiques qui concernent leur périmètre (secrétariat, comptabilité, production, achats, qualité, commerce, etc.). De nombreuses structures étatiques proposent des sensibilisations poussées, certaines très opérationnelles qui s'adaptent aussi au métier de l'entreprise ; c'est aussi le cas d'entreprises privées. Le Pôle d'excellence cyber a produit un Guide de sécurité numérique pour les collectivités, PME/PMI et petites organisations augmentées de nombreux tutoriels pour permettre à tout utilisateur non informaticien de sécuriser au mieux son système Windows 10.

- **Plus largement, faire entrer la cyber dans tous les cursus métiers innovants et porteurs :** santé, maritime, IA, satellite, agro-alimentaire, électronique, nucléaire, etc. C'est ce qui a déjà été fait au Campus ESPRIT de Redon (ESLI) et de Paris (ESTI) pour la logistique et les achats.

- **Permettre aux jeunes et moins jeunes d'avoir une information fiable sur les cursus de formation cyber :** Le Pôle d'excellence cyber a produit un Catalogue National des formations cyber post BAC qui sera bientôt à disposition de tous sur le site d'information et d'aide à l'orientation (Idéo) du Conseil Régional de Bretagne. Les formations ici proposées sont marquées des labels (CyberEdu, SecNumEdu, CGE[1], etc.) qu'elles possèdent.

Actions à moyen terme :

- **Construire une formation socle à Bac+3 en cybersécurité**, un tronc commun post BAC, spécialisé dans le domaine cyber avec une forte proportion liée à l'entrainement (TP/TD autour des problématiques liées à la gestion de l'information et des événements de sécurité (SIEM), de Centre des Opérations de Sécurité (SOC) et de centres d'alerte et de réaction aux attaques informatiques (CSIRT) qui ont besoin de gros volumes de techniciens aujourd'hui.

- **Faire en sorte que tous les cursus proposés par les Universités et les écoles d'ingénieur intègrent des modules liés à la cybersécurité dès les premiers semestres de formation**, ce qui est d'ailleurs déjà le cas dans certaines écoles (ENSIBS[2], ESIEA[3], EPITA[4], *Cyber School* de Rennes, École 2600, CNAM[5], etc.).

- **Créer un guichet unique pour les métiers de la cybersécurité collé au Catalogue National des formations cyber disponible sur Idéo :** Candidatures spontanées, CV, offres d'emplois, d'alternances, de stages régionalisées, information sur les métiers, sur les dispositifs d'accompagnements, les évolutions de carrières, indications sur les salaires. Cet ambitieux projet pourrait répondre aux besoins du marché. Utiliser la matrice des compétences conçue par l'ANSSI[6] pour parfaire les parcours et recommandations

- **L'entreprise doit favoriser la reconversion des personnels qui sont volontaires ou qui possèdent une expertise dans le domaine cyber. L'État doit participer à cette dynamique salutaire pour le pays.** Pour ce faire, la création de modules de formations en distanciel est la solution idéale pour les organisations et les volontaires (type CNED). La période COVID, et la systématisation du télétravail qui a suivi et forgé des habitudes, la volonté des plus jeunes à ce que leur travail soit ainsi aménagé, tout pousse les enseignants à repenser l'éducation et leurs méthodes pédagogiques. L'apparition de *MOOC*[7], *COOC*[8], *SPOC*[9], et le fort développement des moyens numériques souverains (*FUN MOOC*, Tixeo, Whaller, *Private Discuss*, etc.), de plateformes de TP/TD avec une correction par les pairs, sont autant de moyens de bien se former aux différents métiers de la cybersécurité.

1 Conférence des Grandes Écoles.
2 L'École Nationale Supérieure d'Ingénieurs de Bretagne Sud.
3 L'École supérieure d'informatique électronique automatique.
4 L'École pour l'informatique et les techniques avancées.
5 Conservatoire National des Arts et Métiers.
6 https://campuscyber.fr/wp-content/uploads/2022/01/Matrice_competences_metiers_CampusCyber.xlsx
7 Acronyme formé des initiales de Massive Open Online Course, en français cours en ligne ouvert à tous ou CLOT ou encore cours en ligne ouvert massivement ou CLOM.
8 *Corporate Online Open Course.*
9 *Small Private Online Courses*, un *MOOC* payant.

- **Proposer aux gens de la filière cyber des parcours de carrière et des évolutions vers d'autres métiers ou d'autres univers professionnels, cela en fonction de leur profil et de leur formation initiale :** les gens ont besoin de connaître les possibilités d'opportunités tout au long de leur vie professionnelle. Le Pôle d'excellence cyber est au cœur de l'animation de la filière cyber Nationale, en prise directe avec les besoins des industriels et administrations et de l'évolution des cursus de formations. Le Pôle doit favoriser la mutualisation de moyens souverains, informer sur les risques de choix non souverain, labelliser et promouvoir les solutions françaises ou européennes.

- **Saluer l'arrivée des familles sur un territoire pour les gens qui sont en mobilité professionnelle, pour exposer à leur conjoint les possibilités de réinsertion vers la filière cyber avec des parcours adaptés au profil de la personne (type de cursus, technicien ou ingénieur).** Plus largement, promouvoir le territoire Breton grâce à des initiatives cyber dans les filières maritime, santé, satellitaire, agro-alimentaires via des formats atypiques : films, serious games, challenges, jeux, etc. Le Pôle d'excellence cyber est quant à lui en appui des sécurisés pour leur proposer un diagnostic cyber Cyber-diagnostic pour l'Amélioration de la Résilience des Entreprise (CARE), et proposer une liste de sécurisants sur son catalogue CyberLab dans le cadre du projet européen European Digital Innovation Hub EDIH[1], ceux dont le métier est d'aider tous ceux qui ont un besoin d'être sécurisés des partenaires sérieux, filtrés par l'expertise du Pôle.

Logo du diagnostic cyber : Cyber-diagnostic pour l'Amélioration de la Résilience des Entreprise (CARE).

- **Produire des modules de certifications de type SANS Institute[2], en français et en anglais, et les porter à l'Europe :** nous avons toutes les compétences en France pour produire ces modules de formation sur tous les domaines de la cybersécurité, des unités courtes d'enseignements, très opérationnelles, qui délivrent une certification de haut niveau. Le Pôle a pour projet de construire ce type de parcours et de le proposer aux pays européens qui envoient leurs personnels faire ce type de formation. Un partenariat avec l'ENISA est bien entendu envisageable.

- **Par ailleurs, des initiatives comme la CVthèque de Bretagne Commerce International (BCI), ou son nouveau service Business to Students,** permettent d'interfacer les entreprises bretonnes et les étudiants bretons ou suivant un cursus à dimension internationale en Bretagne. En Bretagne, à l'étranger ou à distance, sur des périodes courtes ou longues, il leur est proposé des missions opérationnelles ou d'études, des projets tutorés ou des stages, de potentielles ressources opérationnelles pour accompagner les entreprises bretonnes adhérentes qui ont des activités à l'international. BCI propose aussi des synthèses marchés ou Entreprises et Organismes pour de nombreux pays.

1 Les pôles européens d'innovation numérique (*EDIH*) sont des guichets uniques qui aident les entreprises et les organisations du secteur public à relever les défis numériques et à devenir plus compétitives.
2 https://www.sans.org/cyber-security-courses/?msc=main-nav

Actions à plus long terme :

- **Collégiens & lycéens doivent prendre en charge leur sécurité numérique, les enseignants ayant l'obligation de former les jeunes à la sécurité du numérique.** Un bon moyen de motiver des vocations chez les jeunes garçons et filles. Des filles auxquelles il faut expliciter l'intérêt des sciences et techniques, mais surtout les forts enjeux en termes d'éthique, de souveraineté et d'intérêt pour les constructions de notre monde futur. Faire en sorte que les collégiens et lycéens s'intéressent à ces métiers par leurs pratiques quotidiennes des outils numériques, leur exposer aussi, ainsi qu'au corps enseignant et à leurs parents, la forte dynamique de recrutement dans la filière et les perspectives de carrières variées.

- **Faciliter la transition des organisations vers la cyber :** Le dirigeant, le CODIR, le DSI et le RSSI sont des acteurs complémentaires de la mise en place de la cybersécurité, et un appui opérationnel doit leur être apporté via des informations (FAQ [1] concernant des exemples courants et pratiques, par exemple, ou une liste de prestataires de services souverains et de confiance pour les différents domaines de la cyber (c'est le catalogue de services Cyberlab produit par le Pôle d'excellence cyber, qui permettra aussi de contrer les propositions commerciales parfois agressives de prestataires problématiques)) et des formations courtes en ligne (type MOOC [2] de l'ANSSI), des formations techniques et organisationnelles en présentiel et en format court, surtout pour les entreprises ne disposant pas de ressources dédiées, tout cela pour fluidifier la déclinaison opérationnelle de la sécurité et faciliter sa bonne compréhension par le CoDir [3] .

- **S'appuyer sur les acteurs existant (CARIF-OREF [4], OPCO ATLAS [5], CIO [6], Salons étudiants ou de l'emploi, Universités & Grandes Écoles) pour bien expliciter aux publics concernés en quoi consistent les métiers cyber :** ces métiers techniques sont souvent définis, comme en médecine, par des acronymes et des termes propres à la filière, qui sont donc difficilement compréhensibles pour un néophyte : pentest, forensique, urbaniste, etc. Cela ne favorise pas la projection des étudiants vers ce secteur, d'autant plus que la sécurité, qui tente à bloquer certains usages, parait être une discipline plus rébarbative pour les jeunes que cette ultra connectivité imposée par leurs nombreux appareils (téléphones, tablettes, consoles de jeux, montres, IoT globalement) et logiciels (réseaux sociaux, de partage, boites mèls, etc.).

Carte 1. Localisation des CIO en Bretagne

Source : Rectorat de l'académie de Rennes.

1 Foire aux questions.
2 Acronyme formé des initiales de massive open online course, en français cours en ligne ouvert à tous ou CLOT ou encore cours en ligne ouvert massivement ou CLOM.
3 CoDir: comment organiser un comité de direction.
4 Centres d'animation, de ressources et d'information sur la formation (Carif) et les Observatoires régionaux de l'emploi et de la formation (Oref).
5 Atlas est l'opérateur de compétences des services financiers et du conseil.
6 Centre d'information de l'orientation.

- **Il serait intéressant d'évaluer les besoins par zone géographique, département ou bassin d'emploi,** cela afin de d'informer les prescripteurs RH locaux des besoins en termes de ressources cyber pour leur territoire, que ceux-ci adaptent leur discours aux besoins actuels et futurs, surtout en ce qui concerne les techniciens ; la carte produite par l'APEC montre bien aussi le dynamisme de la filière concernant le recrutement des cadres en 2023. Des études emploi-formation département par département devraient être menées au profit des entreprises qui ont le besoin de se sécuriser.

- **Ainsi, établir dans chaque Bassin d'animation de la politique éducative (BAPE) une dynamique CYBER dès le collège, dans une logique d'ancrage géographique des étudiants jusqu'au niveau BAC+3, un phénomène bien connu.** Le but étant alors que chaque territoire soit doté d'une licence professionnelle au moins partiellement dédiée à la sécurité du numérique. La capacité d'un territoire à proposer une continuité d'études à ses étudiants se lit aussi au regard des filières SIO, CIEL, BUT et Bachelor proposées par les établissements tant publics que privés qui s'y trouvent. Dans ce cadre, les AMI [1] Compétences et Métiers d'Avenir, Cyber4Skills porté par l'Université de Rennes 1 et l'Université de Bretagne Sud d'un côté, et le second porté par le Groupement d'Intérêt Public (GIP) ESPRIT de Redon, IFALP [2] de l'autre pourraient être de formidables outils pour développer ces idées. Dans certains territoires (Saint-Brieuc, Lannion, Redon, etc.), la possibilité de continuité d'études vers la filière sécurité du numérique doit être envisagée.

- **Les filières STAPS devraient être aménagées afin que les étudiants soient aussi formés à la cybersécurité**, une bonne partie d'entre eux devant refaire un cursus tout autre dès sa sortie de formation tant les débouchés sont malheureusement faibles.

- **Favoriser les initiatives de filière et les initiatives locales, avec l'appui du MEDEF, de la CGPME, des grandes entreprises et des ETI,** pour informer et accompagner les structures ne disposant pas des ressources suffisantes pour mettre en place les mesures de base de protection vis-à-vis du risque cyber dans leurs entreprises étendues. La présence du Pôle d'excellence cyber au Forum Economique Breton dans ses 2 premières années d'existence aura permis d'amorcer la sensibilisation des donneurs d'ordres aux problématiques cyber au sein de leur métier. Bretagne Développement Innovation devrait reprendre ces sensibilisations des sécurisés dans ce type de salon, ou dans les autres grands salons bretons (CFIA [3] , pour l'agroalimentaire, par exemple). Le catalogue CyberLab produit par le Pôle d'excellence cyber permettra à ces décideurs de trouver les meilleurs partenaires pour assurer la sécurité leurs productions et développements.

- **Favoriser la mise en avant de professionnels ambassadeurs de la cybersécurité :** force est de constater que les personnes les plus à même de parler de la cybersécurité sont ceux dont c'est le métier, ceux qui ont évolué durant leur carrière d'un poste à un autre, de la technique à l'organisationnel. C'est aussi le cas de passionnés, qui, dans des métiers connexes (Droit, sciences humaines et sociales, renseignement, IA, etc.) travaillent la cybersécurité. Des actions vers les établissements d'enseignement général ou technique ou des témoignages en ligne seraient probants. Le Pôle d'excellence cyber a débuté une série de vidéos de spécialistes cyber qui explicitent leur métier. Nous avons aussi créé un programme « Les cadettes de la cyber » pour promouvoir la place des femmes dans la filière. Enfin, nous avons mis en ligne des podcasts « La matrice a buggé » afin de sensibiliser les plus jeunes dès la 3ième aux risques numériques et aux précautions d'usages. Les services de l'État concernés par les problématiques de cyberdéfense, le ministère de l'Intérieur (Police & Gendarmerie), le ministère des Armées (COMCYBER, COMSIC [4], DGA-MI [5], DRSD [6]), l'ANSSI, le SISSE proposent des actions de sensibilisation sur les dangers du numérique et la protection des données et de la propriété intellectuelle aux établissements qui le demandent ou dépendent de leur périmètre. Ces sensibilisations sont un excellent moyen de toucher les décideurs et de leur faire prendre conscience de la menace grandissante et des actions et financements possibles pour former leurs salariés et se sécuriser.

- **Prendre en compte la dimension européenne :** la mise en place de la norme NIS V2 va augmenter significativement le nombre d'organisations concernées par l'obligation de cybersécurité. C'est à la fois une opportunité pour la filière, mais aussi un challenge colossal qui va demander bien plus de main d'œuvre pour arriver au résultat escompté, sécuriser les organisations européennes. Les entreprises françaises doivent travailler au plus proche de cette norme pour développer au mieux leurs offres de services. Dans le cadre du projet EDIH breton, le Diagnostic Cyber porté par le Pôle d'excellence cyber, CARE, pour Cyberdiagnostic pour la Résilience des Entreprises, permettra aux entreprises bretonnes, françaises et européennes de valider un niveau de maturité et de leur proposer des prestations adaptées pour renforcer encore leur résilience qui seront listées dans notre Catalogue National d'offre de service CyberLab.

1 Appel à manifestation d'intérêt.
2 Institut Français des Achats et de la Logistique publics.
3 Carrefour des Fournisseurs de l'Industrie Agroalimentaire de Rennes.
4 Commandemment des systèmes d'information et de communication à Cesson-Sévigné.
5 Délégation Générale pour l'Armement Maîtrise de l'Information.
6 Direction du Renseignement et de la Sécurité de la Défense.

QUELQUES INITIATIVES COMPLÉMENTAIRES INTÉRESSANTES

Une initiative nationale : AirCyber

Airbus, Dassault Aviation, Thales et Safran ont lancé, en janvier 2019, le programme AirCyber, avec comme objectif d'augmenter la cybersécurité de la *supply chain* aéronautique avec quatre missions :

• Evaluer la maturité de l'entreprise sur la base de critères validés par la filière et par les fondateurs de *BoostAerospace* afin d'établir un plan d'actions cyber ;

• Mettre à disposition une bibliothèque de documents cybersécurité issue des fondateurs de *BoostAerospace* et adaptée aux spécificités de la *Supply Chain* de la filière ;

• Fournir un accès à un catalogue de services et de solutions cyber de confiance adapté à la filière et enrichi en permanence par les retours d'expériences ;

• Accéder à un plan de sensibilisation et de collaboration global grâce à des ateliers, les rapports des autorités de tutelles et l'animation d'une communauté en ligne.

Cette initiative permet aux grandes entreprises de limiter les risques encourus avec leurs partenaires de plus petite taille.

Une initiative régionale des Hauts-de-France : le Pass Cyber Conseil

A l'initiative du Conseil Régional, l'agence Hauts-de-France Innovation Développement propose sur son territoire un accompagnement à la Cybersécurité : le Pass Cyber Conseil. Il s'agit d'un accompagnement sous la forme d'audits ou d'études techniques destinés aux PME (<250 salariés, et qui ne sont pas en difficulté) implantées en Hauts-de-France qui déboucheront sur des préconisations. Les entreprises doivent améliorer leur stratégie en matière de sécurité et respecter des bonnes pratiques pour réduire l'exposition aux menaces.

Le Conseil Régional Hauts-de-France finance 50% de la prestation dans la limite de 10 k€ HT (hors tâches récurrentes de gestion journalière des systèmes d'information). Une entreprise ne peut demander qu'une seule demande d'aide sur ce dispositif dans un délai de 2 ans.

Une initiative locale brestoise : GACYB

Créée en 2017 par la CCIMBO Brest et soutenue par l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information), le GACYB (Groupement des Acteurs en cybersécurité) est une association composée d'une trentaine d'entreprises finistériennes. L'objectif est de sensibiliser l'ensemble des acteurs économiques finistériens à l'importance de la cybersécurité, de les sensibiliser et de proposer une permanence aux professionnels.

Le GACYB intervient sur toute la Bretagne et se développe sur d'autres départements. Cette initiative permet aux entreprises locales de pouvoir disposer d'un interlocuteur référencé, qui puisse les accompagner dans leur démarche de sécurisation du SI de l'entreprise.
Ces différentes initiatives sont pour la plupart des initiatives basées sur le volontariat, ciblées sur des secteurs d'activité précis ou adressé à un nombre réduit d'organisations, via l'intervention d'entités externes et avec un budget significatif pris pour partie en charge.

Une initiative régionale : Breizh Fab

https ://www.breizhfab.bzh/

Breizh Fab, est un programme d'envergure en faveur des PME manufacturières de Bretagne. Il s'inscrit dans la dynamique nationale portée autour de l'industrie.

Agissant comme un accélérateur de l'industrie bretonne, Breizh Fab propose un ensemble de solutions destinées à aider les PME bretonnes à intégrer les mutations technologiques, organisationnelles et environnementales en cours, pour gagner en compétitivité.

Des consultants référencés qui agissent auprès d'entreprises industrielles sur différents sujets (RSE, changement d'*ERP,* etc.), des interventions pouvant être prises en charge pour la phase d'analyse du besoin et de mise en œuvre.

Source : http://www.breizhfab.bzh/

Breizh CTF

Breizh CTF (https://www.breizhctf.com/) : compétition de hacking informatique de type Capture the Flag, 600 passionnés venus de toute la France démontrent par équipe leurs savoir-faire durant 12h de compétition de nuit. Imaginée par deux spécialistes de la cybersécurité, @_SaxX_ et @kaluche_, et organisée par BDI grâce au précieux concours du pool technique gcc_ensibs et la contribution des équipes de Claranet, Icodia & Sekoia. Cette compétition acceuille depuis 2022 un Hack & Job & un Cyber Tour en partenariat avec Rennes Métropole, durant lequel les candidats à la recherche d'opportunités professionnelles peuvent venir rencontrer des entreprises à la recherche de nouveaux talents. L'événement est gratuit pour les participants grâce au partenariat avec la Région Bretagne, Rennes Métropole et la participation de nombreux sponsors.

WeKer - Rennes Métropole

Acteur majeur de la mise en œuvre des politiques publiques de l'emploi, We Ker déploie, sur le Bassin d'Emploi de Rennes, un service de proximité pour notamment animer un réseau de partenaires et coordonner des actions autour des enjeux d'emplois et de compétences. Avec le soutien de Rennes Métropole dans le cadre de son plan de rebond(s), la DDETS35 et le FSE, We Ker porte une mission de Gestion Prévisionnelle des Emplois et des Compétences Territoriale (GPEC) et intervient sur la filière cybersécurité.
Une démarche qui s'inscrit autour de quatre opportunités qui font sens pour la Métropole rennaise : développement économique (direct et indirect), rayonnement majeur à l'international comme territoire de la confiance numérique, un pilier smartcity & cyber (complément du pilier MinArm/régalien), faire de la confiance numérique une réalité pour les gens de la métropole, pour une meilleure acceptation des services numériques.
La GPEC-T Cyber, une démarche qui participe à fédérer et créer des synergies entre acteurs émanant de différentes sphères professionnelles, regroupés autour d'enjeux partagés une démarche portée par un collectif d'acteurs et structurée autour

- Du recensement des besoins RH des employeurs du territoire en particulier via une enquête annuelle validé par un comité de pilotage en présence de l'AUDIAR ;
- De l'identification et la caractérisation de viviers : formation initiale, talents à attirer sur le territoire, personnes en reconversion professionnelle dont étudiant en reconversion, personnes hors de la filière en recherche d'emploi, talents en devenir : lycéens et collégiens.
- D'actions concrètes menées à l'adresse de ces viviers, via la mobilisation de différents acteurs, tables rondes sur les métiers de la cybersécurité lors de différents événements (salon de l'étudiant, salon de l'alternance organisés par l'Etudiant, nuit de l'orientation portée par la CCI35, panorama de métiers porté par l'Exploratoire, semaine du numérique de Pôle Emploi, Printemps du numérique), participation à des forums emplois-métiers (safari métiers du numérique avec ADN Ouest, mobilité défense organisé par l'Antenne Défense Mobilité de Rennes), webinaire à destination de public cadres en partenariat avec l'APEC, mise en place d'actions spécifiques dans le cadre de Plan de sauvegarde de l'emploi (PSE) (avec le Pôle d'excellence cyber, la CyberSchool, Amossys, Orange, BDI, l'Audiar), sensibilisation de consultants-conseillers emplois (AFPA, Groupement Evolution Professionnelle), accompagnement de personnes en reconversion professionnelle via le Syndicat Initiative cyber porté Stéphane Szymanski via la CyberSchool.

Annexes

Les contraintes réglementaires

Ces différentes réglementations imposent aux organisations de se mettre en conformité :

- Loi Informatique et Libertés : Délégué à la protection des données (abrégé DPD, ou *DPO* en anglais, pour Data Protection Officer);
- Règlement Général sur la Protection des Données ;
- Directive sur la sécurité des réseaux et des systèmes d'information, Directive *NIS* (UE) 2016-1148 et maintenant *NIS* V2 ;
- Loi de programmation militaire depuis 2014 ;
- Les normes ISO 27001/2/3/4/5 & 22301, par exemple, plus celles liées aux domaines métiers ;
- L'Instruction Générale Interministérielle n°13000/SGDSN/PSE/PSD du 9 août 2021 ;
- Protection économique des entreprises : réforme de la loi dite « de blocage » de 1968.
  Deux textes de lois viennent compléter et simplifier les modalités de la loi dite « de blocage » de 1968. Celle-ci vise à protéger les intérêts économiques et les entreprises lors d'enquêtes menées par des autorités étrangères. Explications.
  Renforcer la loi dite « de blocage » de 1968 et l'arsenal de protection économique des entreprises face au niveau extraterritorial. C'est l'objectif des deux textes parus au Journal officiel les 20 février et 16 mars relatifs à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.
  Qu'est-ce que la loi dite « de blocage » de 1968 ?
  Cette loi permet d'éviter que les autorités étrangères ne viennent à connaître des informations sensibles attentant aux intérêts de la Nation, y compris ses intérêts économiques essentiels, lors d'enquêtes. Elle oblige les autorités étrangères à respecter les canaux de l'entraide judiciaire ou administrative internationale.
  Ce décret et cet arrêté d'application de la loi s'inscrivent dans un contexte marqué par l'utilisation croissante par des acteurs étrangers de lois à portée extraterritoriale.
  Un parcours d'accompagnement des entreprises
  L'enjeu de cette réforme est donc de clarifier la procédure de saisine pour les entreprises et de désigner un guichet unique pour les acteurs concernés : le service de l'information stratégique et de la sécurité économiques (SISSE) de la direction générale des Entreprises.
  Les entreprises bénéficient désormais d'un interlocuteur privilégié qui, en lien avec les différentes administrations de l'État, peut les accompagner vis-à-vis des demandes étrangères dans le respect de la loi de blocage.
  Il s'agit également de renforcer la sécurité juridique pour les entreprises en leur permettant de disposer d'avis de l'administration dans un calendrier adapté aux procédures administratives et judiciaires. Ces avis renforceront l'opposabilité de la loi de blocage vis-à-vis des juridictions étrangères.Le SISSE propose ainsi un véritable parcours d'accompagnement des entreprises face aux menaces extraterritoriales. (Site du SISSE)

Les contraintes contractuelles

Des clients grands comptes imposent à leurs prestataires et partenaires certaines normes ou label pour se protéger contre le risque cyber, cela afin de limiter le risque par contamination de leur SI, ou tout simplement pour garantir que ses partenaires critiques ne soient pas à l'arrêt (interruption de flux ou de service) suite à une attaque. Cela peut aller jusqu'à imposer une démarche pour l'obtention d'une certification ou d'une normalisation, afin que le sous-traitant parvienne au niveau d'exigence requis par le donneur d'ordre.

Le marché Cyber Français

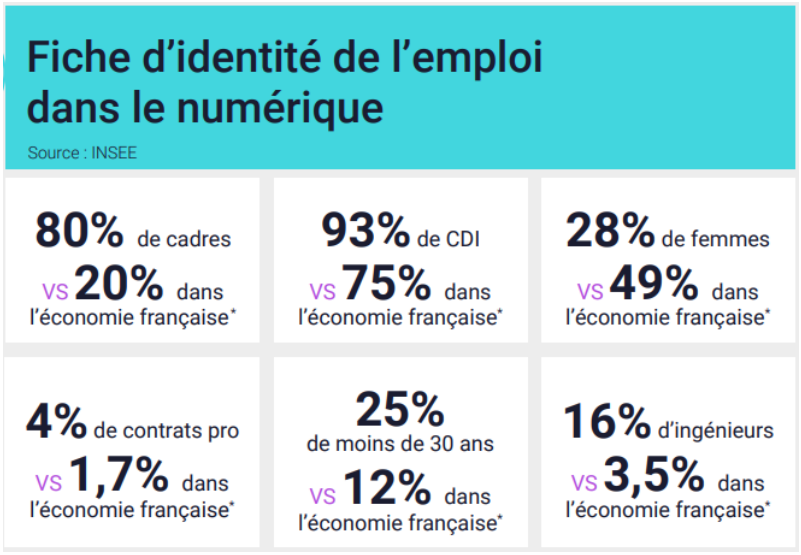
Estimation d'une croissance annuelle de près de 8.5 % par an :

- en 2020 : 2.8 Md d'€;
- en 2025 : 4.2 Md d'€.

Source : Markess by Exaegis

Le marché concerne tous les secteurs de l'économie, tous les acteurs, quelque soit leur niveau.

Cette infographie de l'INSEE montre bien l'importance du secteur du numérique en France, une filière qui attire les jeunes. Féminiser la filière reste un enjeu.



Source : https://numeum.fr/sites/default/files/Documents/NUMEUM_-_Chiffres_et_datas_2021_def.pdf

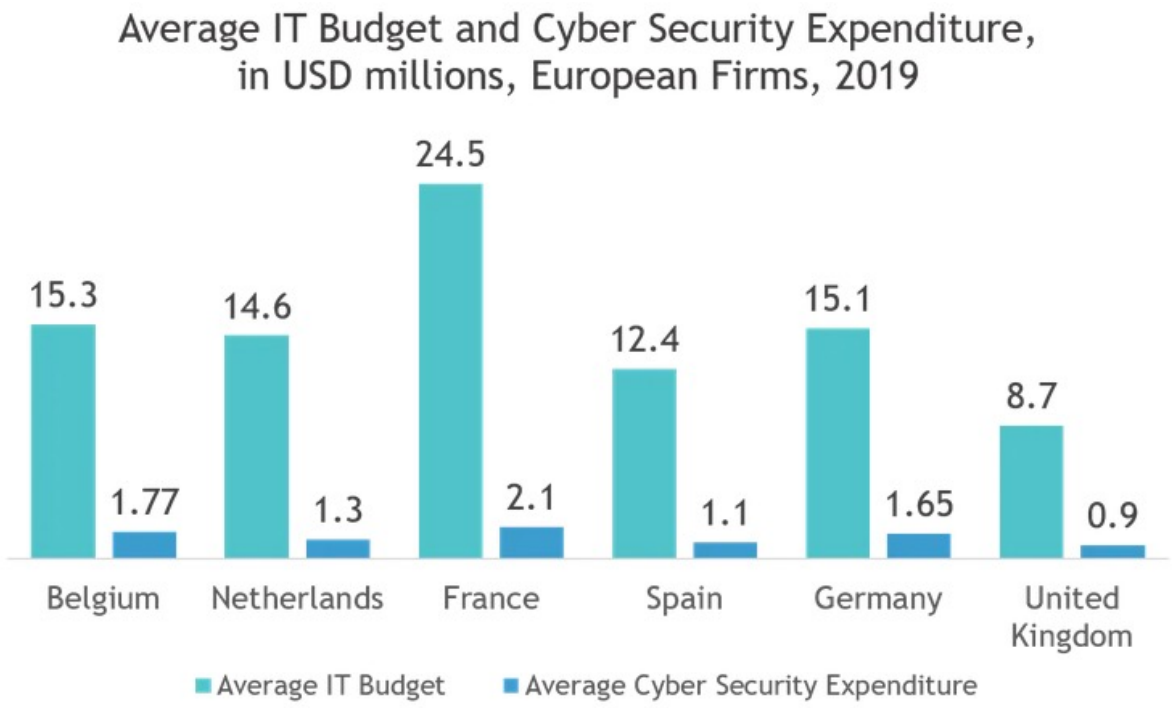
Le marché Cyber Européen

Estimation d'une croissance annuelle de près de 15 % par an :

- en 2020 : 8,56 Md de $;
- en 2027 : une projection de 22,67 Md de $.

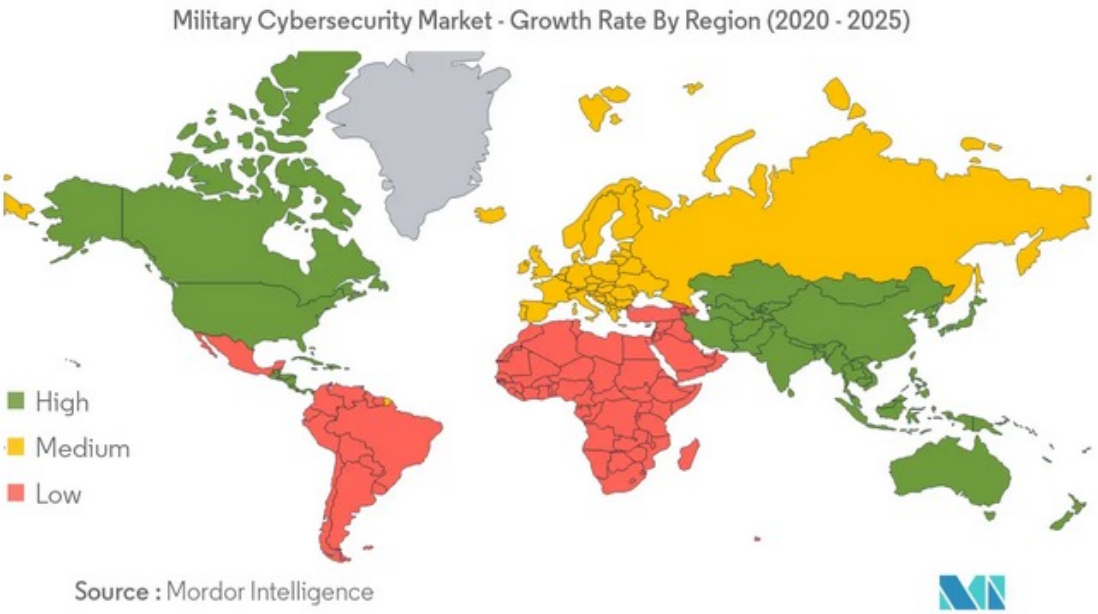
Source : https://www.researchandmarkets.com/r/wdx47r

Notons qu'en 2019 la France était, avec la Belgique & l'Allemagne, le pays européen qui dépensait le plus dans la cybersécurité.



Source : https://www.mordorintelligence.com/fr/industry-reports/france-cybersecurity-market

Le marché militaire mondial



Autres parutions :

La Monographie : formation professionnelle, apprentissage et emploi sorti en février 2023 et les deux documents d'orientation du **contrat de plan régional de développement des formations et de l'orientation professionnelles (CPRDFOP)**, la partie numérique et son annexe qui liste des diplômes du numérique.

Les 2 rapports de l'**Observatoire Régional des Compétences Numériques (ORCN)**, projet porté par ADN Ouest pour les régions Pays de la Loire et Bretagne, viennent conforter notre enquête :

ENQUÊTE BRETAGNE sortie le 23 mai 2023

Retrouvez les résultats complets de l'enquête emploi et compétences de l'ORCN 2023 menée auprès de décideurs du numérique du bassin d'emploi de la Région Bretagne.
En particulier, cette étude révèle les dernières tendances en termes de recrutements, de besoins en compétences, des évolutions des technologies et des métiers recherchés par les entreprises sur le territoire.

RAPPORT D'ANALYSE sortie le 23 mai 2023

Retrouvez l'analyse des résultats de l'enquête ORCN 2023 menée auprès de décideurs du numérique des bassins d'emploi des régions Bretagne et Pays de la Loire.
En particulier, les interviews des professionnels du numérique, du recrutement et de la formation dressent un état des lieux complet des dernières tendances en termes de recrutements, de besoins en compétences, des évolutions des technologies et des métiers recherchés par les entreprises dans le Grand Ouest.

NOTES

NOTES

NOTES

NOTES

PÔLE D'EXCELLENCE CYBER

12 B rue du Patis Tatelin
35700 Rennes
France

www.pole-excellence-cyber.org