ÉCONOMIE I BREST MÉTROPOLE

LA FILIÈRE CYBERSÉCURITÉ DANS BREST MÉTROPOLE

Mars 2025 **RAPPORT D'ÉTUDE**

ADEUPa
BREST • BRETAGNE

SOMMAIRE

CHIFFRES CLÉS

123 emplois dans les entreprises spécialisées

+48 emplois en 5 ans (+64 %)

8 entreprises

89 chercheurs

Des chaires

- AI for privacy (sécurisation des biens et personnes)
- Cyberdéfense des systèmes navals (sécurisation des navires et des ports dans les domaines civil et militaire)
- Cybaile (IA de confiance, robuste et sécurisée en santé)
- Cyberlot (sécurisation des objets connectés)

86 organisations concernées par NIS2 à Brest métropole dont un tiers de collectivités

80 établissements locaux indirectement concernés au travers de leur siège social situé hors territoire

Des organisations d'acteurs

- France cyber maritime
- Gacyb
- Bretagne Cyber Alliance

BRETAGNE Cyber Alliance
Le campus cyber breton

GACYB Bretagne

Deux événements majeurs organisés sur le territoire

UYBHYS et le Breizh cyber show

Cybersécurité, de quoi parle-t-on ?

Qu'est-ce-que la cybersécurité ?

Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), la cybersécurité est « l'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 ». La quête de cet état induit de nombreuses activités économiques comme la recherche, la formation, le diagnostic de système (test d'intrusion), la production et l'intégration de solutions logicielles ou encore la réponse à incident.

Si la cybersécurité est une filière en tant que telle, avec une chaîne de valeur bien définie, elle n'en reste pas moins applicative et transversale à l'ensemble des secteurs d'activités. Elle s'impose naturellement dans les secteurs étroitement liés au numérique, comme le milieu de la banque et des assurances, et elle devient de plus en plus incontournable auprès de secteurs qui opèrent leur transition numérique tels que l'industrie, l'agriculture, le commerce, etc. Certains domaines requièrent des besoins en cybersécurité plus approfondis comme la Défense, la santé ou encore le spatial et apparaissent, de fait, plus attractives auprès des spécialistes. Selon une enquête menée par l'Anssi, 70 % des répondants considèrent l'industrie aéronautique/spatiale et la Défense comme des secteurs très attractifs en termes de métiers de la cybersécurité.

Chaîne de la valeur : de la sensibilisation à la gestion de crise

La chaîne de la valeur de la cybersécurité se décompose en quatre parties. En amont, la sensibilisation et la formation à la cyberprotection regroupe l'ensemble des bonnes pratiques (formation, sensibilisation) et stratégies (audit) visant à protéger le système d'information.

La cyberdéfense se décline en deux activités avec, d'une part, une vocation défensive visant à consolider la robustesse du système d'information face aux attaques en le restructurant, en y ajoutant des couches logicielles par exemple. La mise en place de tests de vulnérabilité, allant du « pentest » au « hacking éthique » en reprenant les mêmes codes que les cybercriminels, fait aussi partie intégrante de la défense du cyberespace.

La lutte informatique offensive (LIO) désigne quant à elle l'ensemble des actions menées pour neutraliser, perturber ou attaquer les systèmes informatiques adverses, dans un cadre stratégique ou militaire, afin de défendre ses intérêts et renforcer sa cybersécurité.

Enfin, le chaînon de la réponse à incident ou la cyberrésilience intervient lorsqu'une organisation a été victime d'une attaque (fuite de données, rançongiciel). Il s'agit d'essayer de stopper la prolifération de la menace, et de faire en sorte que l'organisation puisse poursuivre son activité en mode « dégradé » et qu'elle retrouve, dans la mesure du possible, le maximum de données.

Une dernière phase appelée « cyber renseignement » vise à comprendre, en permanence, le niveau de menace et à retracer les indices laissés après une cyberattaque.

Plusieurs typologies d'acteurs composent la filière :

- La recherche-développement, qu'elle soit hébergée au sein de laboratoires publics ou bien au sein des entreprises.
- Les organismes de formation regroupent les structures d'enseignement qui forment les étudiants aux métiers de la cybersécurité, les organismes de formation continue qui accompagnent les reconversions de salariés ou leur montée en compétences et les sociétés qui interviennent au sein des entreprises pour former à la cybersécurité.
- Les intégrateurs de cybersécurité, dont les propres produits requièrent la mise en place de couches cybersécurisées. Ces entreprises ne sont pas spécialisées dans la cybersécurité et font partie du halo de la filière, par opposition avec les pure players[1] qui composent le cœur de la filière.

1. Entreprises exerçant dans un secteur d'activité unique, en l'occurrence la cybersécurité.

Photo : ©France Cyber Maritime

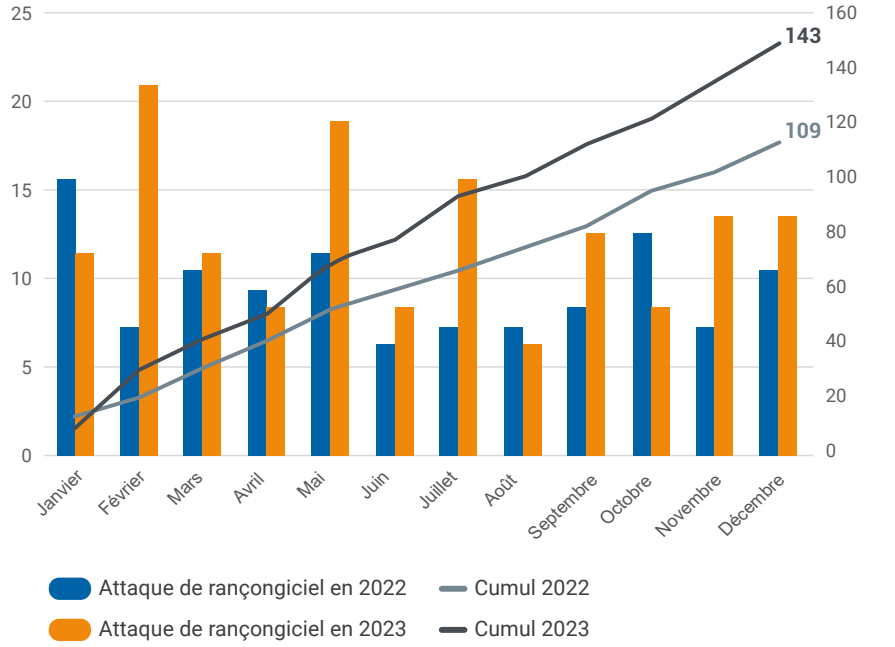
Un marché en explosion dans un contexte de menace omniprésente

Le marché de la cybersécurité est depuis quelques années en pleine croissance. Une étude menée à l'échelle européenne fait état d'une croissance de 8 % entre 2020 et 2021 pour un marché d'environ 34 milliards d'euros. Le business de la cybersécurité devrait atteindre, selon les prévisions, les 45 milliards d'euros en 2025. Le niveau de menace n'a jamais été aussi fort au regard du contexte géopolitique, marqué par de nombreuses offensives d'origine russe visant à perturber les systèmes d'information les processus électoraux en cours. Pour autant, la cybersécurité ne représenterait actuellement que 3 % du marché du numérique. Et même si le secteur progresse rapidement, ce faible ratio montre que les entreprises ne consacrent encore qu'une faible part de leur budget pour renforcer leur sécurité.

Pourtant, le niveau de menace se maintient à un niveau très élevé au regard des attaques enregistrées par l'Anssi. Au total, en France, 143 attaques par rançongiciel ont fait l'objet d'un dépôt de plainte en 2023, soit 34 de plus que l'année précédente, constituant une progression de 31 %. Cette vision ne définit pas le panorama complet de la menace. En effet, encore beaucoup d'organisations passent sous silence les cyberattaques dont elles ont pu être victimes pour préserver leur image auprès du public et de leurs clients. Cette trajectoire traduit une tendance de fond qui permet d'évaluer une hausse continue de la menace et de l'élargissement de son spectre, auprès des organisations publiques (collectivités, hôpitaux, etc.) et des petites entreprises, qui constituent des cibles privilégiées car souvent impréparées au risque cyber.

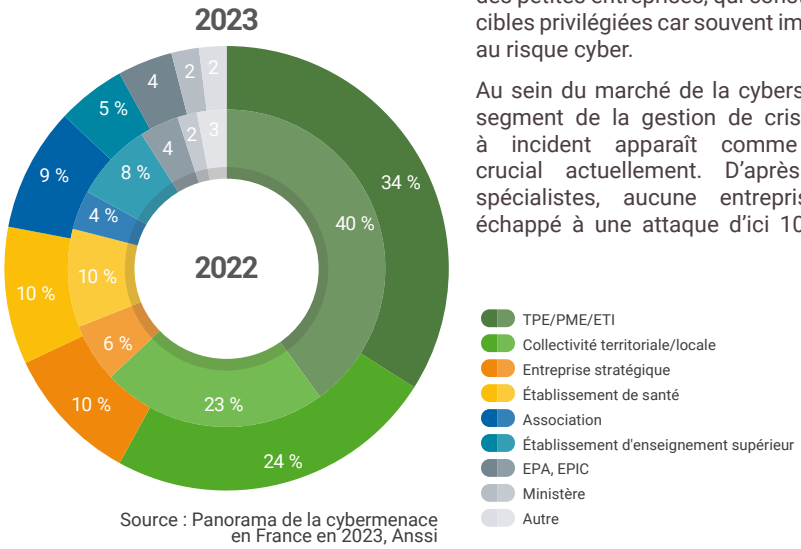
Au sein du marché de la cybersécurité, le segment de la gestion de crise/réponse à incident apparaît comme le plus crucial actuellement. D'après certains spécialistes, aucune entreprise n'aura échappé à une attaque d'ici 10 ans. Les petites et moyennes entreprises demeurent la principale catégorie d'acteurs concernée par les attaques par rançongiciel (34 % du volume d'attaques), mais leur représentativité a diminué de 7 points par rapport à 2022, selon le panorama de la cybermenace réalisé par l'Anssi. Les attaques à l'encontre des organisations publiquent demeurent à un niveau élevé. Près d'un quart (24 %) concernent les collectivités territoriales, 10 % des compromissions sont à l'encontre des établissements publics de santé et 5 % concernent les établissements de l'enseignement supérieur. Enfin, les associations (+5 points) et les entreprises stratégiques (+4 points) constituent des cibles privilégiées des cybercriminels.

Comparaison des signalements d'attaques par rançongiciel en 2022 et 2023



Source : Panorama de la cybermenace en France en 2023, Anssi

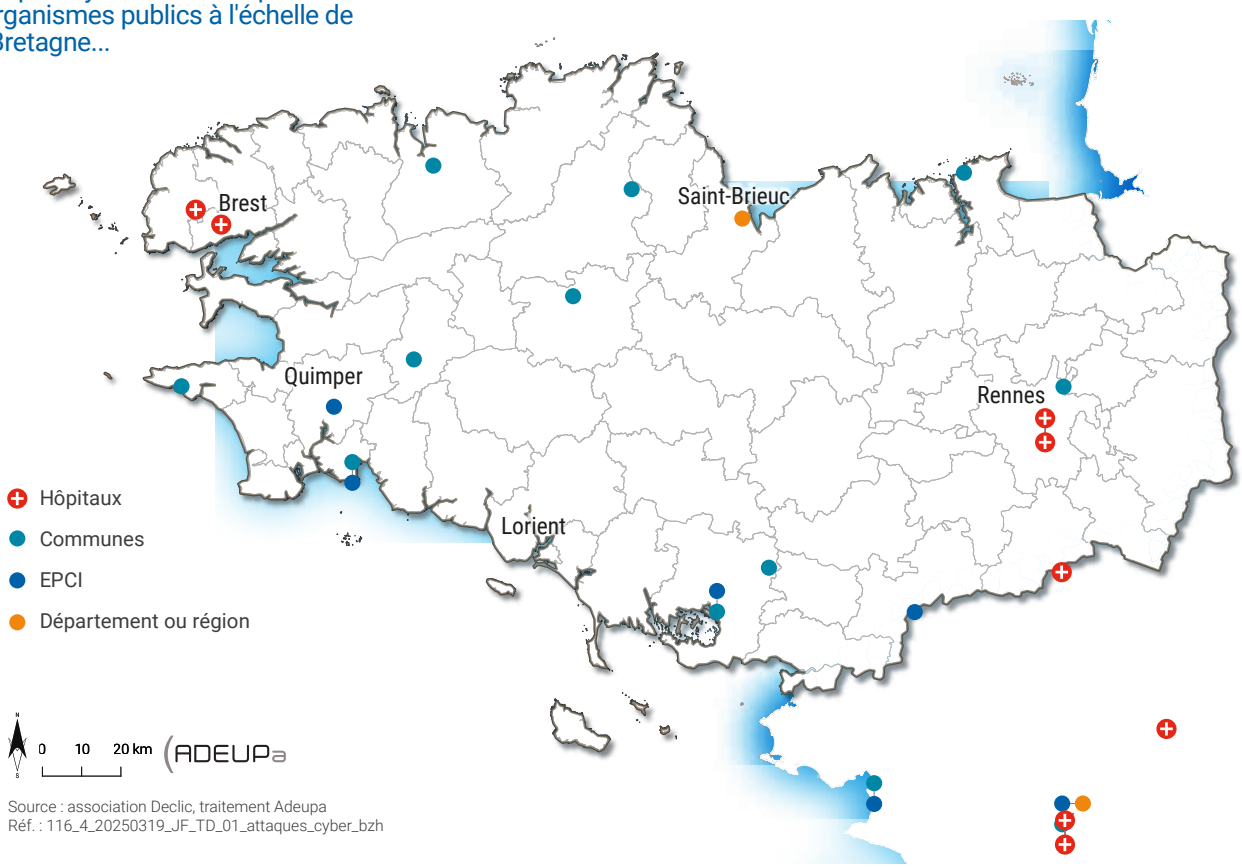
Répartition des victimes d'attaque par rançongiciel



Source : Panorama de la cybermenace en France en 2023, Anssi

> D'après certains spécialistes, aucune entreprise n'aura échappé à une attaque d'ici 10 ans.

Attaques cybersécurité auprès d'organismes publics à l'échelle de la Bretagne...

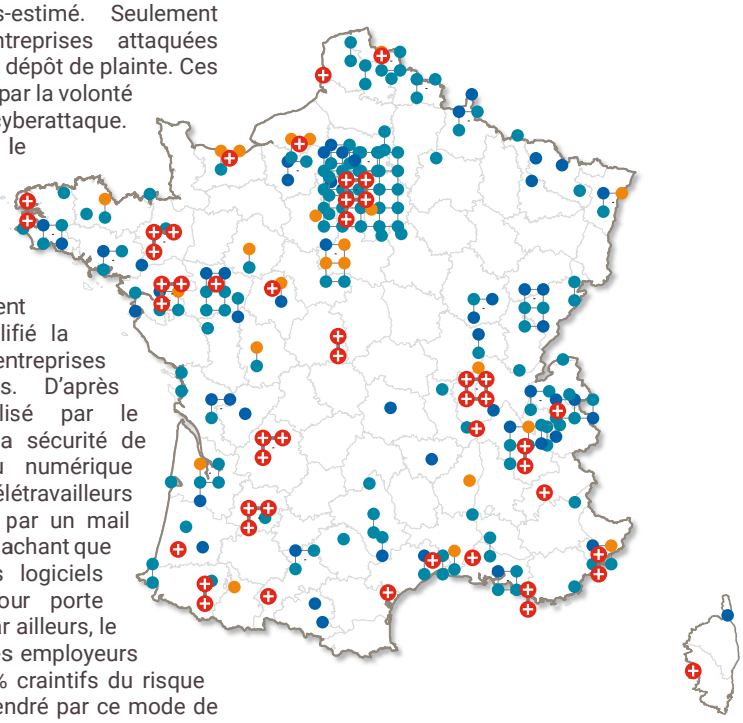


Source : association Declic, traitement Adeupa
Réf. : 116_4_20250319_JF_TD_01_attaques_cyber_bzh

L'association Declic est un réseau fondé en 2005 par et pour les collectivités et les établissements publics de France. Son objectif est de partager l'information et de mettre en commun les outils en lien avec l'informatique. Depuis 2019, elle fait aussi l'inventaire des cyberattaques ayant touché les établissements publics. Au total, 239 d'entre eux en ont été victimes dont 8 en Finistère. En 2020, le bailleur social Finistère Habitat a été victime d'un rançongiciel. Parmi les collectivités locales, les mairies de Primelin, Laz, Morlaix et la CC du Pays fouesnantais ont subi des cyberattaques de diverses natures comme l'utilisation d'un rançongiciel, la fraude à la fausse facture, la neutralisation du parc informatique ou encore le piratage de sites internet. En 2023, l'hôpital de Saint-Renan et surtout le Centre hospitalier universitaire (CHU) de Brest ont subi des tentatives d'intrusion. S'ils ont été assez prompts pour empêcher le vol de données, les différents services ont fonctionné de manière dégradée. Enfin, dernièrement, la scène nationale du Quartz, gérée par la société d'économie mixte Brest'aim, s'est fait voler les données personnelles de 60 000 clients.

Le spectre de la menace est, par conséquent, grandissant et reste d'ailleurs probablement sous-estimé. Seulement la moitié des entreprises attaquées s'engagerait dans un dépôt de plainte. Ces chiffres s'expliquent par la volonté de dissimuler une cyberattaque. Depuis le covid, le déploiement du télétravail et, de fait, l'usage généralisé des outils numériques dans un environnement domestique, a amplifié la vulnérabilité des entreprises face aux attaques. D'après le baromètre réalisé par le Club d'experts de la sécurité de l'information et du numérique (Cesin), 47 % des télétravailleurs auraient été piégés par un mail frauduleux en 2022, sachant que quasiment tous les logiciels malveillants ont pour porte d'entrée un email. Par ailleurs, le télétravail inquiète les employeurs qui se disent à 82 % craintifs du risque supplémentaire engendré par ce mode de travail sur les systèmes d'information.

... et à l'échelle française



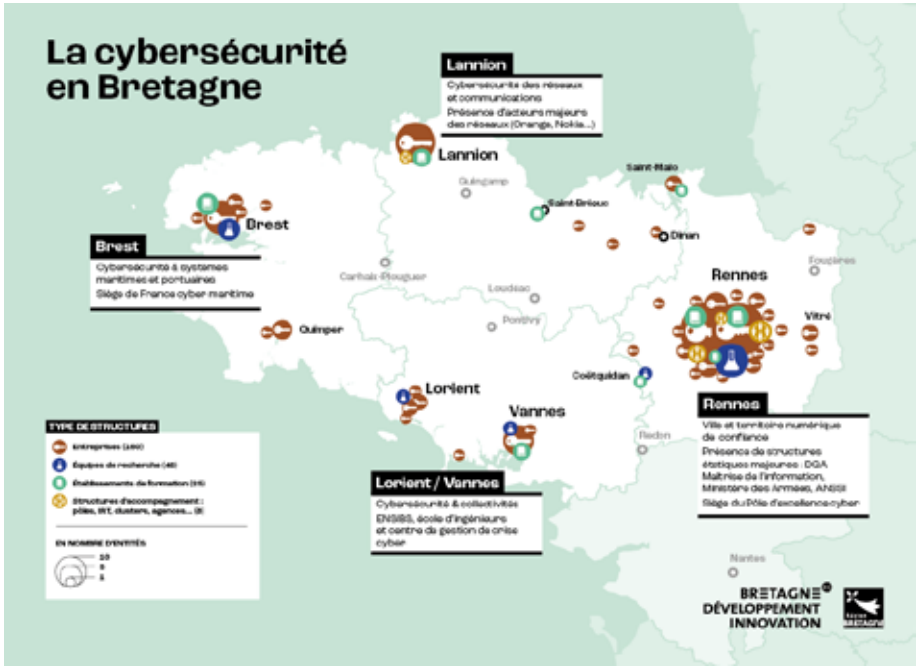
Une montée en puissance de l'écosystème breton

En Bretagne, on estime que l'écosystème de la cybersécurité représente 8 000 emplois répartis au sein de 170 entreprises. La région concentre environ le quart des emplois de la filière cybersécurité en France et génère 1 milliard d'euros de chiffre d'affaires, ce qui la place en deuxième position sur le plan national. Elle forme aussi chaque année 3 500 étudiants.

Depuis 2014, la Région Bretagne consolide ses ressources pour devenir une région leader en matière de cybersécurité. Le Pôle d'excellence cyber (PEC), piloté par le ministère des Armées et la Région Bretagne, constitue sans doute l'une des premières pierres de le stratégie régionale. Portée justement par le PEC, l'European cyber week figure désormais comme l'un des rendez-vous incontournables de la cybersécurité depuis 2016 en Europe, aux côtés de l'Incyber (ex-forum international de la cybersécurité à Lille). La création du commandement de la cyberdéfense (comcyber) en 2019 participe également du renforcement des compétences sur le territoire, sous l'angle de la cyberdéfense. Depuis 2023, la création d'un site de l'Anssi à Rennes renforce la présence institutionnelle de la cybersécurité en Bretagne.

Plusieurs démarches de grande ampleur se déploient progressivement depuis quelques années :

- Un programme « les cadettes de la cyber » à destination des femmes basé sur le mentorat et le parrainage afin d'accompagner les femmes vers les métiers de la cybersécurité.
- La mise en oeuvre d'un baromètre cyber breton, complémentaire au panorama de la menace cyber produit par l'Anssi, qui vise à analyser l'étendue de la menace cyber en Bretagne par l'intermédiaire d'une enquête réalisée auprès des entreprises.



La Région s'est également dotée, depuis la fin d'année 2024, d'un centre de réponse à incident visant à apporter des premières solutions aux entreprises et aux collectivités victimes de cyberattaques.

De manière plus englobante, la Bretagne aspire à devenir la première région en ce qui concerne la formation d'étudiants. Le programme Cyberskill4all, doté de 23 M€ dont 40 % financé par l'État dans le cadre de France 2030, porte l'ambition de sensibiliser 80 000 lycéens aux enjeux de la cyber et de former 15 000 étudiants dont 4 000 spécialistes. Afin de soutenir l'effort, de nombreux modules de formation seront créés.

Enfin, la Région matérialise la création d'un campus cyber breton dont l'ambition sera de conduire l'ensemble des entreprises dans une trajectoire de cybersécurisation et de soutenir l'ensemble de l'écosystème d'innovation et de recherche.

2002 — Création de Diateam

2014 — Création du Pôle d'excellence cyber
Création de la chaire cyberdéfense des systèmes navals entre l'École navale, Naval Group, Thales et IMT Atlantique, avec le soutien de la Région Bretagne et sous le patronage du Pôle d'excellence cyber

2015 — Inauguration du Centre support de cyberdéfense (CSC) de la marine nationale, l'un à Brest, l'autre à Toulon

2016 — Première édition d'Unlock Your Brain Harden your System organisée par Diateam et la cantine numérique de Brest

2017 — Création du Groupement des acteurs en cybersécurité (Gacyb) par la CCI Finistère

2019 — Implantation du Commandement de la cyberdéfense (Comcyber) à Rennes

2020 — Création de France cyber maritime à Brest

2022 — Transfert du siège de SourcITEC à Brest
Première édition du Breizh Cyber Show organisée par le Gacyb
Le groupe Asten crée son pôle cybersécurité, pour valoriser ses missions de cyberprotection défensive et offensive menées auprès de ses clients

2023 — Mise en place du centre de réponse à incident Breizh Cyber
Organisation de l'ISTC à Brest par l'IMT Atlantique, symposium qui réunit les meilleurs spécialistes mondiaux du codage

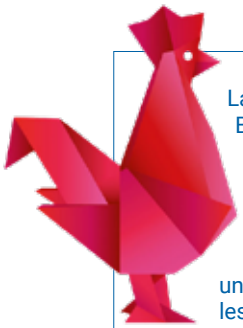
2024 — Lancement officiel du campus Bretagne cyber alliance
BZHunt participe à la sécurisation des infrastructures informatiques des Jeux olympiques de Paris

Une dynamique croissante dans la métropole brestoise

La métropole brestoise constitue l'une des principales polarités de la région en termes de compétences en cybersécurité. En 2025, le cœur de la filière cybersécurité est composé de 8 entreprises employant 123 salarié·es. Cela fait de l'écosystème brestois un noyau très resserré de spécialistes de la cybersécurité. Il peut aussi être caractérisé de « naissant » dans la mesure où la moitié des entreprises qui le composent ont été créées ou se sont implantées au sein de la métropole brestoise durant les 5 dernières années. Les premières traces de cyberactivité remontent au début des années 2000 avec la création de Diateam et d'Asten, même si cette dernière n'a réellement déployé des compétences en cybersécurité que plus tardivement.

Le dynamisme local en cybersécurité s'est donc exprimé, ces dernières années, par la création de nouvelles entreprises comme Aucae, Frogi Secure ou Watoo.

Ces entreprises ont pour point commun d'avoir bénéficié d'un environnement favorable de mise en réseau et d'accompagnement composé entre autres des incubateurs de l'IMT Atlantique, Emergys (Technopôle Brest-Iroise) et du Village by CA.



La French Tech Brest Bretagne Ouest a été identifiée pour être un lieu totem de la cybersécurité au travers du label « Bretagne Cyber Alliance », il deviendra un point de référence pour les initiatives et événements liés à la cybersécurité, permettant ainsi de renforcer le rayonnement de la métropole brestoise au sein du réseau régional et national des campus cyber.

Au global, le cœur de filière a progressé de 48 emplois durant les 5 dernières années, ce qui représente une croissance significative de 64 %. Les récentes créations de startups ont contribué, pour la moitié, à cette dynamique d'emploi, à l'instar de BZHunt qui a connu une croissance très rapide grâce à son positionnement spécifique sur le segment du hacking éthique et in extenso dont la portée est internationale. Le transfert du siège de l'entreprise SourciTEC (10 salarié·es) de Paris à Brest en 2019 a également participé au renforcement de l'offre dans le domaine de la sensibilisation et de la mise en place d'une gouvernance en cybersécurité dans les organisations.

L'héritage maritime de la métropole brestoise et la récente structuration de son écosystème en cybersécurité identifient aujourd'hui le territoire pour son expertise en cybersécurité maritime. Celle-ci se définit par une excellence de la recherche appliquée à des thématiques orientées vers le domaine maritime telles que la dronisation, les communications sous-marines, le spatial… Elle existe également au travers d'une forte densité d'acteurs économiques et institutionnels qui interviennent dans le champ du maritime. La création de l'association France cyber maritime en 2020, dont le rayonnement est national, a permis d'ancrer encore davantage la singularité brestoise en la matière. À Brest, la mer revêt aussi un caractère dual, au regard de la présence de la marine nationale. La métropole héberge au sein de la préfecture maritime de nombreuses compétences de la sécurité et sûreté maritime à l'instar du centre de support de cyberdéfense (CSC), le centre de niveau mondial dédié à la sûreté maritime « Maritime information cooperation & awareness center » (Mica Center) ou encore le centre de contrôle de la corne africaine « Maritime security center Horn of Africa » (MSC-HOA).

Les PME déjà établies dans le paysage ont continué de renforcer leur activité au gré des besoins du marché, comme Diateam dont la majeure partie de l'activité se fait au service des ministères des Armées européens et des opérateurs d'intérêt vital[2] (OIV). Malgré une activité résolument tournée vers l'international et un rachat progressif à partir de 2022 par le groupe italien Cy4gate, Diateam se positionne, de plus en plus, en collaboration avec les autres acteurs brestois, sur une offre de réponse à incidents à destination d'entreprises locales. De son côté, Asten a consolidé sa position à Brest et se développe aussi en France et à l'international, employant aujourd'hui plus de 140 salarié·es dans l'ensemble du groupe.

Malgré des univers et des champs d'intervention relativement différents d'une entreprise à l'autre, les prestataires présents sur le territoire se singularisent par leur expertise dans les domaines du maritime et de la santé. Le groupe Prorisk s'est, par exemple, spécialisé dans la sûreté maritime et portuaire. Il couvre l'ensemble des besoins en cybersécurité, depuis le conseil et la formation jusqu'à la gestion de crise. Diateam, BZHunt et SourciTEC sont aussi en mesure de proposer des solutions spécifiques aux utilisateurs du domaine maritime, et sont d'ailleurs identifiés au sein du collège « solutions » de l'association France cyber maritime.

Dans le domaine de la santé, le territoire présente une activité de recherche relativement intense et atypique, qui donne lieu à de l'essaimage. La création de la startup Watoo, spécialisée dans le tatouage de données, montre la capacité des forces brestoises à faire émerger des projets autour des données de santé conçus sur des innovations en cybersécurité, robustes et de confiance. Autre exemple, l'entreprise Medecom s'est aussi développée sur principe de cryptage des données issues des imageries médicales.

2. Notion introduite par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019. Elle concerne les entités en charge de la protection d'installations d'importance vitale notamment dans le secteur de la Défense, adressant un secteur d'importance vitale ou présentant un potentiel danger pour la population. Les OIV sont désignés par leur ministère de rattachement. La liste de ces entités est confidentielle.

DES CHAMPIONS DE LA CYBERSÉCURITÉ AU SEIN DE LA MÉTROPOLE BRESTOISE

Diateam et BZHunt se distinguent comme les principaux représentants du domaine de la cybersécurité sur le territoire. Leur rayonnement à l'international, voire au niveau mondial, entraîne également dans son sillage la notoriété de la place brestoise et le développement futur de la filière localement.

BZHunt est une entreprise de cybersécurité offensive. L'essentiel de son activité consiste à réaliser des tests d'intrusion dans les systèmes d'information. Par ailleurs, la jeune startup brestoise s'est spécialisée dans le « bug bounty » qui est une sorte de chasse à la prime (parfois très lucrative) organisée par des entreprises clientes auprès de hackers éthiques pour qu'ils trouvent les failles informatiques. BZHunt est l'une de rares entreprises françaises à répondre à ce genre de demandes et dispose d'une expertise reconnue à l'occasion de compétitions internationales remportées telles que les championnats du monde du bug bounty en 2022, ou pour avoir participé à des événements dans le cadre des Jeux olympiques de Paris 2024. Par sa capacité à intervenir en moins de 48h sur l'ensemble du globe, BZHunt s'est constitué une clientèle d'abord internationale, entraînant un rythme de croissance exponentiel sur ses deux premières années d'existence. L'entreprise bénéficie toutefois d'un nombre important de clients locaux mais qui relèvent plutôt de petits contrats, qui pèsent finalement assez peu dans son chiffre d'affaires.

Diateam est l'un des pionniers de la cybersécurité sur le territoire. Depuis 2002, l'entreprise opère depuis Brest et répond aux besoins des États et aux ministères des Armées de différents pays qui font l'objet de besoins en sécurisation. De fait, Diateam s'ouvre naturellement sur l'export. C'est aussi et surtout un laboratoire de la cybersécurité puisque plus de la moitié du temps humain est consacré à la recherche et au développement. Cela a permis à l'entreprise de développer des compétences rares sur les segments de la simulation d'attaques, grâce à l'utilisation de jumeaux numériques capables de reproduire virtuellement l'infrastructure numérique. Malgré une relative ancienneté, elle renforce continuellement ses effectifs qui ont presque triplé ces dix dernières années. Son rachat en 2022 par le groupe italien de cybersécurité offensive Cy4gate n'a pas entravé son ancrage au territoire puisque Diateam co-organise l'événement Unlock your brain, harden your system conjointement avec la cantine numérique. En 2024, Diateam a également équipé l'IUT de Lannion ainsi que l'Enssat en cyberrange pour permettre aux étudiants de développer leurs compétences en cybersécurité par la simulation de conditions quasi réelles de crise.

Un rôle crucial et en devenir des entreprises de services numériques

Dans un périmètre plus large figurent les entreprises de services numériques. Ces dernières détiennent des compétences pour mettre en place un premier niveau d'hygiène informatique qui relève de l'infogérance. Sans être spécialistes, elles s'avèrent cruciales dans le jalonnement progressif des entreprises dans un parcours de cybersécurisation. Leur rôle est amené à se renforcer en vue de la nouvelle directive Network and Information Security 2 (NIS2).

En parallèle, coexistent des entreprises « intégratrices » dont l'activité principale est connexe à la cybersécurité ou fortement numérisée. Ces dernières ont des besoins ciblés en cybersécurité pour des usages très variés comme le développement de logiciels pour les systèmes embarqués ou pour des applications de visioconférence.

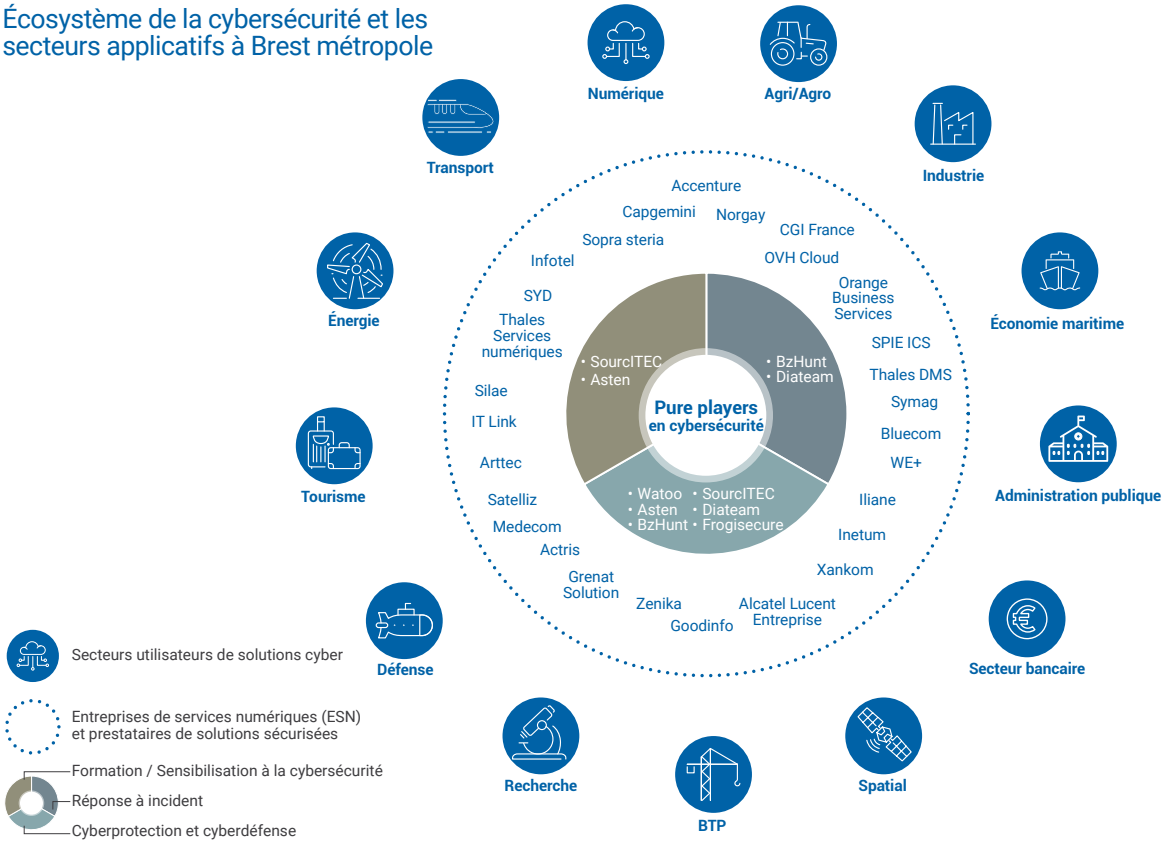
Principales entreprises de services numériques présentes dans Brest métropole (hors pure players)

Entreprises	Effectifs 2024
Infotel conseil	117
Capgemini technology services	110
Norgay	105
Accenture	100
Symag	91
Thales services numeriques sas	70
Asi / Asi informatique	64
Cgi france	55
Sopra steria group	55
E-learning touch'	37

Source : Fichier RCS CCI – Enquête Adeupa

Photo : ©France Cyber Maritime

Écosystème de la cybersécurité et les secteurs applicatifs à Brest métropole



Il y a enfin un halo encore plus large qui regroupe les acteurs qui internalisent des fonctions de cybersécurité. Ces entreprises ne font pas partie de la filière à proprement parler puisqu'elles présentent un profil d'utilisateur ou de client. Toutefois, à partir d'une certaine taille critique au regard d'enjeux internes, certaines entreprises manifestent le besoin de garder, en propre, une direction des systèmes d'information (DSI) ou un responsable de la sécurité des systèmes d'information (RSSI) afin de manager in situ les équipes aux enjeux de cybersécurité.

Des qualifications et certifications comme clé d'entrée sur le marché

Les certifications et qualifications, notamment celles délivrées par l'Anssi, marquent une reconnaissance par l'État de la qualité d'un produit ou d'un service. La détention de ces labels est, en général, un critère discriminant pour obtenir de nouveaux marchés sur le sol national, mais aussi à l'étranger. Toutefois, leur obtention requiert un haut niveau de qualité et des délais parfois longs qui peuvent mettre en difficulté les entreprises en cours de labellisation, mais encore peu visibles pour leurs potentiels clients.

Prestataires d'audit de la sécurité des systèmes d'information (Passi)

La qualification Passi s'adresse aux entreprises qui souhaitent certifier leurs prestations d'audit pour les activités suivantes : audit d'architecture, audit de configuration, audit de code source, tests d'intrusion, audit organisationnel et physique.

Entreprises locales certifiées : Accenture security ; Apixit ; Capgemini/Sogeti ; Capgemini Technology Services ; CGI France ; Sopra Steria infrastructure et security services ; Nokia Networks France ; Scalian ; SPIE ICS.

Prestataires de réponse aux incidents (Pris)

La qualification Pris est primordiale dans le contexte d'augmentation des cyberattaques. Elle qualifie le degré de technicité des entreprises dans la gestion et la réponse aux incidents.

Entreprises certifiées : Sopra Steria infrastructure et security services.

Prestataires de détection d'incidents de sécurité (PDIS)

La qualification PDIS met en lumière les capacités de détection des incidents de sécurité.

Entreprises certifiées : Capgemini Technology Services ; Sopra Steria infrastructure et security services.

ISO 27001:

La norme ISO 27001 vise à protéger la confidentialité, l'intégrité et la disponibilité des informations en appliquant une approche de gestion des risques. La certification ISO/IEC 27001 démontre l'engagement d'une organisation envers la sécurité de l'information et peut servir de facteur de différenciation sur le marché.

Entreprises certifiées : Thales services numériques ; Sopra Steria infrastructure et security services ; Asten Cloud ; Iliane.

Hébergeur de données de santé (HDS)

Le décret n°2018-137 du 26 février 2018 prévoit de garantir la sécurité de l'hébergement des données de santé. Ce référentiel a été revu en 2022 afin de renforcer la souveraineté des données, de clarifier les distinctions avec SecNumCloud[3] et de tenir compte des évolutions de la norme ISO 27001. Il existe à l'heure actuelle environ 300 acteurs certifiés en France sur une ou plusieurs des 6 activités :

- La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé.
- La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.
- La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information.
- La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé.
- L'administration et l'exploitation du système d'information contenant les données de santé.
- La sauvegarde de données de santé.

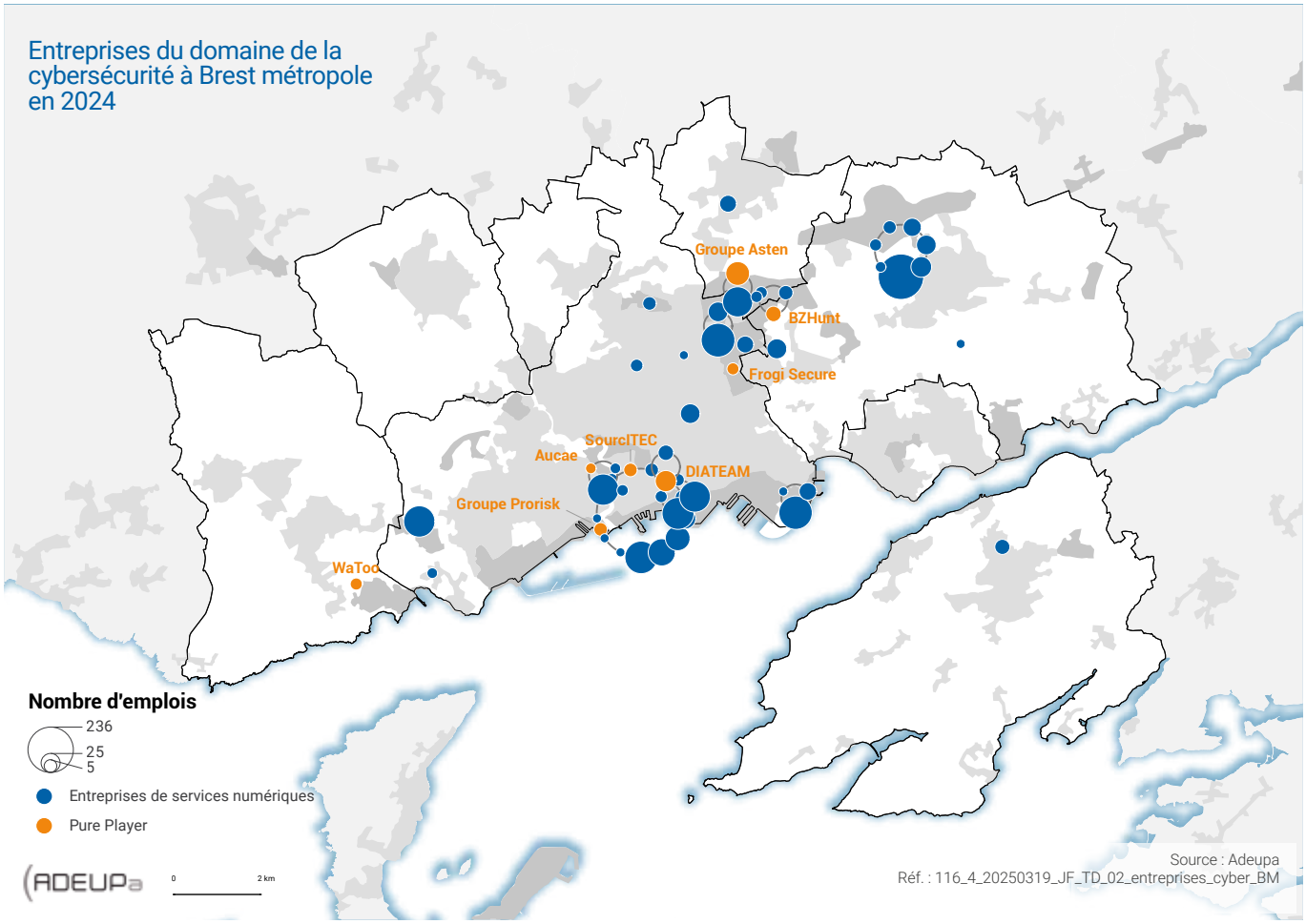
Au sein de la métropole brestoise, plusieurs acteurs ont obtenu la certification mais peu d'entre eux ont leur siège en local : Inetum (ex GFI informatique), Sopra Steria, Vivalto santé services partagés, Thales services numériques, OVH, CGI France, Capgemini TS, Asten, Alcatel Lucent Entreprise, Accenture LLP.

France cybersecurity est un label dont la gouvernance est assurée par un collège étatique (DGA, DGE, Anssi), un collège industriel et un collège utilisateurs. Il vise à certifier, pour une durée d'un an renouvelable, de la qualité des produits (logiciels, services, conseils) mis sur le marché et qui sont conçus et administrés depuis la France. À ce jour, plusieurs offres du territoire ont été labellisées comme Edocsafe, solution de coffre-fort numérique fournie par la société Edocgroup, le HNS platform cyber range, outil de simulation de cyberattaques produit par Diateam.

Au sein de la métropole brestoise, plusieurs acteurs ont obtenu la certification mais peu d'entre eux ont leur siège en local.

3. Qualification délivrée par l'Anssi auprès des opérateurs cloud répondant à un certain nombre de critères et de bonnes pratiques en termes de cybersécurité

Entreprises du domaine de la cybersécurité à Brest métropole en 2024



Source : Adeupa
Réf. : 116_4_20250319_JF_TD_02_entreprises_cyber_BM

Certifications et labels en cybersécurité détenus par les entreprises présentes à Brest métropole

	Passi	PRIS	PDIS	ISO 27001	HDS	France Cyber-security
Accenture	x				x	
Capgemini	x				x	
CGI France	x				x	
Sopra Steria	x	x	x	x	x	
SPIE ICS	x					
Thales Services Numériques				x	x	
Asten Cloud				x	x	
Iliane				x		
Inetum					x	
OVH Cloud					x	
Alcatel Lucent Entreprise					x	
Edoc Group						x
Diateam						x

Une pénurie de talents

De nombreuses études, à commencer par le recensement des offres d'emploi en cybersécurité produit par l'Anssi, estiment à 15 000 le nombre de postes ouverts mais non pourvus en France, dont 5 % en Bretagne soit environ 750 à 800 offres. L'écart entre les besoins du marché et la main-d'œuvre disponible pourrait rapidement s'accentuer au regard de la croissance rapide de la menace et des exigences formulées par les différentes directives amenées à entrer en vigueur dans les mois à venir. L'inadéquation entre les formations et les besoins concrets des entreprises entrave aussi l'insertion professionnelle.

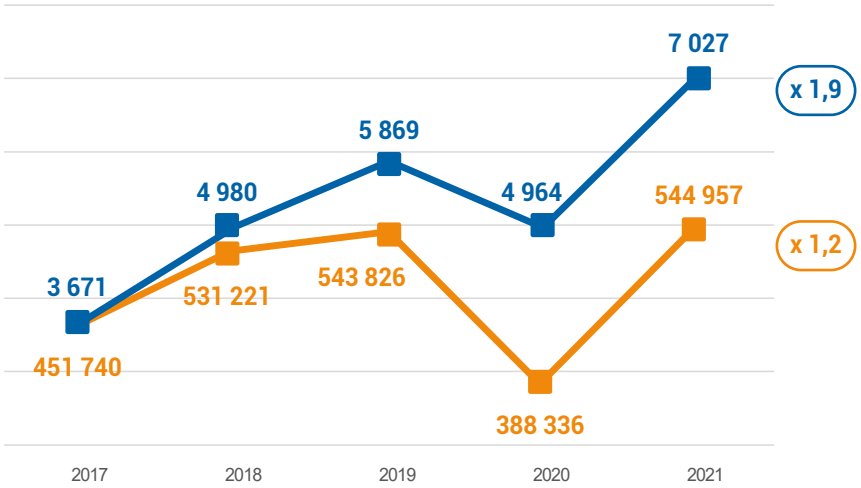
L'essor de la filière cybersécurité en Bretagne expose le territoire directement à ces difficultés de recrutement. Une étude[4] réalisée par l'Association pour l'emploi des cadres (Apec) montre à quel point la tension s'est renforcée. Entre 2017 et 2021, le volume d'offres en cybersécurité a presque doublé, passant de 3 671 à 7 027. Ces besoins ont, comparativement à l'ensemble des offres à destination des cadres, progressé de manière beaucoup plus rapide. Cette dynamique est largement portée par le tissu d'ESN, particulièrement dense sur le périmètre breton. En volume d'offres, la Bretagne n'apparaît que comme la 5e région française, loin derrière l'Île-de-France qui cumule la moitié des besoins de recrutement mais à un niveau relativement proche d'autres régions comme Auvergne-Rhône-Alpes, Occitanie ou Provence-Alpes-Côte d'Azur. Mais en termes de poids de la cybersécurité dans l'ensemble des offres d'emploi, la Bretagne se place en chef de file avec 2,8 % d'offres en cybersécurité[5], devant l'Île-de-France (1,9 %) et l'Occitanie (1,5 %).

4. Cybersécurité : un marché de l'emploi cadre diversifié et de plus en plus porteur

5. Moyenne nationale (1,3 %)

L'essor de la filière cybersécurité en Bretagne expose le territoire directement à ces difficultés de recrutement.

Évolution du nombre d'offres d'emploi cadre en cybersécurité , en comparaison de celui du total des offres (base 100 en 2017*)



* Hors offres doublons et partenaires - Source : Apec Bretagne, périmètre Bretagne

En 5 ans, le nombre d'offres d'emploi cadre en cybersécurité a quasiment doublé

De multiples facteurs de difficultés de recrutement

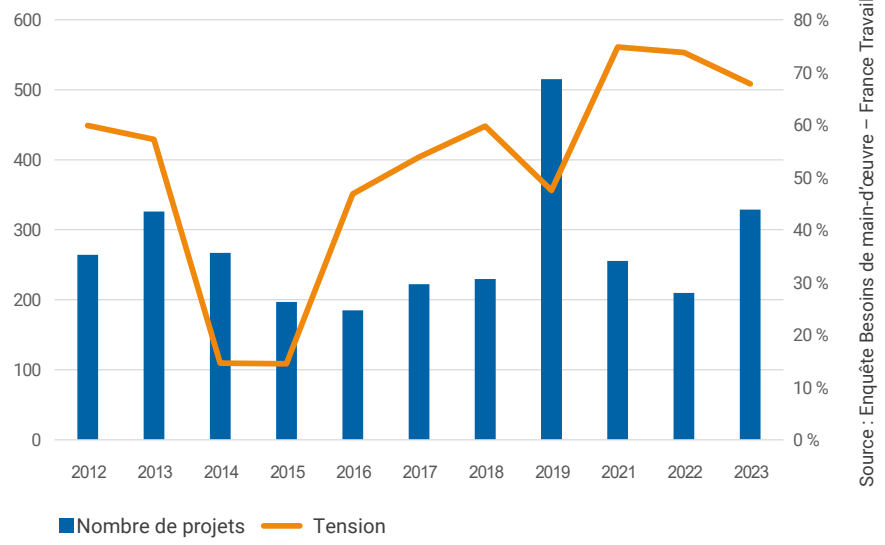
Plus localement, l'enquête portant sur les besoins de main d'œuvre, réalisée par France Travail, permet de faire également le constat d'une hausse tendancielle des recrutements et des difficultés d'embauche pour les métiers[6] ayant un lien avec la cybersécurité.

Dans l'ensemble, les projets de recrutement ont été stables jusqu'en 2018 avec en moyenne 240 intentions d'embauches par an dans le pays de Brest. L'année 2019, pré-covid, a fait état d'une explosion des besoins avec plus de 500 projets. Cette dynamique a été perturbée par la crise sanitaire, au vu des millésimes 2021 et 2022 qui se sont inscrits dans la moyenne des exercices précédents. Toutefois, en 2023, les entreprises semblent avoir remis un coup d'accélérateur sur les procédures d'embauche (328 projets), soit une hausse de 56 % par rapport à l'année précédente.

La tension s'est, quant à elle, aussi renforcée durant les dix dernières années. Malgré un léger tassement en 2022 puis en 2023, elle a atteint un pic de 75 % en 2021. Autrement dit, pour 4 projets de recrutement formulés par les entreprises, 3 sont jugés comme difficiles. Comparativement à la tension relative à l'ensemble des projets de recrutements recensés sur le territoire, les métiers de l'informatique font l'objet de davantage de difficultés.

Outre l'intensité d'embauche et le manque de lisibilité de l'offre de formation, les difficultés peuvent s'expliquer par une mauvaise explicitation des compétences dans les offres d'emploi. Les ESN peuvent éprouver des difficultés à qualifier leurs besoins tandis que les pure players sont parfois peu visibles auprès des agrégateurs d'offres. Par ailleurs, l'attractivité des métiers de la cybersécurité est très variable. Une grande partie des jeunes diplômés aspirent à faire du « hacking éthique », pentest, etc. au détriment de métiers de la gouvernance, risque et conformité (GRC) pour lesquels l'appétence est bien plus faible. Le manque de diversité des profils apparaît aussi comme un point faible de la filière.

Évolution du nombre de projets et de la difficulté à recruter dans les métiers de l'informatique au sein du pays de Brest entre 2012 et 2023



Seulement 14 % des professionnels sont des femmes[7].

Il y a enfin les métiers connexes comme économiste, juriste ou chargé de communication de la cybersécurité qui pâtissent d'une visibilité très réduite.

Une offre de formation relativement riche, mais peu spécialisée

La métropole brestoise dispose d'une offre de formation en lien avec la cybersécurité relativement large. Au total, une vingtaine de formations intègrent a minima des notions de sensibilisation à la cybersécurité et, pour les plus pointues, un niveau de maîtrise, voire de spécialisation dans le domaine.

La plupart des formations certifiées en France, notamment en Bretagne, se situent dans les établissements de l'enseignement supérieur et de la recherche qui coopèrent avec ceux de la métropole brestoise comme l'Université de Bretagne Sud (UBS) ou l'École nationale supérieure des sciences appliquées et de technologie (Enssat) de Lannion. Ils dispensent de nombreuses formations telles que les différents parcours du master Ingénierie des systèmes complexes de l'UBS les différents parcours du diplôme d'ingénieur de l'école nationale supérieur d'ingénieurs de Bretagne-Sud et de l'UBS ; les parcours du diplôme d'ingénieur de l'Enssat à Lannion ; la formation continue « référent cybersécurité » de l'Enssat ; la formation continue « devenir référent cybersécurité en TPE/PME » de la CCI Bretagne.

Certaines formations dispensées à Brest font mention du terme « cybersécurité » à l'instar des BTS cybersécurité, informatique et réseaux, électronique (Ciel) proposés au lycée Vauban ou au sein du groupe scolaire La Croix Rouge, mais n'aspirent pas à former des spécialistes de la cybersécurité. La création, à la rentrée 2025, d'un parcours en collaboration avec la marine nationale devrait davantage colorer la formation sur le thème de la cyberdéfense. D'autres formations de niveau Bac +5 se rapprochent également d'un degré de spécialisation comme le parcours ingénieur de l'Isen Ouest après un parcours en cybersécurité, le master informatique de l'UBO co-accrédité avec l'IMT Atlantique, l'Enib et l'Ensta ainsi que le mastère professionnel manager en infrastructures et cybersécurité des systèmes d'informations au Cesi.

La formation continue apporte une offre complémentaire à la formation initiale. Elle accompagne la montée en compétences des salarié·es au sein de leur organisation et favorise la reconversion professionnelle. L'Afpa Bretagne, le Greta-cfa de Bretagne occidentale et le Cnam Bretagne proposent un certain nombre de formations en cybersécurité, allant du niveau bac+2 au bac+5 sur des métiers très variés (administration des réseaux, direction de projets cyber, conception de logiciels, etc). Le CNAM Bretagne dispose d'ailleurs du label Cyberedu, qui vise à apporter des prérequis en cybersécurité, pour les formations d'analyse en cybersécurité et de technicien·ne de maintenance micro réseaux et internet.

6. D'après le répertoire national des certifications professionnelles et en comparaison avec les familles professionnelles exploitées par France Travail, il est possible d'identifier 6 métiers liés à la cybersécurité : ingénieur et cadre d'études R&D informatique/chef de projet informatique ; ingénieur et cadre d'administration, maintenance informatique ; ingénieur et cadre des télécommunications ; employé et opérateur de l'informatique ; technicien d'études et développement informatique ; technicien de production et exploitation des systèmes d'information

7. Selon l'enquête 2023 portant sur « l'attractivité et la représentation des métiers de la cybersécurité vue par les professionnels » réalisée par l'Anssi

Un écosystème métropolitain de recherche très fort

La place brestoise se distingue comme l'un des principaux viviers de chercheurs dans le domaine de la cybersécurité après Paris, Grenoble et Rennes. L'étude réalisée par Allistene en 2017 faisait état d'une centaine de chercheurs sur le territoire, ce qui semble relativement stable ces dernières années. Les effectifs se concentrent principalement autour du Labsticc, qui compte environ 70 chercheur·euses, malgré une forte présence de quelques équipes dans le bassin lorientais. La montée en puissance du Latim dans sa dimension cybersécurité contribue à donner une coloration « santé » à l'écosystème local ; l'Irenav se spécialise, quant à lui, dans le champ d'application maritime. Enfin, l'Isen Ouest affiche une volonté de développement dans la cybersécurité avec des thèmes d'application très variés.

Malgré son importance, la communauté de chercheurs peine à interagir en interne avec les entreprises du territoire. Aussi, peu de travaux aboutissent à des créations de startups.

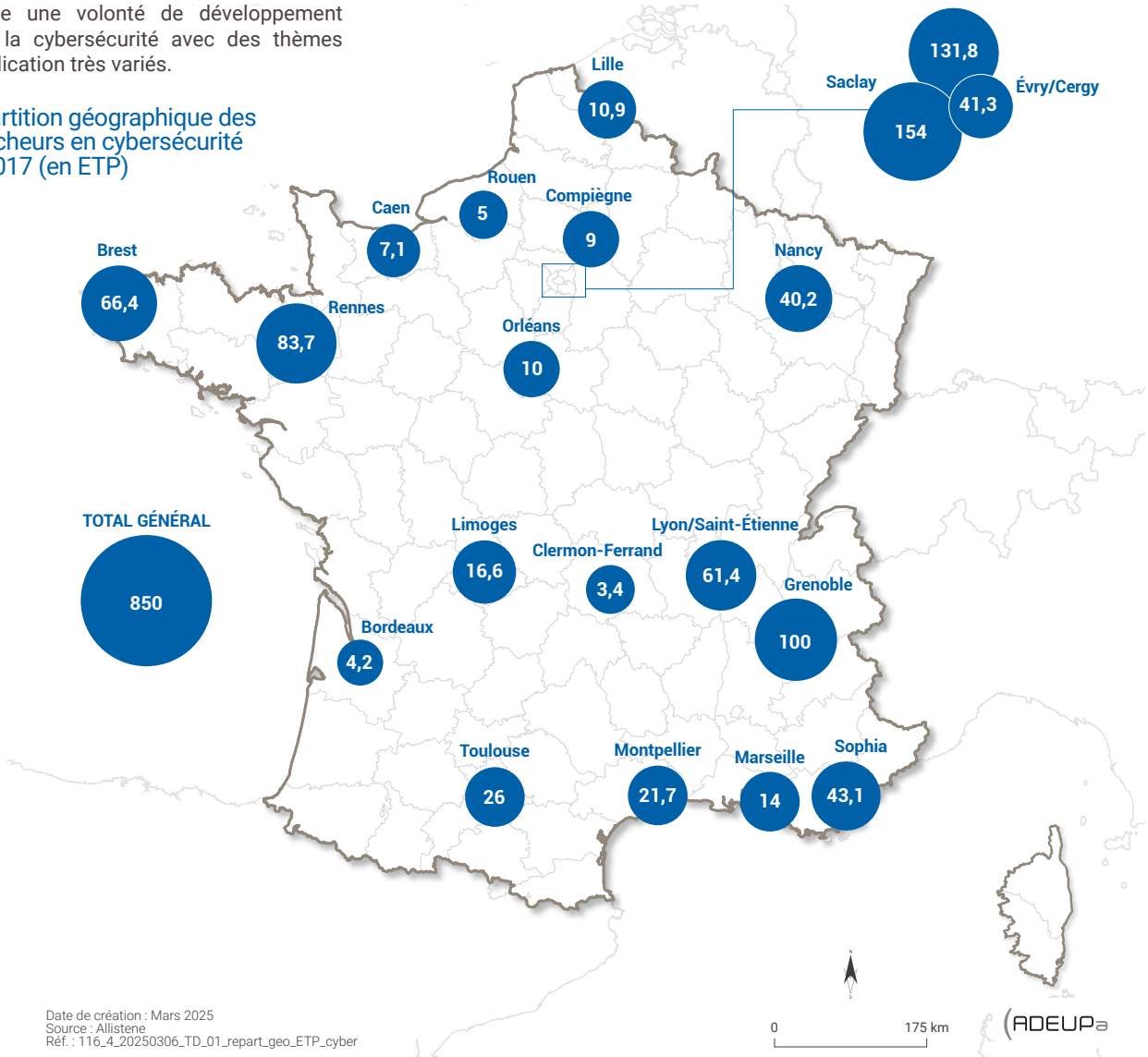
Labsticc : pivot de la recherche en cybersécurité à Brest

Le Labsticc est une unité de recherche mixte[8] dans le domaine de la cybersécurité. Il affiche une spécialisation élevée dans le domaine, au travers du programme transverse « cyber » qui rassemble 7 équipes de recherche du laboratoire. Pour certaines, comme l'équipe Fhoox[9] qui traite l'activité cognitive des professionnels durant les attaques ou l'équipe Iris qui travaille sur la sécurisation des systèmes critiques comme la distribution d'eau ou d'énergie, la thématique de la cybersécurité est au cœur de leurs travaux. Pour les autres, il s'agit davantage d'une couche appliquée à un autre domaine

8. Tutelle partagée entre 6 organismes : IMT Atlantique, ENIB, Ensta, UBO, UBS, CNRS

9. Équipe basée à Lorient

Répartition géographique des chercheurs en cybersécurité en 2017 (en ETP)



Date de création : Mars 2025
Source : Allistene
Réf. : 116_4_20250306_TD_01_repart_geo_ETP_cyber

(maritime, spatial, systèmes embarqués, intelligence artificielle). Malgré son caractère multisites, la majorité des forces de l'unité de recherche est concentrée à Brest. Cela représente plus de cinquante chercheurs, soit environ 60 % de l'ensemble des chercheuses et chercheurs en cybersécurité du territoire.

Malgré sa relative jeunesse, le laboratoire dispose d'un bon rayonnement international d'après l'évaluation réalisée par le Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur (Hcéres) en 2021. Il est d'ailleurs bien identifié sur des sujets d'actualité importants tels que l'intelligence artificielle, l'usine du futur et la cybersécurité. Sa notoriété lui permet de contractualiser de nombreuses thèses Cifre avec des grands groupes industriels tels que Nokia à Lannion, contribuant à la valorisation de la recherche par le transfert technologique.

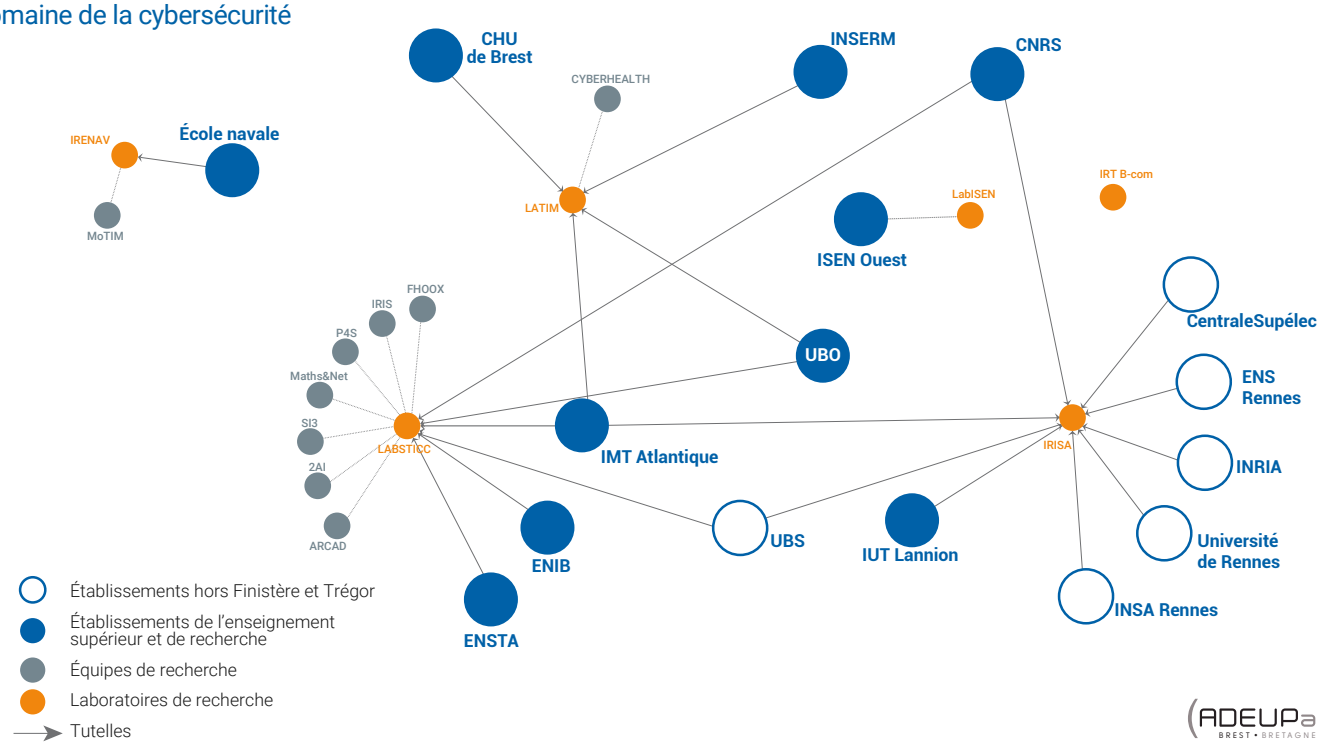
Latim : une compétence cybersécurité dans la santé

Le Latim (laboratoire de traitement de l'information médicale) est une unité de recherche partagée entre la faculté de médecine, le CHU de Brest et l'IMT Atlantique. Il est spécialisé dans le domaine de la santé avec une composante forte pour les sciences et technologies de l'information (traitement de l'information, imagerie, sécurité). Le laboratoire est labellisé Inserm et est reconnu comme très visible sur le plan international, notamment dans les domaines de la cybersécurité. Cette spécificité s'est d'ailleurs renforcée par la création, en janvier 2022, de l'équipe Cyberhealth (cybersecurity of externalized and mutualized healthcare data and processing), composée d'une dizaine de personnes. Il s'agit de la seule équipe de recherche française, positionnée sur le traitement et la sécurisation des données de santé, labellisée Inserm. Sa très forte orientation vers le transfert technologique lui ouvre des marchés auprès de grands groupes industriels. Le Latim a également été associé à la création de la chaire cybersécurité et IA de confiance en santé (Cybaile) en collaboration avec Thales, la startup Aiintense et l'entreprise Sophia Genetic qui conjugue des ambitions d'innovation dans les méthodes d'apprentissage sécurisées à grande échelle et de protection contre la falsification grâce à des systèmes d'IA fiabilisés. La reconnaissance de Brest dans ce domaine s'est matérialisée par la réception de l'international symposium on topics in coding en septembre 2023 (ISTC 2023), qui a rassemblé plusieurs centaines de chercheurs parmi les plus grands spécialistes du codage.

L'Irenav : la cyber dans le domaine maritime au service de la Défense

L'Institut de recherche de l'école navale (Irenav) est une unité de recherche placée sous la tutelle de l'école navale et qui développe des thématiques de recherche en lien avec les besoins de la marine nationale. L'équipe Modélisation et traitement de l'information maritime (Motim) s'est spécialisée dans l'approche numérique du milieu maritime au travers de l'acoustique sous-marine et de la science de la donnée (algorithmie et sécurisation). La cyberdéfense couvre une bonne partie des activités de l'équipe. Elle entretient des partenariats au sein de la chaire cyberdéfense des systèmes navals. Le rapport d'évaluation de l'Hcéres 2023-2024 qualifie d'« exceptionnel » le dynamisme de la chaire au regard des nombreux contrats industriels et des thèses Cifre qu'elle met en œuvre. L'implication de l'équipe dans les appels à projets européens et nationaux auxquels elle prend part, grâce notamment à son cyberrange, lui assure une reconnaissance importante dans le domaine.

Les unités de recherche dans le domaine de la cybersécurité



Des chaires pour consolider les synergies entre les acteurs privés et la recherche

La chaire cyberdéfense des systèmes navals développe, depuis plus de 10 ans et sa création en 2014, des travaux de recherche dans les domaines de la protection des équipements à bord des navires et de la formation spécifique à la cybersécurité maritime dans un contexte de forte autonomisation des navires, et donc d'augmentation du champ de vulnérabilité des systèmes embarqués. Elle s'inscrit dans un écosystème maritime et portuaire très dense et marqué par sa dualité civil/militaire, par la présence de la marine nationale, qui est à l'origine de la création de la chaire, des deux principaux industriels de la Défense présents à Brest (Naval Group et Thales), ainsi que de l'expertise des structures de l'enseignement supérieur et de la recherche du territoire (IMT Atlantique, Ensta, École navale).

La chaire Cyberlot est une démarche portée par l'université de Bretagne occidentale (UBO) par l'intermédiaire de l'Institut brestois du numérique et des mathématiques (IBNM) et appuyée par des unités de recherche (LMBA et Labsticc). Elle vise à amplifier la sécurisation des couches physiques des objets interconnectés. Alors que les études sont relativement limitées dans ce domaine, la chaire doit permettre de faire de Brest l'un des piliers de la connaissance des systèmes cyber-physiques.

La chaire Cybaile associe le Latim, l'UBO et l'IMT Atlantique aux acteurs privés Thales, Aiintense et Sophia Genetics autour des sujets d'intelligence artificielle et de sécurisation des données de santé. Elle développe une expertise relativement unique en France pour la sécurisation des algorithmes d'apprentissage de données de santé face aux attaques et à leur fiabilisation contre les données tronquées. Elle approfondit également les recherches concernant le chiffrement des modèles d'apprentissage pour les sécuriser et garantir à la fois la traçabilité et l'anonymisation des patients.

La chaire AI for privacy est une chaire collaborative entre Isen Ouest et l'entreprise Arclan dont le but est de mettre l'intelligence artificielle et la sécurisation des données au service d'une technologie de reconnaissance faciale. Elle s'appuie sur une innovation brevetée capable de crypter le visage des êtres humains à la source.

Des chaires sur des sujets connexes

Isen Ouest se montre particulièrement actif sur des sujets de recherche ayant trait à la cybersécurité. La charte Internet of Things (IOT) a été créée en 2016, en collaboration avec Isen Méditerranée et plusieurs entreprises comme Thales ou IBM, pour mettre en commun les sujets de données massives, de leur sécurisation et de leur hébergement.

D'autres chaires, davantage en lien avec la science de la donnée mais non éloignées du sujet de la sécurisation, ont été développées à l'instar de celles sur la science des données pour l'industrie 4.0 ou de la chaire intelligence artificielle et robotique – vers l'entrepôt du futur dont le sujet est d'amplifier la connaissance pour optimiser le rendement des lignes de production, l'entreposage et le conditionnement en entrepôt au travers de la reconnaissance, la détection anticipée d'anomalies, etc. La chaire Transformation numérique pour l'observation, la surveillance et la sécurité du milieu marin (Transnum), créée 2019 en collaboration avec l'Ensta et Thales, vise à s'appuyer sur les technologies de drones maritimes et d'autonomisation du monde maritime pour améliorer la connaissance et la sécurisation du milieu marin, dans un contexte d'amplification des menaces (environnementales, terroristes, économiques, …).

Il existe également le groupement d'intérêt scientifique (GIS) Collaboration for Research regarding Maritime technologies, Observation, security, surveillance with Thales (Cormorant), lancé à l'initiative de Thales, qui réunit un consortium d'acteurs brestois composé de laboratoires et de leurs tutelles (Labsticc, Labisen, Irenav). Il vise à dynamiser la recherche en Bretagne sur les thèmes de l'industrie navale et aéronautique, où les enjeux de cybersécurité sont en filigrane, au même titre que l'intelligence artificielle. Son activité se décline en trois axes : l'autonomie des systèmes ; le facteur humain et l'interface avec la machine ; les capteurs et le traitement intelligent. Le GIS dispose d'un budget de fonctionnement de 500 000€ qui permet de financer des thèses, et indirectement d'attirer des talents, ainsi que des micro-projets proposés à l'occasion de journées d'idéation. En revanche, les liens avec les entreprises innovantes du territoire pourraient être approfondis.

Photo : Pierre-François Watras - Brest métropole

Les projets collaboratifs

Le projet Arsene s'inscrit dans le cadre du programme et équipements prioritaires de recherche (PEPR) cybersécurité lancé en juin 2022, financé à hauteur de 65 M€ sur 6 ans. Il vise à répondre à 10 défis de recherche dans le domaine de la cybersécurité. Le projet Architectures sécurisées pour le numérique embarqué (Arsene) fait lui l'objet d'un financement de près de 8 M€ et rassemble plusieurs acteurs académiques du territoire tels que l'Ensta ou l'UBO.

L'objectif du projet Arsene est de contribuer aux travaux de recherche de la communauté française sur la sécurisation des processeurs, de leur intégration dans les system on chip, les nouvelles primitives de sécurité, des méthodologies et outils pour la sécurisation des logiciels embarqués et des noyaux sécurisés des systèmes d'exploitation.

La collaboration s'étend aussi au niveau européen à l'instar de projets comme Cybermar dont le consortium est composé de Diateam et Naval Group. La portée du projet est d'améliorer la gestion des risques dans les milieux du transport maritime et portuaire par le développement d'outils de simulation. Dans la même veine, le projet Foresight est un autre exemple de projet de recherche financé dans le cadre du programme Horizon 2020, intégrant l'école navale et dont l'objectif est de développer une plateforme de gestion des menaces cybernétiques.

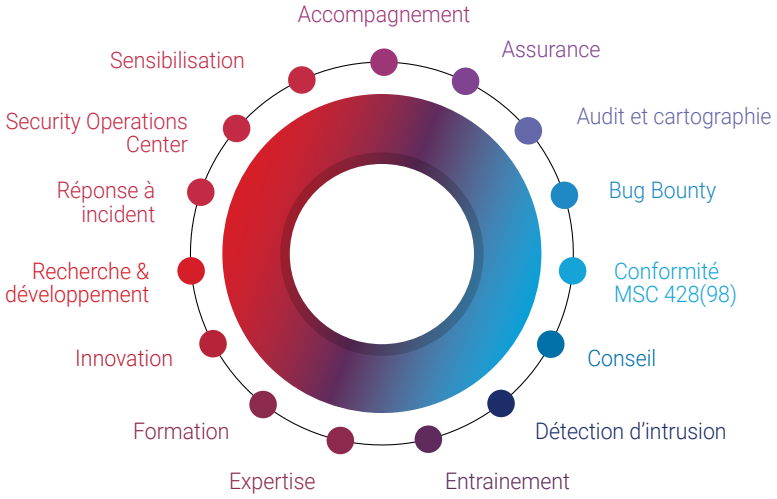
Des organisations d'acteurs qui jouent un rôle moteur

Le territoire présente la particularité d'héberger quelques organisations institutionnelles qui participent du rayonnement de la filière, et qui contribuent à faire du lien entre les entreprises qui rendent des services de cybersécurité et les potentiels clients.

Le Gacyb, un rôle d'intermédiaire entre les prestataires et les utilisateurs

Le groupement des acteurs de la cybersécurité (Gacyb) est une association fondée en 2017 à l'initiative de plusieurs chef·fes d'entreprise finistériens du numérique et du digital, avec pour objectif de sensibiliser les acteurs du territoire aux enjeux de la cybersécurité. Le groupement a pu compter sur le soutien de la chambre de commerce et d'industrie métropolitaine de Bretagne Ouest (CCIMBO) et de l'Anssi. La structure a rapidement pris de l'ampleur. Elle rassemble aujourd'hui une trentaine de membres dont la plupart des pure players locaux, et continue d'être sollicitée par de nombreux acteurs.

La première ambition a été de produire une charte des bonnes pratiques qui soit éclairante pour l'ensemble des acteurs qui ne disposent ni des ressources internes ni du socle de connaissance suffisant pour appréhender les risques qui pèsent sur leur activité. L'ambition seconde est de mettre en œuvre un label qui certifie de la qualité de l'engagement des entreprises en matière de cybersécurité. Il permettra de soutenir l'activité des sociétés labellisées, dans une filière où les labels sont des passeports d'entrée sur le marché. Au quotidien, les membres du Gacyb tiennent bénévolement une permanence afin d'apporter du conseil et des clés d'entrée auprès des acteurs privés et publics du territoire. L'association participe également à l'organisation d'ateliers, de conférences, de séances de coaching et même d'événements (Breizh Cyber Show).



France cyber maritime, le bouclier numérique de la sécurité maritime

France cyber maritime (FCM) est une association, fondée en 2020, sous l'impulsion d'acteurs publics et privés, avec la caution de l'Anssi et impulsée par le secrétariat général à la mer. Elle regroupe environ 70 membres partout en France et vise à apporter des réponses au monde maritime et portuaire qui justifie de besoins très importants en termes de sécurisation numérique. Le Panorama de la cybermenace maritime 2022 coréalisé en partenariat avec l'entreprise de cybersécurité OWN témoigne d'une augmentation de 235 % des incidents notables et publics entre 2020 et 2022, qui ne correspond qu'à la face visible des attaques menées contre les acteurs du monde maritime. La localisation à Brest de cette structure contribue à faire rayonner et à faire connaître la métropole comme un territoire d'excellence en matière de cybersécurité appliquée au maritime à l'international. Au-delà de ses missions de sensibilisation et de porter à connaissance, FCM dispose de son propre poste opérationnel, le Maritime Computer Emergency Response Team (M-CERT). Il s'agit d'un centre d'alerte et de réaction aux attaques informatiques (CSIRT) qui propose de nombreux services de prévention des risques. Il veille en amont à informer les acteurs des menaces détectées, à apporter de l'information (lettres destinées aux membres), à enquêter sur les différentes vulnérabilités, et en aval à coordonner la gestion des incidents.

Le territoire bénéficie également du rayonnement de structures basées ailleurs en Bretagne comme le Pôle d'excellence cyber (PEC), porté par le ministère des Armées et le Conseil régional de Bretagne et basé à Rennes. Il organise notamment l'événement international European Cyber Week qui rassemble près de 5 000 participants et dont la 9e édition s'est déroulée du 18 au 21 novembre 2024 à Rennes. Le PEC met l'accent sur le volet académique de la filière en participant au développement des formations en cybersécurité et à l'implémentation de briques cyber au sein de formations non dédiées au domaine. Il vise aussi à soutenir l'activité de recherche qui développe et maintient les compétences et les savoir-faire sur le territoire, dans un objectif final de souveraineté de la cybersécurité. Le PEC rassemble aussi des acteurs du territoire tels que l'UBO, l'IMT Atlantique, l'Isen Ouest ou l'Ensta dans la sphère académique et des acteurs privés comme Diateam, Arkea, Naval Group ou Thales.

Basé à Brest et conventionné par le ministère des Armées, le Pôle Mer Bretagne Atlantique soutient l'innovation maritime et joue un rôle clé en cybersécurité. Il intervient auprès de ses adhérents et des politiques publiques à travers le développement de la cybersécurité maritime et portuaire, avec des projets régionaux, nationaux et européens ; la recherche, notamment via la chaire de cyberdéfense des systèmes navals et des travaux avec l'Agence nationale de la recherche (ANR) ; l'accompagnement des entreprises adhérentes, en particulier celles de la Base Industrielle Technologique de la Défense (BITD), sur la cybersécurité et la conformité ; la gouvernance de France Cyber Maritime, dont il est membre fondateur.

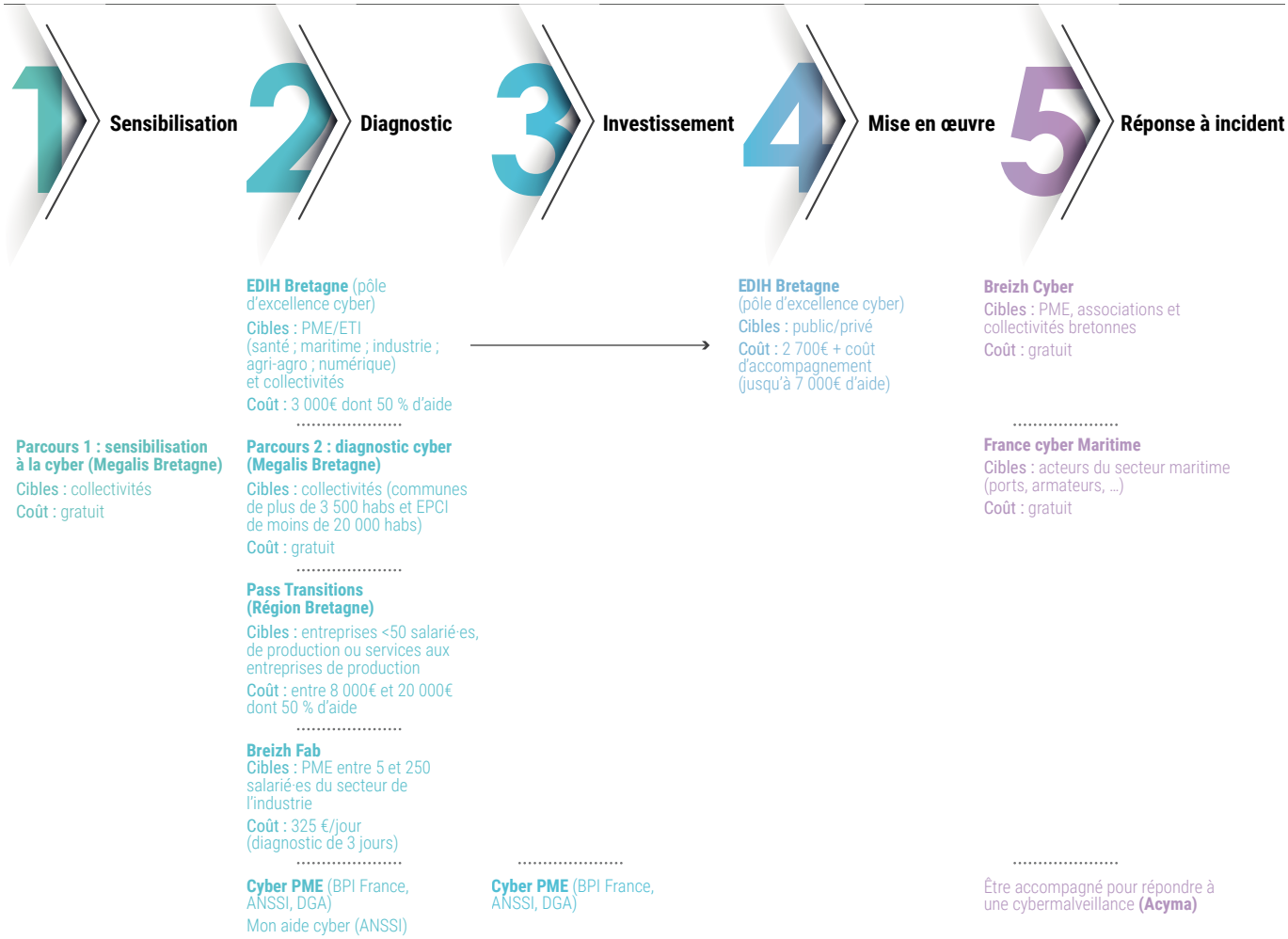
L'implantation de l'Anssi à Rennes, signe de la reconnaissance de l'expertise régionale

En novembre 2023, l'Anssi, qui n'est autre que l'autorité française en matière de cybersécurité, a inauguré sa première antenne en région, précisément à Rennes. Près de 200 agents devraient d'ici à 2025 assurer les services fournis par l'autorité nationale en termes de cybersécurité. Le choix de Rennes envoie un signal fort sur le niveau de maturité de l'écosystème régional et sa forte structuration autour d'acteurs de première importance tels que la Direction générale des armées (DGA), du commandement de la cyberdéfense (Comcyber), du pôle d'excellence cyber (PEC) et des acteurs privés innovants.

Au même moment, la Région Bretagne a inauguré son Computer emergency response team (CSIRT) pour couvrir les besoins des entreprises et acteurs publics victimes de cyberattaques. En l'espace d'un an, il a traité plus d'un centaine d'incidents différents. Il a la capacité d'accompagner la plupart des requêtes, et travaille aussi en collaboration avec un réseau de prestataires de confiance parmi lesquels plusieurs sont localisés au sein de la métropole brestoise.

Des outils pour sensibiliser et sécuriser le tissu économique breton

Le European Digital Innovation Hub (Edih) est une plateforme régionale visant à accélérer la transition numérique dans les secteurs de l'agri-agro, du maritime, de la santé et du numérique. Il a été sélectionné en juin 2022 par la commission européenne pour intégrer un réseau de 140 pôles au niveau européen. L'Edih Bretagne possède la particularité d'accompagner les collectivités, les PME et ETI du territoire dans un parcours de transformation digitale en y intégrant des enjeux de cybersécurité et d'intelligence artificielle au sein des organisations. Il opère sur les volets de la sensibilisation, de la mise en œuvre de plans d'actions en complément des services de sensibilisation et d'investissement dans des produits cyber proposés par les organismes nationaux tels que l'Anssi ou BPI France.



Des événements qui fédèrent la communauté cyber du territoire

Le Brest cyber show s'inscrit dans la veine des missions menées par le Gacyb, à savoir sensibiliser aux risques liés à la cybermalveillance. Cet événement se déroule sous forme de conférences et de tables rondes, et réunit les meilleurs experts locaux et nationaux à Brest. Avec déjà trois éditions au compteur, le Breizh cyber show a pu mettre l'accent sur le hacking éthique, le coût de la cybersécurisation, le déroulement d'une cyberattaque au travers de témoignages, etc.

Unlock your brain, harden your system (UYBHYS) est un événement co-organisé par Diateam et la cantine numérique de Brest et soutenu par de nombreux partenaires économiques. Il se déroule sur deux journées et conjugue des cycles de conférences, des ateliers et des jeux en ligne type « capture the flag[10]» . Sa vocation est de donner à voir sur les nouvelles technologies et de moderniser la cybersécurité auprès des jeunes.

La métropole accueille d'autres événements en lien avec la cybersécurité. La plupart sont relativement complémentaires. Le cyber lunch tour est un événement itinérant, organisé par BT-BLUE (ex-Bretagne Telecom) et en partenariat avec le Village By CA, qui vise à répondre à quelques questions triviales de prévention et de gestion de crise.

Même si l'agenda local est fourni en événements cyber, le constat établi par la communauté cybersécurité du territoire fait un état d'un manque de visibilité auprès du tissu économique et de la communauté nationale, voire internationale. Il existe donc un enjeu à capitaliser sur les événements existants et à développer un programme de sensibilisation vers les entités les plus éloignés du sujet.

Photo : Événement "Unlock your brain, harden your system". Crédit UYBHYS

10. Capture de drapeau, jeu consistant à se faire affronter deux équipes qui doivent exploiter les vulnérabilités de sorte de pénétrer les ordinateurs des adversaires pour récupérer un drapeau, preuve de l'intrusion.

Contexte et orientations stratégiques

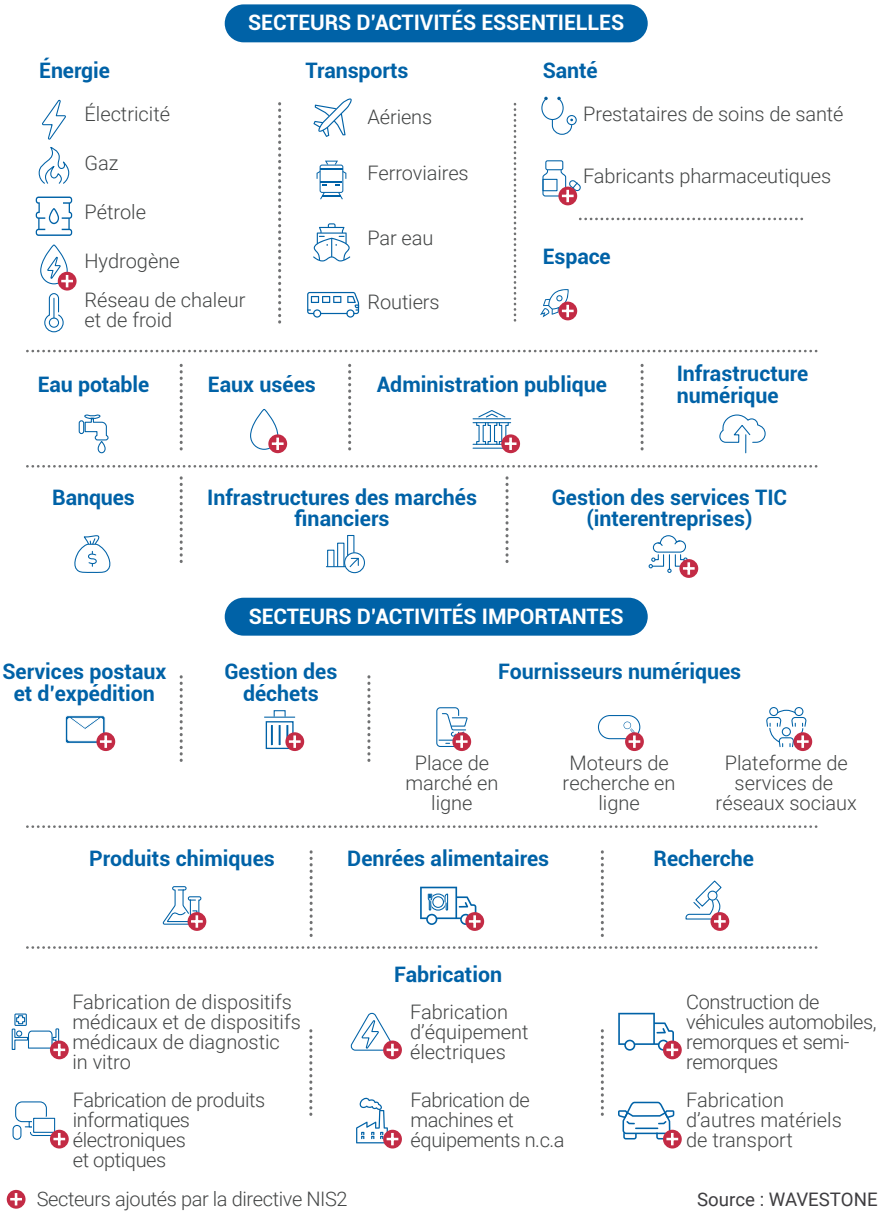
NIS2 : une directive pour booster la mise en conformité des entreprises et des acteurs publics en matière de cybersécurité ?

Votée au Parlement européen le 14 décembre 2022, la directive Network and Information Security 2 (NIS2) vise à harmoniser et renforcer la cybersécurité au sein de l'union européenne à partir de 2025. Elle vient en appui de la NIS préexistante et à un cadre réglementaire[11] riche, qui s'est renforcé au cours des années.

Elle poursuit l'ambition de renforcer le niveau de protection des acteurs économiques d'au moins 50 salariés par un élargissement des secteurs concernés, en incluant notamment l'administration publique déconcentrée et décentralisée, et en révisant à la hausse le niveau d'exigence concernant la sécurisation du système d'information. Elle s'étend désormais à 18 secteurs (contre 7 auparavant), et décline en deux niveaux hiérarchiques : « hautement critiques » et « autres secteurs critiques ». Outre l'administration publique, qui constitue l'une des principales nouveautés, plusieurs domaines émergents ont été intégrés à l'instar du spatial, et d'autres plus traditionnels tels que l'agroalimentaire ou l'industrie automobile. Par ailleurs, certains secteurs déjà présents dans la NIS1 ont été amendés comme l'énergie auquel le segment de l'hydrogène a été ajouté.

NIS2 apparaît comme une opportunité pour stimuler à la fois l'offre et la demande sur le marché de la cybersécurité. D'un côté, une plus large frange d'utilisateurs finaux va devoir mettre en place un protocole complet (gouvernance, formation, prévention des risques, notification en cas d'incident et de continuité de service), notamment les acteurs publics, les entreprises de l'énergie, du spatial ou des services numériques qui sont nouvellement inclus dans les secteurs jugés comme hautement critiques, de la même manière que les autres secteurs critiques. De l'autre côté, les pourvoyeurs de services en cybersécurité pourraient bénéficier de clients supplémentaires, ce qui devrait aider à rendre leur offre lisible. Cette directive pourrait aussi revêtir une dimension davantage punitive en cas de non-conformité avec les règles en vigueur. En cas de contrôle de l'Anssi, les entités essentielles pourraient recevoir une amende plafonnée à 10 millions d'euros ou équivalant à 2 % du chiffre d'affaires, et de 1,4 % s'agissant des entités importantes. Dans ce contexte, les certifications délivrées par l'Anssi pourraient servir de caution de conformité auprès des entreprises détentrices de ces labels.

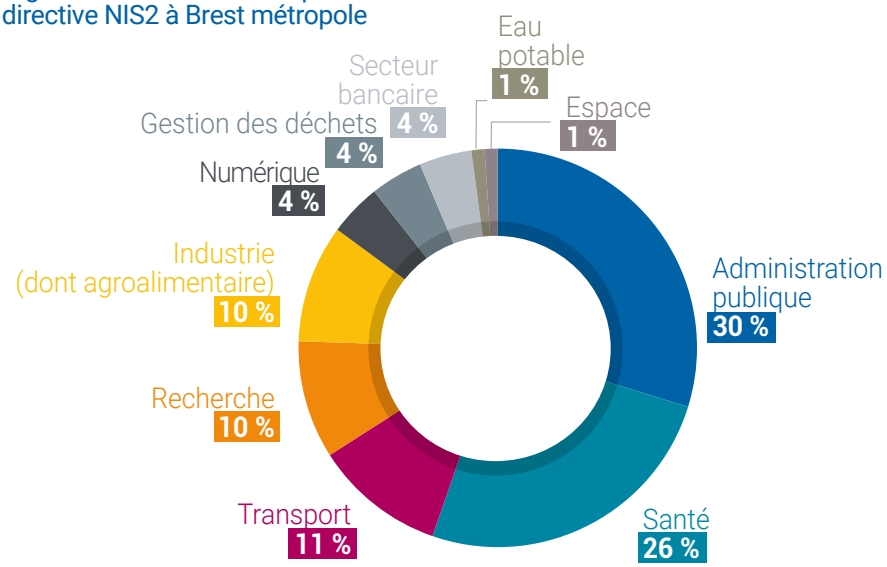
La nouvelle mouture de loi devrait s'adresser directement à près de 90 organisations différentes sur le périmètre de Brest métropole, dont un peu plus de la moitié seraient nouvellement concernées par les exigences en termes de cybersécurité. Certaines sont d'ailleurs concernées à plusieurs titres. Une grande



Source : WAVESTONE

11. International hip and port facility Security en 2004 ; loi de programmation militaire en 2013 ; Cyber defense act en 2019

Répartition par secteur des organisations concernées par la directive NIS2 à Brest métropole



Source : Capfinancials - Traitement : Adeupa

partie des nouveaux entrants concerne l'administration publique puisque 28 entités répondent aux critères imposés par la NIS2 parmi lesquelles figurent Brest métropole et ses communes, des établissements scolaires (lycées, collèges, …) et de l'enseignement supérieur (université, écoles d'ingénieurs), la chambre de commerce et d'industrie, le CHU et des organismes de recherche comme Ifremer.

Par ailleurs, environ 80 établissements secondaires d'entreprises, dont le siège ou l'établissement principal se situe en dehors du territoire, pourraient aussi avoir des répercussions indirectes de la NIS2, dans la mesure où les protocoles devraient s'étendre à l'ensemble des établissements des entreprises. Cela recouvre quelques gros employeurs locaux tels que la RATP développement, les cliniques privées, la Poste, Naval Group, Thales ...

À noter que les acteurs du secteur bancaire seront soumis au règlement européen Digital Operation Resilience Act (Dora) qui est une application sectorielle de NIS2. Avec une entrée en vigueur prévue en janvier 2025, elle prévoit de renforcer la gouvernance en cybersécurité du monde de la finance, de la prévention du risque à la mise en œuvre de la résilience post-attaque. Elle complète NIS2 en mettant davantage l'accent sur la prévention et la neutralisation des attaques et la supplante en étant le cadre de référence pour les établissements du milieu bancaire et des sous-traitants, à l'exception des acteurs du numérique qui fournissent des services à ce secteur qui devront toujours se référer à NIS2.

Des ambitions locales insérées dans une mouvance nationale et régionale

En février 2021, l'État s'est doté d'une stratégie d'accélération cyber d'un montant d'un milliard d'euros pour faire face aux menaces grandissantes qui pèsent sur les entreprises et les collectivités sur leur sécurité informatique.

L'objectif est, à très court terme (2025), de tripler le chiffre d'affaires généré par la filière sur le territoire national pour atteindre 25 milliards d'euros, et de doubler les effectifs pour atteindre 75 000 emplois en soutenant des entreprises à fort potentiel de développement. Elle vise aussi à stimuler la recherche en doublant le nombre de thèses Cifre et en augmentant de 30 % la recherche partenariale. Sa mise en œuvre se décline en 5 axes prioritaires :

1. Développer des solutions souveraines et innovantes de cybersécurité
2. Renforcer les liens et synergies entre les acteurs de la filière
3. Soutenir la demande en sensibilisant mieux tout en faisant la promotion des offres nationales
4. Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre
5. Soutenir le développement des entreprises de la filière via un abondement de fonds propres

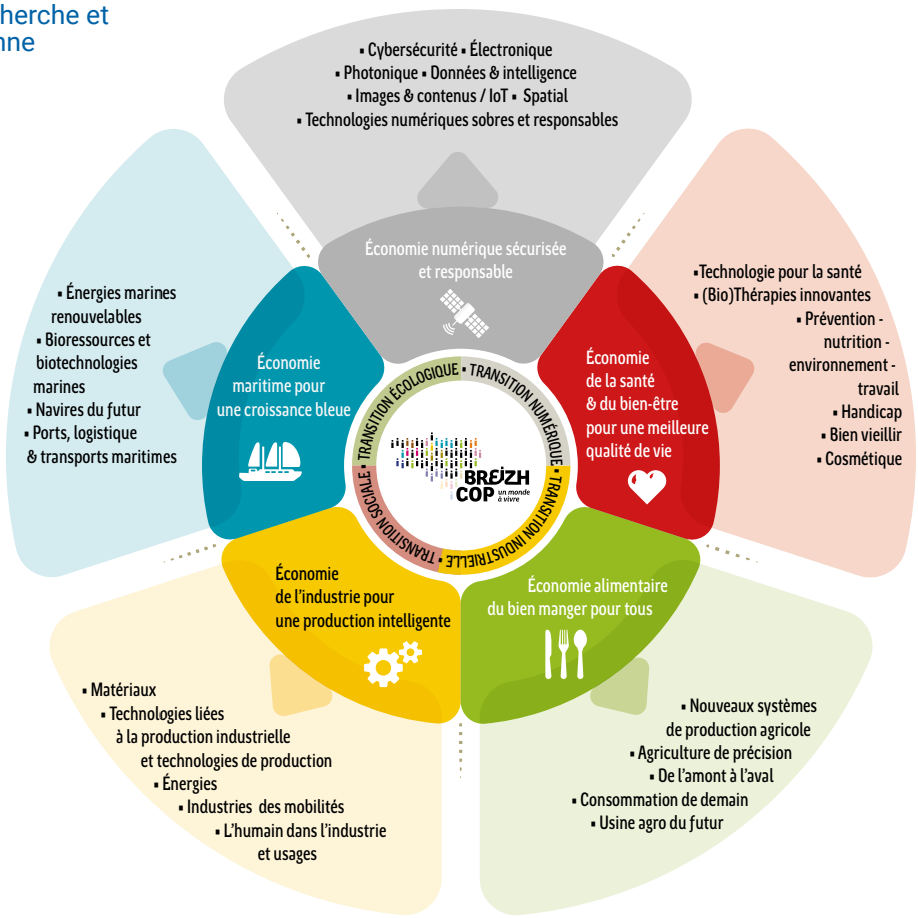
Cette stratégie a emboîté le pas de France 2030 qui intègre plusieurs stratégies visant à développer les technologies numériques en France. Dans ce cadre, le programme Tech DeepNum20 a permis de récompenser 17 lauréats dans les 5 dispositifs d'appels à projet et manifestation d'intérêt. L'entreprise Apizee, basée à Lannion a été retenue pour son offre de visio conférence sécurisée et souveraine, financée à hauteur de 517 000€ par l'État.

À l'échelle régionale, la Bretagne a inscrit la cybersécurité au sein de sa stratégie de recherche et d'innovation (S3) au sein du volet économie numérique responsable et sécurisée. Au regard de la puissance du marché au niveau mondial, et du potentiel palpable sur le territoire, l'objectif est de rendre la Bretagne plus visible sur ce sujet en France et en Europe. Pour ce faire, la stratégie inclut 5 axes opérationnels :

- Organiser et soutenir un écosystème construit breton puissant et en croissance (attractivité)
- Développer les compétences et la formation pour répondre aux besoins croissants en matière d'emploi, d'éducation et de sensibilisation des professionnels
- Soutenir les investissements publics et privés dans des approches innovantes orientées vers la recherche et l'innovation (dont C-Cube, centre de compétences en cybersécurité)
- Engager des initiatives nationales collectives sur notre territoire
- Participer aux programmes et projets stratégiques à l'échelle européenne ; soutien aux PME pour accéder au marché européen

Aussi, les problématiques de cybersécurité sont largement diffusées dans le domaine de l'économie bleue, au travers d'un axe dédié à la sécurité maritime. Les navires et les écosystèmes portuaires font face à des menaces de plus en plus grandes, c'est pourquoi la Région Bretagne, qui possède une légitimité dans ce domaine, par la présence de France cyber maritime notamment, aspire à renforcer sa position en nourrissant l'ambition de devenir leader dans le développement de solutions et de systèmes de sécurité maritime dans les domaines de la cybersécurité maritime. Les autres objectifs visent au développement de l'usage de la robotique à des fins de sécurité maritime, à l'utilisation de l'IA pour surveiller les océans et les activités en mer et à l'enrichissement de l'offre de formations pour répondre aux besoins en compétences et en expertise.

La stratégie de recherche et d'innovation bretonne



La cybersécurité se trouve aussi, plus indirectement, dans le volet « données et intelligence » avec un objectif de mise en commun des travaux en cybersécurité au service de la collecte, du stockage et du traitement des données sensibles. Cette dimension d'interopérabilité est également partagée avec le domaine des technologies de la santé, et notamment sur l'impératif de renforcer les liens entre les big data, l'IA et la cybersécurité pour l'exploitation des données de santé et le développement d'innovations. Elle se décline aussi dans le domaine de l'industrie, notamment en ce qui concerne l'autonomisation des véhicules et plus globalement l'industrie 4.0 (robotique, IA, cybersécurité, etc.).

La Bretagne : un modèle à suivre au niveau européen ?

La cybersécurité est sous de multiples facettes inscrite dans la stratégie régionale de recherche et d'innovation avec l'enjeu de faire de la Bretagne un chef de file européen de la filière, en s'appuyant sur notamment sur ses complémentarités infrarégionales entre Brest et Rennes. La Bretagne se positionne comme une région moteur dans le domaine de la cybersécurité. La cartographie réalisée dans le cadre du projet européen Connecting européean cyber valley montre à quel point le territoire est imbriqué dans les différentes actions pilotées par l'Union européenne et reconnu comme un modèle dans le domaine de la cybersécurité.

La Bretagne se distingue par le pilotage de projets européens structurants à l'instar du projet Cyber, financé à hauteur de 1,6 millions d'euros dans le cadre du programme Interreg Europe 2014-2020 et dont la gouvernance est organisée par Bretagne développement innovation. Cela démontre le rôle de chef de file de la région pour améliorer les coopérations interrégionales, notamment entre les petites et moyennes entreprises afin qu'elles renforcent leur compétitivité. L'expérience bretonne est aussi utilisée comme modèle au sein du projet Interreg Campus dont l'objectif est de renforcer la résilience numérique des collectivités territoriales.

La Bretagne est aussi à l'origine d'une communication conjointe avec d'autres partenaires institutionnels de pays membres (Espagne, Allemagne, Finlande, Estonie) au Parlement européen intitulée « Résilience, dissuasion et Défense : doter l'UE d'une cybersécurité solide ».

Elle est également membre de la European Cybersecurity organisation (Ecso), créée en 2016, au sein de laquelle elle joue un rôle proactif. L'association a pour mission de favoriser les collaborations entre les entreprises, le monde de la recherche, les administrations publiques, les utilisateurs finaux et les structures d'accompagnement. Elle met aussi en valeur les initiatives régionales telles que la création du campus cyber breton.

La Région se distingue aussi par son Edih, dont le rôle est d'amener l'ensemble du tissu économique breton vers une meilleure connaissance de sa maturité en cybersécurité et en intelligence artificielle, et une meilleur prise en compte de ces enjeux au sein des organisations.

La Bretagne se positionne comme une région moteur dans le domaine de la cybersécurité.

Le 26 avril 2024, la Région Bretagne, en partenariat avec 5 membres fondateurs territoriaux dont Brest métropole, a officialisé la création de son campus cyber Bretagne cyber alliance (BCA), le troisième labellisé en France par le campus cyber national. Il a la particularité, au regard de la composition de son consortium, de diffuser son action de manière territorialisée. La présence d'acteurs économiques et institutionnels reconnus au sein de Brest métropole fait de la collectivité un maillon essentiel du fonctionnement du campus. La feuille de route de BCA se décline en 4 ambitions.

- Favoriser le développement des pure players de la cybersécurité en leur donnant un accès plus facile aux mécanismes de financement, notamment européens, et en fluidifiant la mise en relation avec le tissu économique à sécuriser.
- Adapter la carte de formations avec les besoins des acteurs du territoire en développement de nouvelles formations (initiales et continues) et en attirant des profils plus diversifiés vers les métiers de la cybersécurité (femmes, publics éloignés de l'emploi, ...).
- Conforter un positionnement de pointe dans les domaines de la recherche et de l'innovation en stimulant le transfert technologique notamment.
- Faire approprier la culture cyber par l'ensemble de la société bretonne (entreprises, collectivités, jeunes publics).

Méthodologie

Recensement des établissements

On parle de « pure players » pour désigner les entreprises dont le cœur de métier a principalement pour vocation de fournir des biens et services spécialisés dans la cybersécurité (audit, test d'intrusion, édition de logiciels, prestations de réponse à incident, ...). Les entreprises ont été identifiées sur la base des connaissance de l'ensemble des partenaires de l'étude : Technopôle Brest-Iroise, Pôle Mer Bretagne Atlantique, Chambre de commerce et d'industrie du Finistère. Le recensement s'appuie également sur la base de données de Bretagne Développement Innovation (BDI), les annuaires du Gacyb et de FCM. Un requêtage a été effectué sur l'application Capfinancials pour croiser les sources d'informations sur la base des mots-clés ou expressions suivants : cyber ; cybersécurité ; cyberdéfense ; cyberprotection ; cyberrésilience ; cyberrange ; cybermaritime ; hacking éthique ; bug bounty ; RSSI ; réponse à incident.

La liste des entreprises de services numériques (ESN) possédant une activité en cybersécurité a été construite en croisant les entreprises couvertes par le code APE 6202A (conseil en système et logiciels informatiques) avec celles répondant au mot-clé « infogérance » et/ou disposant d'une certification ou labellisation en cybersécurité.

Seuls les effectifs des pure players sont comptabilisés, et dans leur intégralité. Les emplois en cybersécurité dans les ESN, secteurs connexes ainsi que dans les entreprises utilisatrices des secteurs non-technologiques faisant l'objet d'un recensement partiel ne sont, par conséquent, pas inclus. Cette partie de l'écosystème fera l'objet d'un inventaire plus détaillé dans le cadre d'un travail de gestion prévisionnelle des emplois et compétences (GPEC), engagé par Brest métropole en 2025. Par ailleurs, les effectifs de la Défense ne sont pas inclus.

Sources

- Fichier des établissements enregistrés au RCS
- Fichier Sirene, Insee
- Capfinancials
- Datavisualisation BDI
- Entretiens réalisés en présentiel et/ou par téléphone

Bibliographie

- *L'excellence cybersécurité civile et militaire dans Rennes métropole*, Novembre 2020, Audiar
- *Panorama de la cybermenace 2023*, 2023, Anssi
- *L'attractivité et la représentation des métiers de la cybersécurité vue par les professionnels*, Enquête 2023, Anssi
- *Cybersécurité en Bretagne : l'enjeu des compétences* , juin 2017, Apec Bretagne

LA FILIÈRE CYBERSÉCURITÉ DANS BREST MÉTROPOLE

Direction de la publication
Yves Cléach

Rédaction
Quentin Delaune

Maquette et mise en page
Timothée Douy

Crédit photographique de couverture
DIATEAM

Relecture
Magali Can

Tirage
50 exemplaires

Contact
contact@adeupa-brest.fr

Dépôt légal
1er trimestre 2025

Référence
25-066

AGENCE D'URBANISME DE BREST • BRETAGNE
18 rue Jean Jaurès - 29200 BREST
Tél. 02 98 33 51 71

www.adeupa-brest.fr