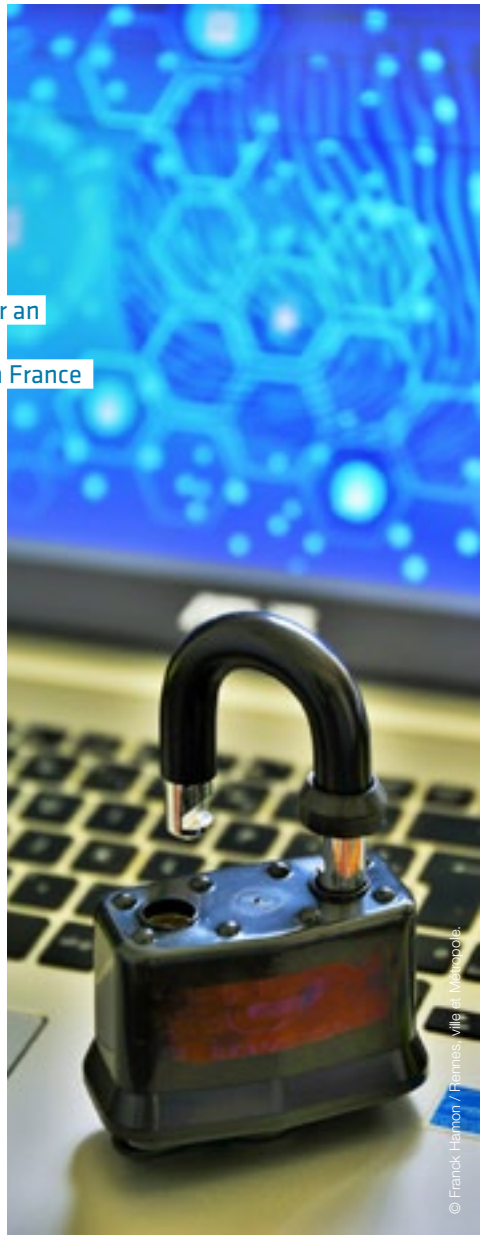
ACTUALISATION 2020

L'excellence cybersécurité civile et militaire dans Rennes Métropole

NOVEMBRE 2020

AUDIAR RENNES

SOMMAIRE



Synthèse : la cyberforce rennaise porte l'emploi local

En 2020, le confinement et l'intensification du télétravail ont participé à l'accroissement des activités mondiales de cybersécurité, déjà très sollicitées par les tensions géopolitiques et les menaces terroristes. Rennes, qui en 2019 faisait état d'un écosystème innovant et puissant en ce domaine, consolide également son positionnement.

D'abord sur le plan des activités militaires où le déploiement de la stratégie de l'État conduit à l'installation à Rennes du Groupement de la cyberdéfense des armées et de l'ANSSI. D'ici 2026, 940 emplois nouveaux seront générés dans les sites cyber de l'État. À proximité du ComCyber, le quartier de La Courrouze prend d'ailleurs une forte tonalité cyber avec Airbus Cybersecurity, Thales Services, Altran…

Ensuite, sur le plan des acteurs privés, la dynamique s'intensifie : 13 entreprises nouvelles ont été créées en deux ans. Pour la 3ème année consécutive, Rennes est n°1 (hors Île-de-France) au classement Wavestone des startups en cybersécurité.

Tout est donc réuni pour que cette cyberforce porte l'emploi local, et les chiffres l'attestent : avec +670 emplois en 21 mois, la cybersécurité est un domaine aux potentialités de développement intenses.

Les acteurs territoriaux assurent pour leur part les conditions optimales pour créer des liens de coopération et accompagner les différents acteurs.

Cyberdéfense Factory (incubateur dual civil et militaire), Cyberschool (école universitaire de recherche), Cyberplace (immobilier aux normes de confidentialité), CyberGPEC… autant de réponses adaptées aux besoins d'innovation de ce secteur.

En effet, l'enjeu pour la métropole est, à la fois, de développer l'attractivité du territoire pour les talents en recherche, d'étoffer l'offre de formation, de poursuivre la dynamique d'accompagnement des entreprises, des grands groupes et des startups, de cultiver ce terreau de confiance entre acteurs afin d'accompagner la filière de cybersécurité de confiance à prendre son essor à Rennes et, par delà, en Bretagne. Il s'agit aussi pour le territoire de consolider sa visibilité nationale et de poursuivre sa reconnaissance européenne et internationale.

À Rennes se rassemblent toutes les énergies dans le domaine de la cybersécurité dans un ensemble cohérent permettant, à travers une vision partagée, les plus grandes ambitions pour cette « cyber valley européenne».

La cybersécurité dans Rennes Métropole en 2020

Une intense création d'emplois

4 160 emplois

3 280 emplois privés dans **76** entreprises privées

880 cybercombattants du ministère des Armées

Une croissance de **26 %** des emplois privés en 21 mois

13 entreprises nouvelles en deux ans

Implantation de l'**ANSSI**

Un fort développement attendu

940 emplois nouveaux attendus dans la sphère publique d'ici 2026 :

220 postes à l'ANSSI

720 personnels cyber supplémentaires dans les Armées

Un écosystème leader

Rennes est n°1 (hors Paris Île-de-France)

> en recherche académique avec **150 chercheurs**

> au palmarès Wavestone des startups en cybersécurité

Des spécificités uniques :

« Cyberschool », école européenne universitaire de recherche

« Cyberplace », immobilier dédié en cyberdéfense

Le pôle d'excellence cyber, animateur d'innovations

Un dialogue militaro- industriel unique en France

Rennes, 1ère force cyber des Armées en région

La **Cyberdéfense Factory**, un incubateur dual civil et militaire unique

Des **chaires industrielles** mixtes

Des groupes industriels impliqués

Airbus Cybersecurity, très associé à la recherche locale

Thales Services, une « ruche » pour accueillir des startups

Le CyberSoC d'Orange Cyberdefense, place forte du groupe

La cybersécurité dans Rennes Métropole : 4 160 emplois directs

3 280 emplois privés dans les entreprises de la cybersécurité dans Rennes Métropole

76 entreprises spécialistes de la cybersécurité

Fin 2020, l'Ille-et-Vilaine accueille 76 établissements privés spécialistes de la cybersécurité.
Ces 76 établissements représentent au total 3 279 emplois privés.
70 % de l'emploi est concentré dans les 8 entreprises privées de plus de 100 salariés. La moitié des établissements ont moins de 10 salariés.

Cette année, trois établissements ont fermé : Swid, Teclib et Tibsys (représentant au total très peu d'emplois, de l'ordre de 3 à 5 emplois).
À l'inverse, durant les deux dernières années, 10 nouvelles entreprises ont été créées : IpCyb, Anozrway, Wallix, Malizen, Synacktiv, Glimps, Lootus, Sec-It Solutions, Wallack, Quarkslab et 3 sont en cours d'immatriculation juridique (Gatewatcher, Sahar et CyMind).
La quasi-totalité de ces établissements privés est implantée dans Rennes Métropole. Seules 9 sociétés sont installées dans le reste du département, comptabilisant au total une cinquantaine d'emplois salariés (dont une trentaine de cyberspécialistes d'Apixit installé à Montauban de Bretagne – donnée 2019).

Ces spécialistes de la cybersécurité s'articulent avec un écosystème numérique intense à Rennes qui comprend environ 30 000 emplois dans 4 000 établissements, et qui lui-même développe nécessairement des compétences et un savoir-faire généraliste en cybersécurité.

© Anthony Micallef - Rennes, Ville et Métropole.

© Destination Rennes.

ÉTABLISSEMENTS SPÉCIALISÉS EN CYBERSÉCURITÉ

À noter : Sont recensées ici les entreprises dont le cœur de métier est majoritairement ou exclusivement la cybersécurité.

A
- ABAK SYSTEMES
- ACCEIS
- ACE TIMING
- ACKLIO
- AIRBUS CYBERSECURITY
- AKERVA
- AKKA I&S
- ALCYCONIE
- ALTEN
- ALTRAN TECHNOLOGIES
- AMOSSYS
- ANOZRWAY
- ARIADNEXT
- ARX ARCEO
- ASSURABLE (OBDO)
- AVIXA

B
- BUGLAB
- BLOO CONSEIL

C
- CAILABS
- CAPGEMINI
- CARDELYA
- CLARANET
- CONTENTARMOR
- CRYPTOVIA
- CY MIND
- CYBERPROASSUR

D
- DGA Mi (Direction générale de l'armement Maitrise de l'information)

E
- EASYLIENCE (NANOCODE LABS)
- EDSI
- EXAPROBE

F
- FAMOCO
- FORMIND

G
- GATEWATCHER
- GARNAULT & ASSOCIES
- GLIMPS

H
- HARDENING CONSULTING
- HOGO BUSINESS SERVICES

I
- ICODIA
- INTHREAT
- IPCYB

K
- KEREVAL

L
- LAMANE
- LAMARK
- LOOTUS
- LSTI

M
- MALIZEN
- MINISTÈRE des ARMÉES (autres sites que DGA)

N
- NAGRA (NEXGUARD LABS France)
- NEXTIRAONE FRANCE
- NOMIOS OUEST

O
- ONE WAVE
- ORANGE
- ORANGE CYBERDEFENSE
- OSYTOS

P
- PHOENIX ENGINEERING

Q
- QUARKSLAB

R
- Recherche publique
- RETIS APIXIT
- RSDA Renseignement sécurité défense analyse
- RUBYCAT LABS

S
- SAHAR
- SEC-IT SOLUTIONS
- SECURE IC
- SEKOIA
- SENSEYOU
- SERMA SAFETY AND SECURITY
- SHADLINE (OWALTECH)
- SIB
- SILICOM
- SODIFRANCE
- SOPRA STERIA GROUP
- SQUAD
- SYNACKTIV
- SYNETIS
- SYSTANCIA (IPDIVA)

T
- TAZTAG (NEWPADMAKER)
- THALES
- THALES SERVICES

W
- WALLACK
- WALLIX
- WOLEET

Y
- YAGAAN
- YES WE HACK

Z
- ZEROCHAIN

Des produits et solutions diversifiées

Il est difficile de dresser un portrait des spécialités précises des entreprises rennaises, certaines sont généralistes, d'autres développent leur business à partir d'une technologie clé ou d'un service novateur. Des sociétés développent des audits, conseils, formations et produits de sécurisation de la messagerie, des applications, des data, des infrastructures et des équipements, du cloud, des objets connectés… D'autres travaillent sur la prévention des menaces mais aussi sur la gestion de crise (Alcyconie, Cyberproassur…).

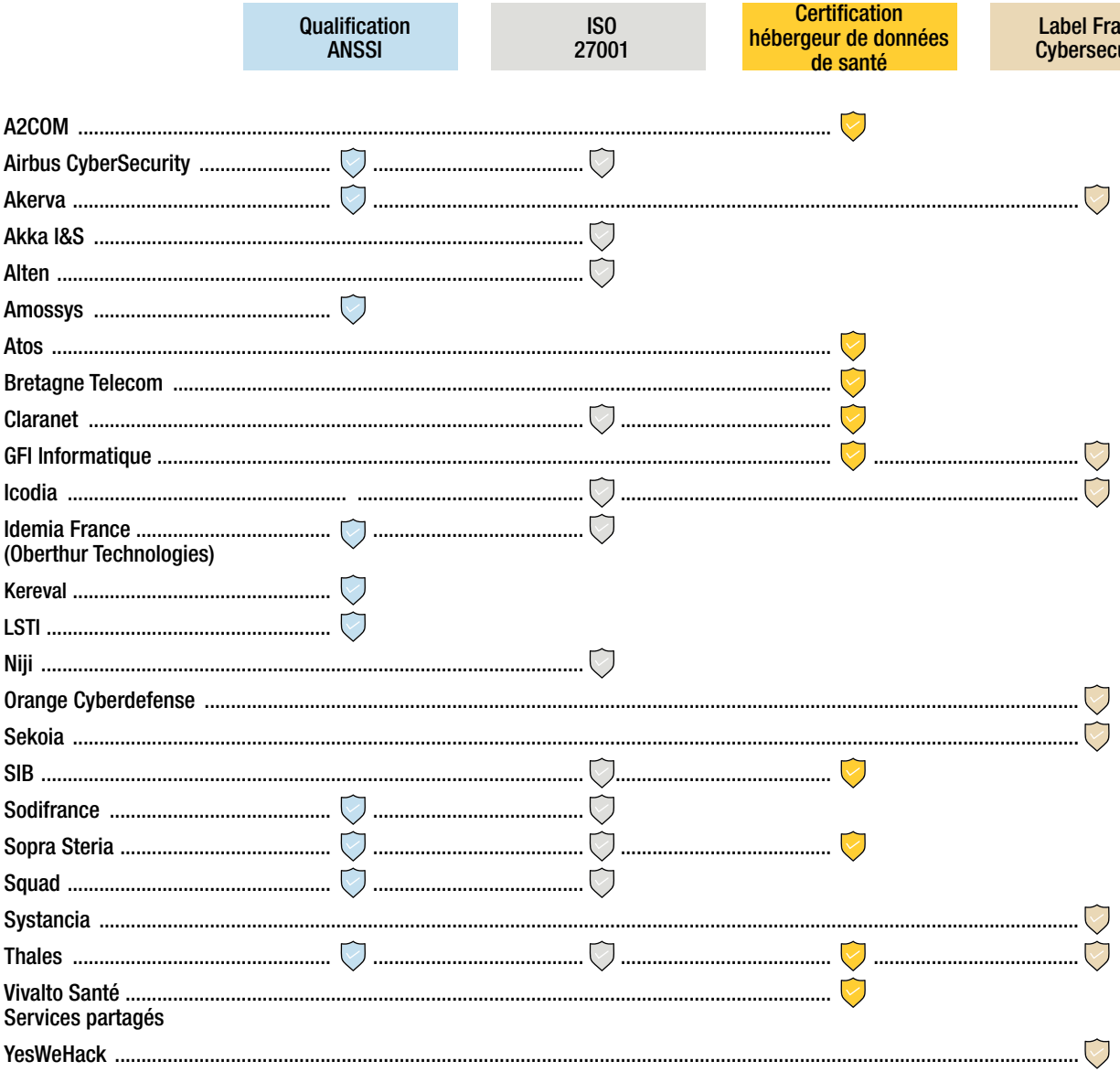
Par exemple, Acklio se dédie à la sécurisation des réseaux sur lesquels sont branchés les objets connectés. Ariadnext travaille sur l'identité numérique, la sécurisation de documents et la signature électronique. Rubycat est éditeur de logiciels spécialisé en traçabilité numérique. Shadline développe des solutions de repli numérique en cas de cyberattaque. Synackactiv réalise des tests d'intrusion et propose des recommandations...

EXEMPLES DE DOMAINES D'INTERVENTION
DES ENTREPRISES RENNAISES

Une dynamique de certification de l'écosystème

À Rennes, 10 établissements sont qualifiées ANSSI (soit 6 de plus qu'en 2019), 12 entreprises sont certifiées ISO 27001 Management de la sécurité de l'information (contre 7 en 2019) et 8 ont le label France Cybersecurity.
En outre, 9 établissement sont certifiés « hébergeur de données de santé » (3 en 2019). Cet agrément permet de certifier que l'hébergement de données de santé, jugées sensibles, sera effectué dans des conditions de sécurité adaptées à leur criticité, fixées par la réglementation française.

ENTREPRISES PRIVÉES RENNAISES CERTIFIÉES



© ANSSI : produits et/ou services qualifiés des entreprises au siège social / LSTI : certification ISO 27001 au 20/09/2019 / Agence du numérique en santé 2020.

880 cybercombattants du ministère des Armées

Rennes Métropole est reconnu comme LE pôle cyber du ministère des Armées en région avec la Direction Générale de l'Armement Maîtrise de l'Information (DGA-MI) et des composantes opérationnelles du Commandement de la cyberdéfense (ComCyber) et de formation.
Représentant actuellement 880 emplois, cette cyber vallée européenne (discours de Florence Parly ministre des Armées 7 septembre 2020) sera confortée : d'ici 2025 sont attendus 1 600 cyberspécialistes dans les forces armées en Ille-et-Vilaine.

Direction Générale de l'Armement Maîtrise de l'Information (DGA-MI) à Bruz : 580 cyber experts

La DGA-MI Bruz est depuis 2012 un centre référent en matière de cyberdéfense au sein des Armées.
Son activité de cybersécurité est en croissance continue depuis 10 ans avec 574 personnels sur ces sujets en 2020 (l'effectif de 2011 était de 970 emplois soit +680 personnes ou +70%). Des perspectives de 800 cyber-experts d'ici à 2025 sont tracées.
L'activité cyber-défense/sécurité représente actuellement plus d'un tiers de l'activité du centre DGA-MI de Bruz qui emploie au total 1650 personnes en 2020.

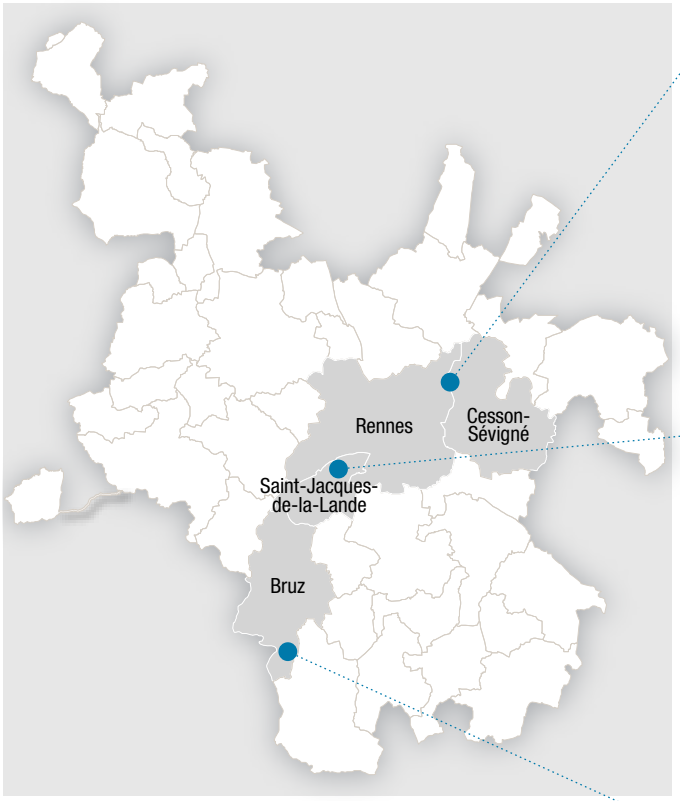
© UR1/DirCom/JLB.

Le site est spécialisé notamment dans la protection et défense des systèmes d'information du ministère des Armées, l'accompagnement et la validation technologique des développements des grands programmes d'armements, les luttes contre les attaques électromagnétiques ou l'usage de l'intelligence artificielle au service de la Défense.
Avec un rythme de l'ordre de 130 embauches par an, la DGA-MI à Bruz a pour perspective d'atteindre 2200 emplois au total d'ici 2025.

Ministère des Armées à Rennes - Saint-Jacques : 300 cybercombattants dans le « Temple de la cyberdéfense »

Outre la DGA-Mi, le ministère des Armées dispose de plus de 300 spécialistes de la cybersécurité sur le site dédié du quartier Stéphant La Maltière (Saint-Jacques-de-la-Lande). Le site regroupe désormais des équipes du centre d'analyse de lutte informatique défensive (CALID), du centre d'audit de la sécurité des systèmes d'information (CASSI), du centre de la réserve et de la préparation opérationnelle de cyberdéfense (CRPOC), ainsi que la 807ème compagnie de transmission de l'armée de Terre.
Ces implantations représentent un « investissement de plus de 200 millions d'euros entre 2019 et 2025, dans la zone de la Maletière située à Saint-Jacques-de-la-Lande, pour y construire le temple de la cyberdéfense. Deux autres bâtiments seront également construits d'ici 2025 pour accueillir les cybercombattants de demain ».
En effet, « d'ici 2025, le groupement de la cyberdéfense des armées sera entièrement regroupé à Rennes. Ce groupement créé en septembre 2020 permet actuellement d'articuler les compétences de 3 unités différentes, implantées entre Rennes et Paris : le CALID, le CRPOC et le CASSI.

FORCES EN CYBERSÉCURITÉ DU MINISTÈRE DES ARMÉES DANS RENNES MÉTROPOLE



© Audiar.

QUARTIER LESCHI

QUARTIER STEPHANT LA MALTIÈRE

DGA MAÎTRISE DE L'INFORMATION

Les effectifs du groupement de la cyberdéfense des armées monteront progressivement en puissance pour atteindre 430 personnels contre 300 aujourd'hui. » (discours de Florence Parly, ministre des Armées, 7 septembre 2020).

Des écoles et centres de formation des Armées

Les forces armées disposent également d'établissements de formation, notamment en cybersécurité : l'École des transmissions installée à Cesson-Sévigné au quartier Leschi, ainsi que les écoles de Saint-Cyr Coëtquidan à Guer (Morbihan) (ESCC).
(Effectifs non comptés dans la présente étude).

Implantation de l'ANSSI à Rennes : 200 cyberspécialistes d'ici 2026

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cyberdéfense et de cybersécurité. Service à compétence nationale, l'ANSSI est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN) qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Composée aujourd'hui de plus de 500 agents, elle continue de renforcer et atteindra 750 agents à l'horizon 2025. Cette croissance doit lui permettre de faire face à la menace cyber grandissante.

L'un des grands enjeux à venir pour l'agence est son installation sur deux nouveaux sites, en complément de ses deux implantations parisiennes historiques, à l'Hôtel national des Invalides et à la Tour Mercure. L'ANSSI va donc s'étendre en région parisienne, au sein du futur campus cyber, et à Rennes.

À Rennes–Saint-Jacques, dans le quartier de la Courrouze, la montée en puissance se fera progressivement, entre 2021 et 2026, pour atteindre la cible de 200 agents.

D'abord constituée d'une petite équipe transférée depuis Paris, le site rennais sera ensuite constitué par recrutement externe et mobilités internes.

Les missions de l'antenne seront définies en détail d'ici à 2022, sur la base des orientations déjà proposées et discutées, comme la détection des menaces, le traitement massif des data et une activité de formation pointue réservée aux agents publics de l'État.

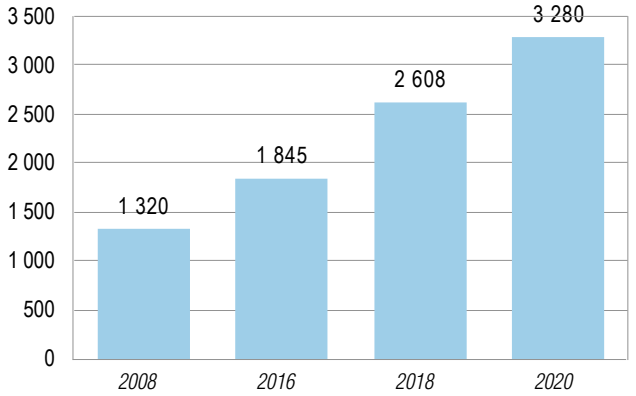
Grâce à sa proximité avec la DGA Maitrise de l'information et avec le CALID (COMCyber) du ministère des Armées, l'ANSSI a déjà établi de nombreux liens avec l'écosystème rennais. L'antenne rennaise permettra d'approfondir ces liens et d'en développer de nouveaux avec les acteurs de la recherche académique et des entreprises locales.

26 % de croissance de l'emploi privé en 21 mois

L'emploi privé est en forte croissance dans la cybersécurité : + 26 % entre janvier 2019 et septembre 2020.
Et cette augmentation est encore plus intense dans les entreprises de plus de 2 ans d'existence. En effet, l'enquête réalisée par l'Audiar auprès des 76 entreprises de la cybersécurité a permis de recueillir l'effectif exact de leur personnel. Parmi les 49 entreprises qui existaient en 2018 et ont bien voulu communiquer leur effectif 2020, on constate une croissance de 29 % des emplois en 21 mois.

L'emploi salarié privé en cybersécurité en Ille-et-Vilaine a donc été multiplié par 2,5 en 10 ans.

EMPLOI PRIVÉ DANS LA CYBERSÉCURITÉ EN ILLE-ET-VILAINE



Source : Insee et Diane Astrée. Enquête Audiar.

AIRBUS CYBERSECURITY : UNE CROISSANCE DE 20 % / AN DES EFFECTIFS DE SON SITE RENNAIS

Entité d'Airbus Defence and Space, Airbus CyberSecurity est spécialisée dans la protection des gouvernements (défense, activités militaires…) ainsi que des opérateurs d'importance vitale (OIV). Adressant tous les secteurs d'activités, Airbus CyberSecurity compte plus de 300 experts en France, dont 34 à Rennes, 35 à Toulouse et 270 à Elancourt en région parisienne.

Le site rennais ouvert en 2018 a un développement rapide qui a nécessité l'extension des locaux. Les travaux menés avec les organismes militaires (DGA, ComCyber…) sont nombreux, d'où la croissance rapide. Rennes est une place forte de la cybersécurité des armées et de l'Etat, et ces derniers ont un rôle important de prescripteurs et leaders dans la filière.

Le groupe prévoit une progression annuelle de ses effectifs de 15 à 20 % à Rennes pour 2021 et les années suivantes. Et cette croissance est plus intense dans ce territoire que dans ses autres sites français.

Le groupe participe à la création de talents en collaborant avec des formations supérieures locales. Sur le plan de la recherche et de l'innovation, Airbus CyberSecurity France vient de signer un accord avec l'IRT b<>com pour les 3 années à venir. Le groupe préside également la Chaire CNI lancée par l'IMT Atlantique. En Bretagne, il soutient également des thèses en cybersécurité, dont les travaux peuvent être intégrés à des solutions proposées par Airbus.

*Extrait de l'interview de **Frédéric Julhes**, directeur d'Airbus CyberSecurity France menée conjointement par Destination Rennes et l'Audiar.*

Une excellence académique ancrée au monde industriel

La formation en cybersécurité à Rennes : 90 doctorants et 110 étudiants spécialisés par an

Rennes dispose d'équipes de recherche de classe mondiale couvrant l'ensemble de la chaîne de la cybersécurité, de la physique au droit, en passant par l'électronique, les mathématiques et l'informatique. Actuellement, le site rennais compte plus de 200 étudiants en formation et 150 chercheurs en exercice qui travaillent spécifiquement des sujets d'excellence de la cybersécurité techniquement très avancés. Rennes est un lieu unique en matière de formation et de recherche en cybersécurité à l'échelle de la France, mais aussi en Europe.

La spécialisation en cybersécurité

90 doctorants rennais réalisent actuellement une thèse liée à la cybersécurité. Ils sont 30 à commencer une recherche tous les ans. Un tiers est financé par la DGA et la Région Bretagne, un deuxième tiers est en thèse CIFRE et un dernier tiers est soutenu par les projets européens, l'ANR ou les écoles doctorales.

110 étudiants sont inscrits en master dans des **formations spécialisées en Cybersécurité** à Rennes :

- Master informatique, parcours cybersécurité – Université de Rennes 1 ;
- Master mathématiques et applications, parcours mathématiques de l'information, cryptographie - Université de Rennes 1 ;
- Master international EIT Digital master school, parcours cybersécurité – Université de Rennes 1 ;
- Master informatique parcours recherche en cybersécurité - Université de Rennes 1 ;
- Mineure cybersécurité du programme d'ingénierie - INSA ;
- Majeure cybersécurité du programme d'ingénierie - CentraleSupélec ;
- Majeure cybersécurité du programme d'ingénierie – IMT Atlantique.

Labels de qualité délivrés par les grandes écoles, les mastères spécialisés sont destinés aux étudiants diplômés et aux actifs avec une expertise de haut niveau. Ils apportent des compétences pointues dans un domaine précis et sont reconnus par les acteurs socio-économiques en tant que tels. Dans la cybersécurité, deux mastères spécialisés sont proposés localement :

- IMT Atlantique et CentraleSupélec : mastère spécialisé en Cybersécurité (32 places). La moitié des promotions est composée de jeunes diplômés et l'autre d'actifs en emploi ;
- École de Saint-Cyr Coëtquidan : Mastère Spécialisé Opérations et Gestion des Crises en Cyberdéfense – Saint-Cyr Coëtquidan Guer.

En complément des mastères spécialisés, le site rennais dispose également de nombreuses formations continues pour les actifs et les militaires. Elles sont dispensées par les grandes écoles comme l'ETRS ou l'IMT Atlantique, les entreprises comme Amosys et l'université de Rennes 1.

Plus d'un millier d'étudiants formés en cyber

Prise au sens large, la cybersécurité est enseignée auprès d'un millier d'étudiants dans de nombreux établissements et formations :

- ESIR : diplôme d'ingénieur dans la spécialité technologie de l'information et dans une des options Systèmes d'information, Télécommunications et réseaux et IoT, sécurité et ville intelligente ;

- Rennes 1 ISTIC (UFR informatique et électronique) : formation d'architectes logiciels avec des bases solides en cybersécurité ;
- IEP Rennes : master en Sécurité défense et intelligence stratégique (SE-DEFIS) ;
- ENS Rennes : ingénierie de systèmes complexes (électronique, informatique, mécatronique, etc.) ;
- CNAM Bretagne Rennes : licence Pro Analyste en sécurité des systèmes télécoms réseaux et informatiques ;
- INSA Rennes : diplôme d'ingénieur en Informatique ;
- IMT Atlantique : formation d'Ingénieur Généraliste ;
- CentraleSupélec : diplôme d'ingénieur ;
- ENS Rennes : diplômes d'ingénierie de systèmes complexes (électronique, informatique, mécatronique, etc.) ;
- Lycée Maupertuis à Saint-Malo : BTS SN-IR (Systèmes Numériques & Informatique et Réseaux) ;
- Epitech : parcours général post-bac et MSc Pro Transformation Digitale et Innovation Technologique ;
- IUT Bretagne propose 17 formations entre Brest, Lannion, Rennes, Saint-Malo et Vannes liées à la cybersécurité.

14 entreprises cyber rennaises ont accueilli pour 970 mois de stage en immersion

Les entreprises participent aussi directement à la formation en recevant des stagiaires. Dès 2013, 67 étudiants des universités rennaises ont été reçus dans 14 entreprises rennaises de la cybersécurité pour un total de 970 mois cumulés de formation en immersion.

1ère force de recherche après Paris avec 150 chercheurs spécialisés

Un tissu de recherche en cybersécurité très dense et diversifié

Les forces de recherche en matière de cybersécurité à Rennes sont constituées de 150 personnes sur des thématiques technologiquement très avancées. Elles sont présentes dans les organismes de recherche et équipes de projets spécialisées comme l'IRISA/Inria dont les équipes de recherche CIDRE, EMSEC, TAMIS…, l'IRMAR ou le centre de Recherche des Écoles de Saint-Cyr Coëtquidan (dans le Morbihan).

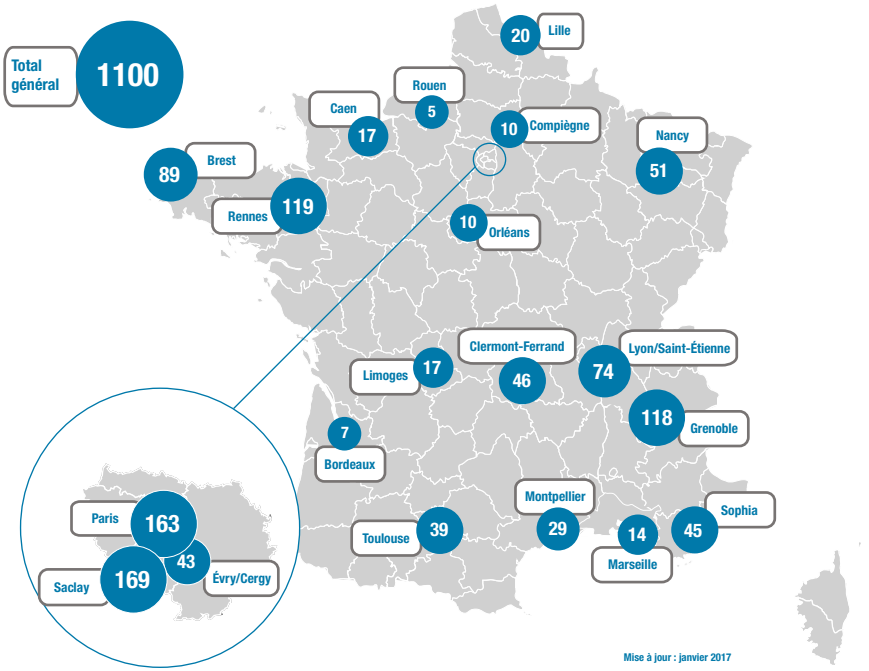
Plus largement, on dénombre 560 personnes dédiées à la recherche sur des thématiques en relation avec le monde de la cybersécurité dans plusieurs organismes et laboratoires de recherche :

- Inria/IRISA mène des recherches en informatique, en mathématiques appliquées et en traitement du signal et des images ;
- Institut de recherche en mathématiques de Rennes (IRMAR), réalise en particulier des recherches en cryptographie ;
- Institut d'Électronique et de Télécommunications de Rennes (IETR) poursuit des activités de recherche dans le domaine des sciences et technologies de l'information et de la communication ;
- Centre de Recherche des Écoles de Saint-Cyr Coëtquidan : la recherche y est organisée autour de quatre thèmes principaux : Éthique et environnement juridique, Défense et sécurité européennes, Action globale et forces terrestres, Science et technologie de la défense ;
- IODE, le laboratoire de recherche en droit, a développé un axe de recherche sur le droit numérique et les sciences où la cybersécurité et la cybercriminalité sont abordés sous l'angle juridique ;

- LAB-STICC, installé à Lorient-Brest et ayant une activité en lien avec le pôle rennais, est un laboratoire de recherche multidisciplinaire dans le domaine des sciences et technologies de l'information et de la communication dont le thème principal est « du capteur à la connaissance ».

La recherche rennaise peut également compter sur le Laboratoire Haute Sécurité (LHS) qui est une plateforme de recherche partagée entre Inria, CentraleSupélec, l'Université de Rennes 1 et le CNRS. Spécialisé pour la recherche en virologie et l'analyse de la menace, le LHS est aussi un incubateur au service du transfert industriel.
Des établissements de recherche rennais sont aussi membres des laboratoires d'excellence Labex Henri Lebesgue, qui travaillent notamment sur la crypographie et COMIN Labs « COMmunication and INFormation sciences Laboratories » qui permet de progresser dans le domaine de l'analyse, des probabilités et des statistiques et d'explorer leurs interactions avec les problématiques liées aux systèmes complexes rencontrés dans les applications socio-économiques (santé, numérique, matériaux…). Les deux laboratoires ont pour coordinateur Rennes selon les données du Programme d'investissement d'avenir. Au total, 7 millions d'euros sont destinés aux partenaires de Lebesgue et 14 millions d'euros à ceux de COMIN Labs.
L'IRT b<>com complète ce dispositif.

RÉPARTITION GÉOGRAPHIQUE DES PERSONNELS EN CYBERSÉCURITÉ



© Bulletin de la société informatique de France – numéro 11, septembre 2017.

Une croissance des effectifs de la recherche

La croissance des effectifs de chercheurs en cybersécurité est intense : en janvier 2017, Allistène recensait 119 personnes à Rennes (1er site après Paris). Depuis, la capitale bretonne a recruté près de 30 personnes.

41 brevets déposés par les entreprises rennaises de cybersécurité

Bien que toutes les innovations ne fassent pas l'objet de brevets, ces partenariats de recherche ont notamment permis les dépôts de nombreux brevets. Entre 2006 et 2019, 41 brevets ont été déposés par les entreprises de la cybersécurité comme Acklio, Cailabs, Orange, etc. Ils concernent entre autres la sécurisation des transmissions de données, de l'accès internet dans le réseau domestique ou encore l'apprentissage de procédés de compression.

La CyberSchool de Rennes : unique école universitaire de recherche en cybersécurité en France

La CyberSchool

L'école universitaire de recherche (EUR) en cybersécurité « CyberSchool » a ouvert en septembre 2020. Pensée sur le modèle des graduate schools, il s'agit de l'unique école universitaire de recherche en cybersécurité en France.

Son objectif est de doubler le nombre d'étudiants en cybersécurité à Rennes pour atteindre à terme un total d'environ 580 personnes.

D'envergure internationale, elle propose outre des formations en anglais, un programme de mobilité au sein d'un réseau d'universités étrangères prestigieuses et des bourses d'excellence pour attirer les meilleurs étudiants en France et à l'étranger.

La CyberSchool offre une formation de pointe innovante et internationale adossée à la recherche au niveau Master et Doctorat, pour former des futurs experts, ingénieurs et scientifiques en cybersécurité. Elle intègre dans son parcours de fortes synergies entre le cursus académique, la recherche et l'expérience professionnelle.

L'EUR s'appuie sur une approche interdisciplinaire associant mathématiques, sciences et technologies numériques et sciences humaines et sociales au sein de six axes de recherche : Cryptographie / Droit et protection de la vie privée / Intelligence artificielle et sécurité / Matériel et systèmes embarqués / Méthodes formelles et sécurité / Sécurité des logiciels et des systèmes

Portée par l'Université de Rennes 1, CyberSchool s'appuie sur les expertises des universités rennaises, de quatre grandes écoles d'ingénieurs (CentraleSupélec, IMT Atlantique, INSA Rennes et ENSAI), de l'ENS Rennes et de Science-Po Rennes, en lien étroit avec le CNRS et Inria, et en collaboration avec la Région Bretagne, Rennes Métropole et la Direction Générale de l'Armement.

Elle s'appuie sur des synergies fortes entre la recherche académique et la R&D en entreprise : alternance, projets de recherche et stages en laboratoire universitaire ou industriel.

Lauréate de la 2ème vague d'appel à projets Écoles universitaires de recherche du Programme d'investissements d'avenir, CyberSchool bénéficie d'un financement de l'État à hauteur de 5,75 millions € sur 10 ans.

Le projet C CUBE

C CUBE (pour « Centre de Compétences en Cyber sécurité » ou C3) est un projet porté par la région Bretagne, des établissements académiques renais (CentraleSupélec, ENS de Rennes, ENSAI, IMT Atlantique, INSA de Rennes, IEP, Université Rennes 1 et Université Rennes 2) et des grands organismes de recherche (CNRS et Inria).

Il implique une large communauté pluridisciplinaire (électroniciens, informaticiens, mathématiciens, juristes, géostratèges, sociologues…) et porte une ambition scientifique de haut niveau interdisciplinaire.

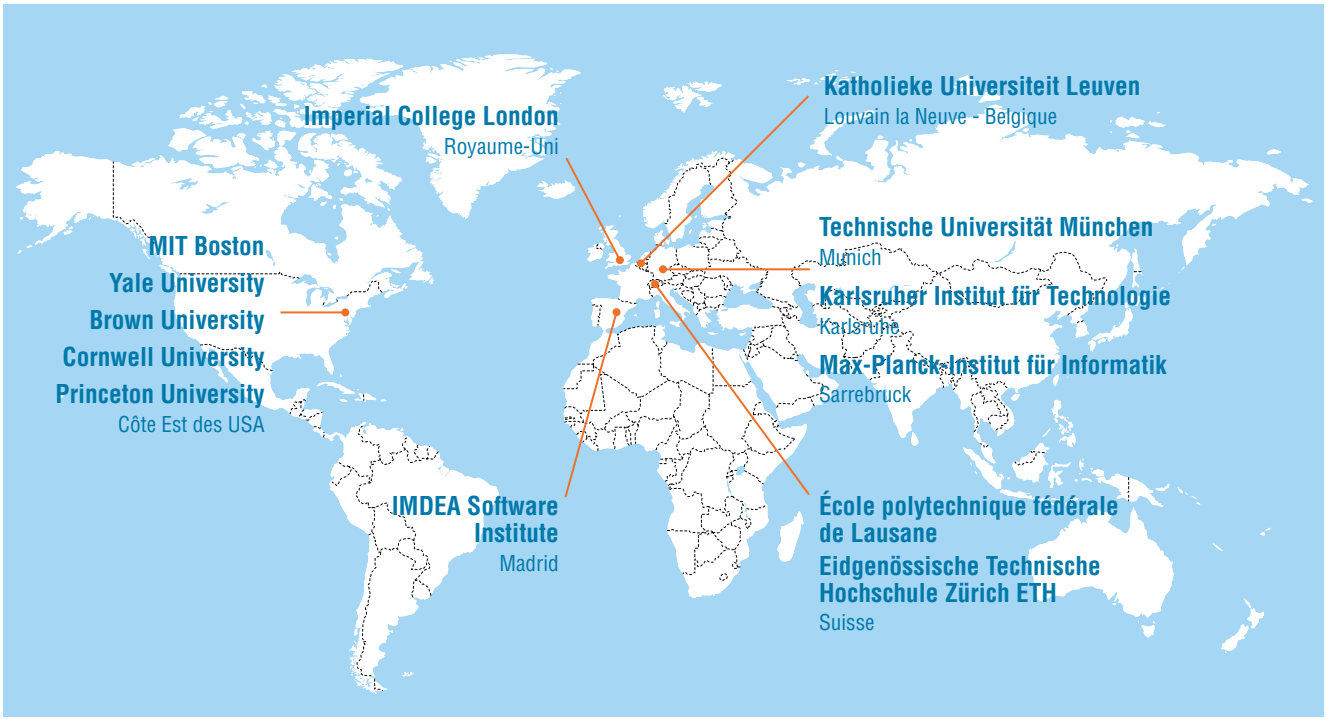
C3 coordonnera les plateaux techniques académiques en cybersécurité et hébergera le Laboratoire Haute Sécurité, l'EUR CyberSchool, le DIH Cyber Sécurité et le siège du Pôle Excellence Cyber.

C3 s'appuiera sur un lieu physique permettant la co-localisation d'activités de la cybersécurité, sur le campus de Beaulieu de Rennes et sera inscrit au prochain CPER (Contrat de plan État-Région).

Une excellence reconnue à l'international

Des partenariats avec des universités prestigieuses

Les établissements prestigieux et innovants comme le MIT ou Havard ont des conventions d'échanges avec les partenaires de la CyberSchool rennaise.



© Audiar.

Source : CORDIS - Union Européenne - Traitement Audiar.

De fortes connexions à l'international via les projets de recherche collaboratifs

H2020

Les entreprises et les forces de recherche rennaises sont impliquées dans plusieurs projets majeurs soutenus par le **programme européen H2020**.

L'UMR 6074 IRISA et l'INRIA Rennes - Bretagne Atlantique sont engagés dans les projets SPARTA, PROMETHEUS, POPSTAR (Reasoning about Physical properties Of security Protocols with an Application To contactless Systems) et VESTA (VErified STAtic analysis platform). Près de 4,5 millions d'euros ont été levés pour les partenaires bretons grâce à ces programmes.

Le consortium SPARTA, piloté par le CEA, rassemble un groupe de 44 acteurs au sein de 14 États Membres de l'UE, incluant l'ANSSI, l'IMT, INRIA, Thales et YesWeHack pour la France. Il propose 4 grands programmes de recherche : détection et lutte contre les attaques informatiques, validation de propriétés de sécurité et de sureté pour des objets et services en environnement dynamique, solutions pour sécuriser les environnements matériels et développement des intelligences artificielles sûres et compréhensibles.

Le projet PROMETHEUS qui réunit des universités européennes (Université de Rennes 1, Ruhr-Universitaet Bochum, Orange, Thales, Weizmann Institute Of Science…) a pour objectif de proposer des constructions cryptographiques résistantes aux attaques quantiques.

En mutualisant toutes les expériences et les compétences, les défis et les capacités, les programmes H2020 en cybersécurité contribuent au renforcement de l'autonomie stratégique de l'UE.

LABORATOIRES DE RECHERCHE PUBLIQUE POSITIONNÉS SUR LA CYBERSÉCURITÉ

Acronyme du projet	Type de projet	Organisme portant le contrat de subvention	Acronyme du laboratoire impliqué	Nom du laboratoire impliqué	Nom du chercheur contact (PI)
PROMETHEUS	Projets collaboratifs de recherche et d'innovation (RIA, IA)	UR1	UMR 6074	Institut de recherche en informatique et systèmes aléatoires (IRISA)	Pierre-Alain FOUQUE
SPARTA	Projets collaboratifs de recherche et d'innovation (RIA, IA)	Inria RBA	Inria RBA		Thomas JENSEN
POPSTAR	POPSTAR	CNRS	UMR 6074	Institut de recherche en informatique et systèmes aléatoires (IRISA)	Stéphanie DELAUNE
VESTA	Projets individuels d'excellence (ERC)	CNRS	UMR 6074	Institut de recherche en informatique et systèmes aléatoires (IRISA)	David PICHARDIE

La cartographie des liens construits entre les sites rennais et les territoires étrangers via les projets H2020[1] montre bien le rayonnement et l'ouverture à l'international. L'Espagne est le pays le plus intensément connecté à Rennes en cyber avec des relations établies avec les Universités de Madrid, Malaga, Thales Alenia Space España, Telefónica Investigación y Desarrollo, Nokia Spain, Atos Spain… Du point de vue des collaborations, des liens forts unissent également Rennes avec l'Allemagne.

1 20 projets H2020 dont le thème principal n'est pas la cybersécurité mais qui en ont une composante importante (ex : 5G et la sécurité afférente).

Les autres projets collaboratifs

Le soutien des pôles de compétitivité et des institutions (ANR, Région Bretagne, ministères…) via leurs appels à projets dynamise également l'écosystème. En 10 ans, 27 projets ont rassemblé les entreprises rennaises et leurs partenaires nationaux et internationaux autour de sujets clés technologiquement avancés.

Acteur de l'innovation technologique, l'IRT b<>com a contribué à 13 projets européens dont le thème principal n'est pas la cybersécurité mais qui ont une composante importante en cyber. Ceux-ci, en collaboration avec des acteurs majeurs européens (Orange, Thales, Nokia, Ericsson, etc.) notamment à travers le projet 5G-ENSURE dont l'objectif est de définir une architecture de sécurité.

RELATIONS À L'INTERNATIONAL : NOMBRE DE COOPÉRATIONS INTERNATIONALES DANS LES PROJETS CYBER RENNAIS

Un écosystème avec de fortes intensités relationnelles

La Cyberdéfense Factory : lieu unique militaro-civil d'éclosion de startups

En 2019 a été créée la « Cyberdéfense Factory » un espace dédié à favoriser l'innovation en offrant un hébergement, l'accès à des données d'intérêt cyber et la capacité à tester avec des opérationnels du ministère des Armées. Grands groupes, PME et la recherche académique y travaillent au contact des équipes militaires.

Installé sur 200 m² dans le quartier de La Courrouze à quelques centaines de mètres du ComCyber, ce site unique en France, coordonné par l'Agence de l'innovation de Défense, permet à des universitaires et des entreprises de travailler avec des experts de la DGA-MI et du Comcyber, de façon agile et réactive. En vitesse de croisière, une vingtaine de personnes travailleront sur place, pour des périodes de 6 à 12 mois, avec une dizaine de projets menés en parallèle.

La partie incubateur a accueilli sa première start-up en 2020 : GLIMPS, créée par quatre ingénieurs de DGA-MI et spécialisée dans la rétro-conception logicielle. D'autres appels à projets permettront de rejoindre la Factory.

Un fonds de prise de participations de 80 millions d'euros[1] à l'échelle nationale (porté par ACE Management — avec l'appui de l'expertise technique du ministère des Armées) pourra également accompagner les besoins de financement des startups du domaine cyber.

© D.R.

1 ACE Management est une société de gestion de fonds et spécialisée dans l'investissement en capital au service de l'industrie et de l'innovation. Elle gère 3 grandes lignes de produits, représentant 500 millions d'euros de capitaux : Aerofund (aéronautique), Brienne (cybersécurité et défense) et Atalaya (maritime). Les souscripteurs des fonds gérés par ACE Management sont les groupes industriels et des institutionnels de premier plan parmi lesquels figurent : Airbus, Airbus Group, Safran, Airbus Helicopters, Thales, Naval Group, Louis-Dreyfus Armateurs, CEA, Orano, GICAN (Groupement des Industries de Construction et Activités Navales), Bpifrance, Fonds de Solidarité des Travailleurs du Québec (FSTQ), Société Générale, Crédit Agricole, CIC, AXA, et 4 Régions (Occitanie, Nouvelle Aquitaine, Pays de la Loire et Centre-Val de Loire). Source : www.acemanagement.fr

Des coopérations entre recherche civile et militaire

Un accord général de partenariat entre la DGA et le monde académique

Le ministère de la Défense, représenté par la Direction générale de l'armement (DGA), la Région Bretagne et 11 universités, écoles d'ingénieurs et institutions de la recherche ont signé en 2014 un Accord général de partenariat (AGP) pour la recherche en cyberdéfense. Les établissements rennais figurent parmi les 11 signataires académiques[1] bénéficiant de cet acte. Cet accord définit une vision stratégique commune en matière de recherche et de valorisation en lien avec le tissu industriel. Il permet, par exemple, de financer des thèses dans le domaine cyber. Grâce aux différents dispositifs de soutien à la recherche & technologie de la DGA et à l'abondement de la Région, près de 2 millions d'euros par an sont investis dans l'écosystème breton de recherche cyber au titre de cet accord général de partenariat.

Trois chaires industrielles cybersécurité associant recherche académique, ministère des Armées et entreprises locales

L'intensité des relations entre les entreprises et la recherche se matérialise notamment par la création et le développement des chaires industrielles. Trois chaires, c'est-à-dire trois collectifs autour de projets d'enseignement, de recherche et de développement industriel, dont l'objet est la cybersécurité, sont actuellement actives dans l'Est breton :

- Saint-Cyr Coëtquidan possède une Chaire Cyberdéfense depuis 2012 en partenariat avec Sogeti et Thales. Elle prépare notamment les futurs officiers de l'armée de terre à faire face aux cybermenaces. Son but est de développer une réflexion scientifique de premier plan sur les dimensions stratégiques du cyberespace ;

- IMT Atlantique a mis en place la Chaire Cyber CNI dédiée à la cybersécurité des Infrastructures Critiques depuis 2016 en partenariat avec le Pôle d'excellence cyber, la fondation et Institut Mines-Telecom, la Région Bretagne, Airbus Defense and Space, Amossys, BNP Paribas, EDF et Nokia Bell labs. Elle a été renouvelée pour 3 ans en début d'année 2019 ;

- CentraleSupélec a développé une Chaire Cybersécurité sur l'Analyse de la Menace en partenariat avec la Région Bretagne, la DGA-MI, le Pôle d'excellence cyber et l'Inria.

1 Ministère de la Défense (DGA), Région Bretagne, Centre national de la recherche scientifique (CNRS), Institut national de recherche en informatique et en automatique (INRIA), UNIVERSITE européenne de Bretagne (UEB), UNIVERSITE de Bretagne-Sud (UBS), UNIVERSITE de Bretagne occidentale (UBO), UNIVERSITE Rennes 1, UNIVERSITE Rennes 2, École normale supérieure de Rennes (ENS Rennes), École supérieure d'électricité (SUPELEC), Institut national des sciences appliquées de Rennes (INSA Rennes), Télécom Bretagne.

Des liens forts entre entreprises et établissements de recherche rennais

Des acteurs rennais très fortement impliqués dans le Pôle d'excellence cyber

Le Pôle d'excellence cyber (PEC) regroupe aujourd'hui une cinquantaine de membres, dont la moitié sont des sociétés ou des sites d'écoles et universités implantées en Ille-et-Vilaine :

11 sociétés ayant un site en Ille-et-Vilaine

Airbus CyberSecurity
Capgemini
Systancia
SIB
Amossys
Thales
Safran
Secure-IC
Sopra Steria
Cisco
YesWeHack
Orange

14 sites d'écoles et universités

Campus E.S.P.R.I.T / ESL
Sciences-Po Rennes
EPITA
ENS Rennes
ENSAI
CentraleSupélec Rennes
École des Transmissions (ETRS)
Université Rennes 1
CNAM Bretagne
INSA Rennes
Groupe Saint-Jean
IMT Atlantique
Écoles de Saint-Cyr Coëtquidan (ESCC)
ISEN-YNCREA

Initié en 2014 par le ministère des Armées (pacte défense cyber) et par le Conseil régional de Bretagne (Pacte d'avenir) avec une portée nationale et un objectif de rayonnement international, le PEC a pour ambition d'accélérer la construction d'une filière en cybersécurité-cyberdéfense souveraine ancrée en Bretagne et d'envergure nationale, contribuant au développement européen et au rayonnant à l'international.

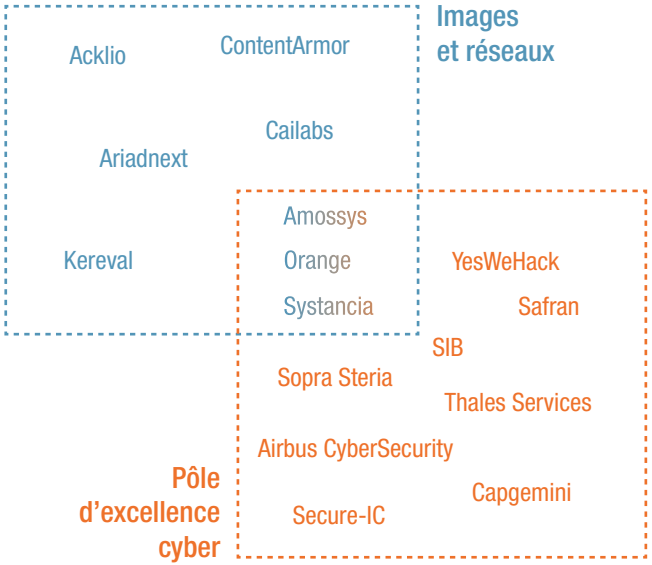
Le Pôle d'excellence cyber s'appuie sur le tissu académique et industriel régional ainsi que sur des partenaires nationaux ou d'autres territoires[1]. Il a pour mission de stimuler le développement de l'offre de formation cyber (initiale, continue, supérieure), la recherche académique cyber, la base industrielle et technologique de cybersécurité, avec une attention particulière portée aux PME-PMI innovantes, y compris à l'export. Le Pôle d'excellence cyber répond ainsi à trois enjeux majeurs, au profit de la communauté nationale de cyberdéfense et de cybersécurité : disposer des compétences nécessaires pour répondre aux besoins de développement de la filière, d'une offre de recherche en adéquation avec les besoins du ministère et des industriels, et de produits et services de confiance.

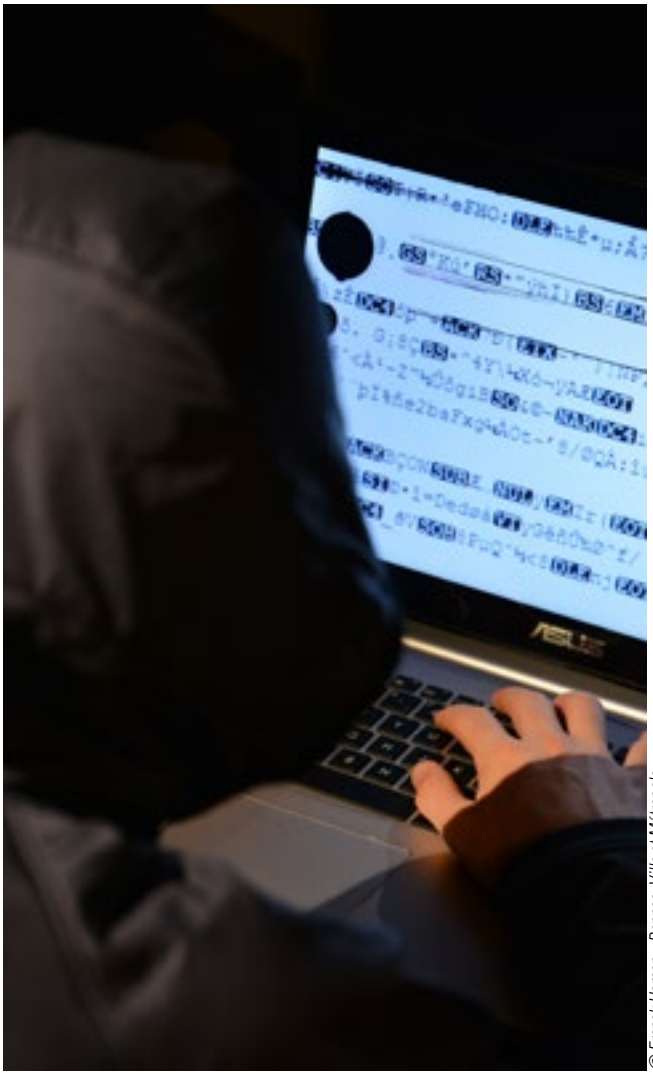
1 https://www.pole-excellence-cyber.org/presentation-du-pole/

Des entreprises insérées dans les réseaux d'innovation dédiés

Les startups et scaleups de la cybersécurité sont très attentives à la fois à leur certification et aussi à leur insertion dans les réseaux d'innovation ; de fait, 16 entreprises et groupes spécialistes en cybersécurité sont membres du PEC et/ou du pôle de compétitivité Images et réseaux.

ENTREPRISES PRIVÉES RENNAISES DE LA CYBERSÉCURITÉ DANS LES RÉSEAUX D'INNOVATION





© Franck Hamon - Rennes, Ville et Métropole.

Une communauté reconnue et récompensée

Des startups accompagnées et labellisées

Des startups locales récompensées par le Pass French Tech et d'autres prix

Secure-IC, Cailabs et Famoco ont été labellisés par la French Tech via le Pass French Tech, accordé aux entreprises à fort développement, après sélection. Sélectionnées et accompagnées de manière privilégiée par les opérateurs territoriaux du Pass French Tech, ces pépites bénéficient de l'appui de Bpifrance, la DGE, Business France, Coface, l'INPI, l'AFPC et l'AFIC.

Sekoia a été récompensée en 2019 par Banking Cyber-Security Innovation Awards de Wavestone et Société Générale : Les « Banking Cybersecurity Innovation Awards » s'adressent aux startups et PME européennes innovantes pour qu'elles fassent découvrir et qu'elles mettent en valeur leurs solutions en matière de cybersécurité, en particulier sur les thématiques de la sécurité de la Blockchain, les services FinTech, le paiement mobile…

Des entreprises rennaises accompagnées par le fond DefInvest et RAPID

Unseenlabs, entreprise rennaise à la croisée de la cybersécurité et des telecoms, a bénéficié d'un apport de DefInvest dans sa dernière levée de fonds (au total 7,5 millions d'euros) pour accompagner son projet de surveillance maritime par nano-satellites. Le ministère des Armées et Bpifrance ont créé fin 2017 Definvest pour soutenir le développement de PME stratégiques pour la défense. L'objectif est de sécuriser le capital d'entreprises d'intérêt stratégique pour le secteur de la défense, de soutenir leur développement notamment en matière d'innovation et de participer à des opérations de croissance externe permettant de consolider la filière.

PASS FRENCH TECH

Les sociétés rennaises de la cybersécurité ont également obtenu environ 6,3 millions d'euros de subvention au titre de « RAPID » (Régime d'Appui pour l'Innovation Duale) depuis la création de celui-ci. Dispositif mis en place par la DGA (Direction générale de l'armement) et la DGE (Direction générale des entreprises), il subventionne des projets de recherche industrielle ou de développement expérimental intéressant le secteur de la défense. Les projets éligibles doivent être innovants, à fort potentiel technologique et présenter des applications à la fois sur les marchés militaires et civils.

La French Tech Rennes Saint-Malo membre du réseau #Security #Privacy de la French Tech France

Rennes Saint-Malo, Montpellier et Côte d'Azur font partie du réseau #Security #Privacy de la French Tech France, réseau animé par le Pôle d'excellence cyber.

Des talents internationalement reconnus implantés sur le territoire

Des lauréats de l'European Research Council et de l'Institut universitaire de France

Stéphanie Delaune (DR CNRS, IRISA) et David Pichardie (PR ENS Rennes, IRISA) ont été lauréat de l'ERC pour leurs travaux en lien avec la cybersécurité et ont chacun reçu une bourse de plusieurs millions d'euros. En effet, le Conseil européen de la recherche (ERC) accorde un soutien individualisé à des scientifiques qui mènent des projets dans des domaines de recherche en émergence, pour des applications qui inaugurent des approches non conventionnelles et innovantes. Les projets retenus pour un financement ERC sont sélectionnés sur la base d'avis d'experts internationaux, avec l'excellence (du porteur et du projet) comme seul critère.

Stéphanie Delaune travaille sur la vérification des protocoles cryptographiques pour les systèmes sans contact. Elle souhaite réaliser la preuve formelle, mathématique, du fonctionnement adéquat du protocole de sécurité. Les travaux de recherche de David Pichardie concernent notamment le domaine de la preuve de programme, qui permet de s'assurer qu'un logiciel se comportera comme on l'avait prévu, durant son exécution. C'est essentiel pour certains logiciels qualifiés de critiques (logiciels embarqués sur les téléphones mobiles, les cartes bancaires mais aussi au cœur des avions, des centrales nucléaires ou des transports) car leur éventuel dysfonctionnement pourrait provoquer des catastrophes humaines et financières.

Le territoire compte également deux lauréats de l'Institut universitaire de France (IUF) : Pierre-Alain Fouque (professeur Université Rennes 1, IRISA) et Gildas Avoine (professeur INSA Rennes, IRISA) ont été primés pour leur expertise en cybersécurité.

Pour favoriser le développement de la recherche de haut niveau et viser l'excellence de l'université, IUF récompense chaque année 110 enseignants-chercheurs. Pendant cinq ans, ces derniers bénéficient d'une promotion exceptionnelle de leur recherche à travers l'attribution de moyens financiers et une compensation de décharge de service. Après examen de leur candidature par un jury international qui apprécie la qualité du travail scientifique et le projet de recherche, les candidats sont sélectionnés et deviennent alors membres actif de l'IUF pendant 5 ans.

Des gagnants de l'European Cybersecurity challenge

5 jeunes étudiants ayant participé en équipe de France à l'European Cybersecurity challenge (ECSC) de 2018 ont des attaches en Bretagne (4 personnes formées à l'ENSIBS et 1 personne actuellement en poste à Cesson-Sévigné chez SII Group). Ils ont remporté la 2ème place européenne.

6 Rennais parmi les 100 de la Cyber

Le magazine l'Usine Nouvelle [1] a repéré 6 personnalités rennaises parmi les « 100 de la Cyber » :

- Adrien Facon, Directeur recherche et innovation de Secure-IC, Rennes « prodige du quantique »,
- Patrice Georget, Capitaine de la brigade numérique de la gendarmerie nationale, Rennes « à l'écoute 24h/24h »,
- Jean-Louis Lanet, Responsable du laboratoire de haute sécurité (Inria), Rennes « chasseur de malware »,
- Jean-Marc Jézéquel, Directeur de l'IRISA et coordinateur de la recherche du PEC, Rennes « chef d'orchestre de la cyber »,
- Frédéric Cuppens, porteur de la chaire de cybersécurité des infrastructures critiques (réseaux d'énergie, process industriels, systèmes financiers...), fondée sur le campus de l'IMT Atlantique à Rennes « l'apôtre de la cyber-résilience »,
- Clément Domingo, expert technique cybersécurité Sopra Steria, Rennes « champion de la faille ».

1 Le choix des 100 Français qui font la cybersécurité a été réalisé par la rédaction Usine Nouvelle. Les candidats ont été retenus pour l'impact de leur action au sein de la communauté cyber et le niveau de reconnaissance auprès de leurs pairs après avis de plusieurs experts du domaine pour tester et compléter cette sélection. L'Usine Nouvelle a également respecté le souhait de certains de ne pas apparaître dans cette sélection pour des raisons de sécurité ou de discrétion du fait de leurs travaux.

© MRW Zeppeline, Destination Rennes.

Des événements économiques majeurs en cybersécurité à Rennes

3 500 visiteurs à l'European Cyber Week

Avec une hausse de 70 % des congressistes et deux fois plus de partenaires, la 4ème édition de l'European Cyber Week à Rennes a pris un essor considérable en 2019.

Plus de 3 500 personnes ont participé à ce rendez-vous annuel de novembre qui réunit entreprises, laboratoires de recherche, institutions et étudiants européens dans le cadre de conférences techniques et scientifiques, de rencontres d'affaires et d'évènements.

Les visiteurs provenaient de près de 14 pays différents.

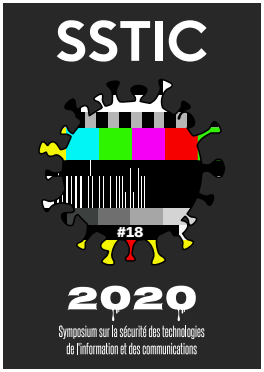
Annulée en 2020 pour cause de crise sanitaire (confinement), la prochaine édition de l'European Cyber Week se tiendra à Rennes du 16 au 18 novembre 2021.

Breizh CTF (Capture the Flag) de Rennes

Le Breizh CTF est une compétition de sécurité informatique. Il est ouvert à tous, professionnels, étudiants, hackers passionnés de sécurité informatique. La prochaine édition se tiendra en 2021.

Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)

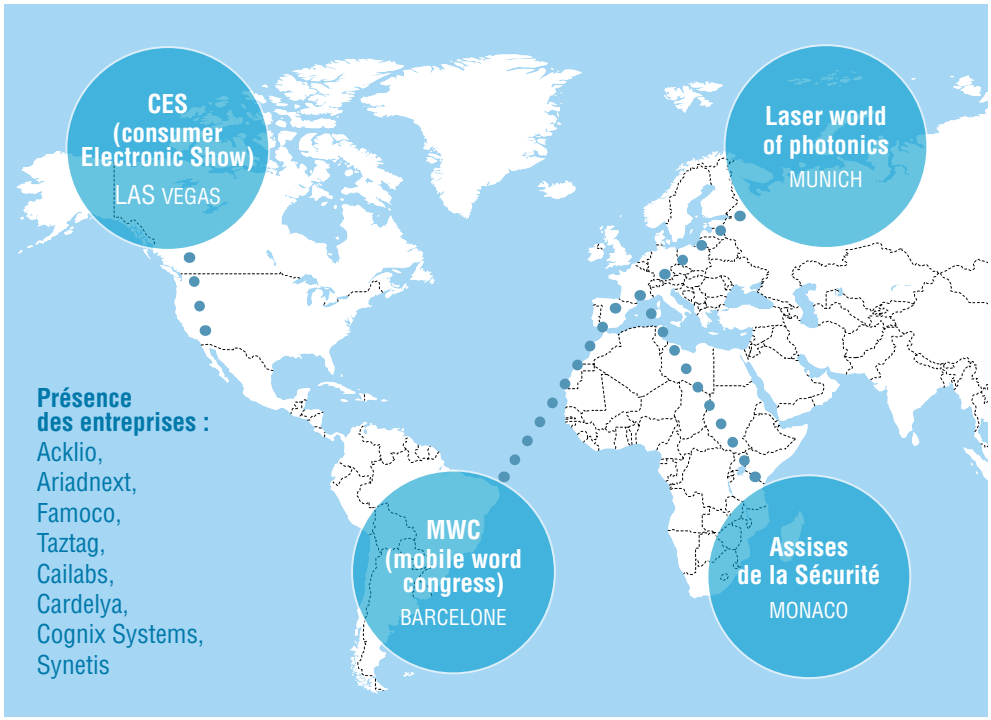
Le SSTIC est une conférence annuelle sur le thème de la sécurité de l'information. Elle rassemble chaque année, en juin, environ 800 personnes de différents horizons : universités, industrie, organisations gouvernementales, autour de présentations sur l'état actuel de la sécurité informatique en France et dans le monde.



Des entreprises présentes dans les salons internationaux

Les entreprises rennaises de la cybersécurité sont présentes sur les salons internationaux comme le CES de La Vegas, les Assises de la Sécurité à Monaco, le Mobile World Congress de Barcelone, le Laser world of photonics à Munich, le IT-sa Messe à Nuremberg ou le Farnborough International Airshow au Royaume-Uni.
Elles sont également présentes dans les salons nationaux de référence comme Milipol, salon professionnel consacré à la sécurité intérieure des États, ou le Salon international de l'aéronautique et de l'espace de Paris-Le Bourget. Sans oublier, bien sûr, le Forum international de la cybersécurité (FIC) qui se tient tous les ans en janvier, à Lille.

SALONS INTERNATIONAUX



Source : Sites internet des salons, 2018 et 2019

© Audiar.

Une métropole accompagnatrice et facilitante

Rennes Métropole, une collectivité impliquée

Un soutien à l'investissement

Depuis 2014, Rennes Métropole a versé plus de 1,5 million d'euros de subvention pour soutenir 10 dossiers d'entreprises de la cybersécurité représentant 8 millions d'euros d'investissement et 166 créations de postes.

Plus globalement, Rennes Métropole et la Région Bretagne s'impliquent fortement de concert pour accompagner l'émergence de la filière de cybersécurité de confiance en s'attachant à mettre en place un environnement favorable au profit des entreprises, des chercheurs et des initiatives collectives.

Un territoire acteur de la cybersécurité au service de la smart-city

La Métropole de Rennes, elle-même e-administration, est également impliquée sur le sujet de la safecity et est partenaire du Comité stratégique de filière (CSF) des industries de sécurité, en particulier sur le grand projet « les territoires de confiance », dont le but est d'assurer la sécurité des villes intelligentes connectées.

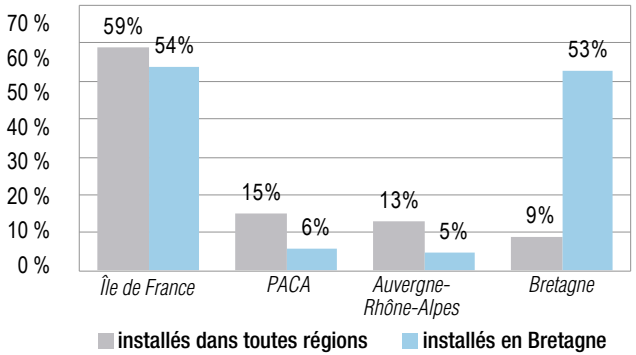
Rennes Métropole est également membre du Pôle d'excellence cyber.

Des actions pour relever les enjeux de recrutement

La Bretagne : une région attractive pour les talents de la cyber

Selon une enquête de l'APEC, l'excellence bretonne en matière de cybersécurité est reconnue. Ainsi, les informaticiens interrogés placent la Bretagne au 3ème rang des régions (hors Paris) les plus à la pointe sur la cybersécurité, après PACA et Auvergne Rhône-Alpes. Les informaticiens bretons, déjà installés dans cet écosystème performant, la classent même en 1ère position des régions françaises hors Paris.

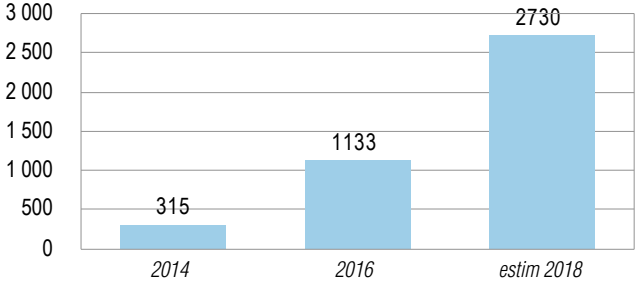
RÉGIONS LES PLUS INNOVANTES EN CYBERSÉCURITÉ, SELON LES INFORMATICIENS (deux réponses possibles)



Des tensions permanentes sur le recrutement

Le secteur de la cybersécurité fait face à d'intenses besoins en main d'œuvre, avec un doublement des offres à l'échelle nationale entre 2016 et 2018.

OFFRES D'EMPLOI DIFFUSÉES PAR L'APEC POUR DES POSTES EN CYBERSÉCURITÉ (FRANCE ENTIÈRE)



À l'échelle locale, un regard rapide sur les offres d'emplois actuelles en cybersécurité montre une forte attente des entreprises d'Ille-et-Vilaine : 232 postes sont publiés sur le site www.recrutement-rennes.com au 14/10/2020.

Cette plateforme recrutement-rennes.com est le guichet fédérateur de l'emploi local. À l'initiative de Rennes Métropole, ce service gratuit pour les candidats et pour les entreprises qui recrutent est actif depuis mi-2019. Il propose actuellement un total de 13 700 offres, tous domaines d'activité.

Une GPEC territoriale sur la « cybersécurité »

Considérant le fort besoin en ressources humaines, Rennes Métropole a confié à We-Ker (fusion de la Mission locale et de la MEIF) la mise en place d'une gestion prévisionnelle de l'emploi et des compétences (GPEC) territoriale spécifique à la cybersécurité.

Ses objectifs sont multiples :

- mettre en cohérence les ressources humaines du territoire avec les besoins des employeurs,
- accompagner la montée en compétence de certaines filières non spécialisées afin que les personnes formées puissent être employées dans la cybersécurité,
- développer l'attractivité, la lisibilité et l'accessibilité des métiers de la cybersécurité qui peuvent être jugés, en première lecture, comme très spécialisés, réservés à des seuls profils d'ingénieurs spécialisés et réduits quelque fois à une dimension technique.

Afin de mettre en œuvre ces objectifs, différentes actions sont déjà menées comme une enquête sur les modalités de captation des nouveaux profils, la réflexion autour de modalités de recrutement partagées et la mobilisation de réseaux spécifiques.

Un travail sur les viviers mobilisables et les compétences attendues par les entreprises est également en cours, afin de conforter l'attractivité de Rennes où, au regard des multiples opportunités, une carrière en cybersécurité très diverse et enrichissante est possible.

EXTRAIT DU SITE RECRUTEMENT-RENNES

Une offre d'immobilier « confidentiel défense »

Une protection physique des locaux, essentiellement à certaines activités

La préservation de l'intégrité des systèmes d'information nécessite deux protections, celle des systèmes d'information eux-mêmes et celle des bâtiments qui abritent les activités.
Ces niveaux de protection sont normés ; ainsi, la protection du secret Défense est fixée par des instructions générales interministérielles, celle relative aux locaux abritant des activités de recherche ou de production stratégiques est déterminée par un statut de zones à régime restrictif. Ces ZRR ont pour but de protéger, au sein des établissements de recherche publics et privés, l'accès à leurs savoirs et savoir-faire stratégiques ainsi qu'à leurs technologies sensibles.
Ces quelques exemples montrent que le développement d'une offre immobilière spécifique est essentielle à l'essor de la filière civile et militaire dans la métropole.

Une offre d'immobilier adaptée dans Rennes Métropole

Afin de disposer sur son territoire de locaux adaptés aux contraintes imposées, trois types d'actions sont menés par la Métropole de Rennes :

- consolider la disponibilité de box « confidentiel défense » dans une pépinière,
- accompagner les entreprises ou constructeurs souhaitant aménager des locaux « confidentiel défense »,
- faciliter l'émergence d'une offre immobilière de locaux sécurisés dans le cadre des échanges entre la collectivité et les porteurs de projets immobiliers.

Digital Square : une pépinière avec box sécurisés

Située sur la ZAC des Champs-Blancs à Cesson-Sévigné, la pépinière Digital Square accueille des jeunes entreprises du numérique et de cybersécurité.
Elle propose trois box sécurisés de 15, 17 et 23 m². Citédia assure la gestion et l'animation de cet espace entreprises de Rennes Métropole depuis 2017.

Cyberplace : un espace dédié aux entreprises de la cybersécurité

Cyberplace est un immeuble réalisé par NGE Immobilier qui sera livré fin juillet 2022, dans le nouveau quartier ViaSilva à proximité de la station Atalante de la ligne b de métro.
Proposant 4 grands espaces pour 7 600 m² au total, il se composera d'une pépinière spécialisée en cybersécurité, de plateaux de bureaux sécurisés zone à régime restrictif (ZRR), d'un espace de flex office et de services communs.

Cyberplace, un investissement de 20 millions €.

© Atelier(s) Alfonso Femia.

© www.i2c-ingenierie.fr.

Projet Art & Fact, Legendre Immobilier.

Courrouze : un pôle d'activités cyber

Le quartier de La Courrouze abrite notamment les équipes de Thales Services dans ce qu'il appelle sa « Ruche ». Les équipes y œuvrent sur des projets de cyberdéfense dans deux domaines :

- la cybersécurité du domaine aérien avec une approche baptisée CybAIR, en étroite collaboration avec la Direction générale de l'armement,
- la cyberdéfense, au profit du ComCyber du ministère des Armées.

Une partie des équipes travaillant au sein de la CyberDéfense Factory du ministère des Armées est installée dans le même bâtiment que La Ruche de Thales.

Un bâtiment appelé Art & Fact réservé à la cybersécurité est également en cours de réalisation par Legendre dans ce même quartier.

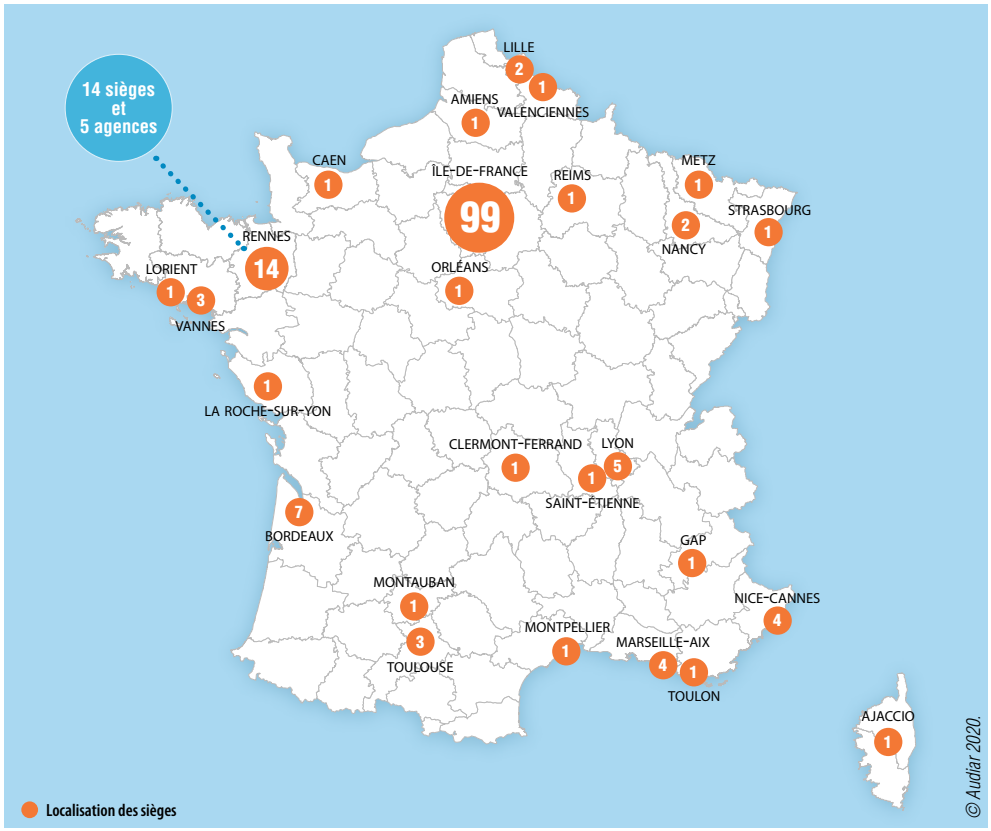
Benchmarking

Rennes, 1ère place en startups spécialistes de cybersécurité en France (hors Paris/IDF)

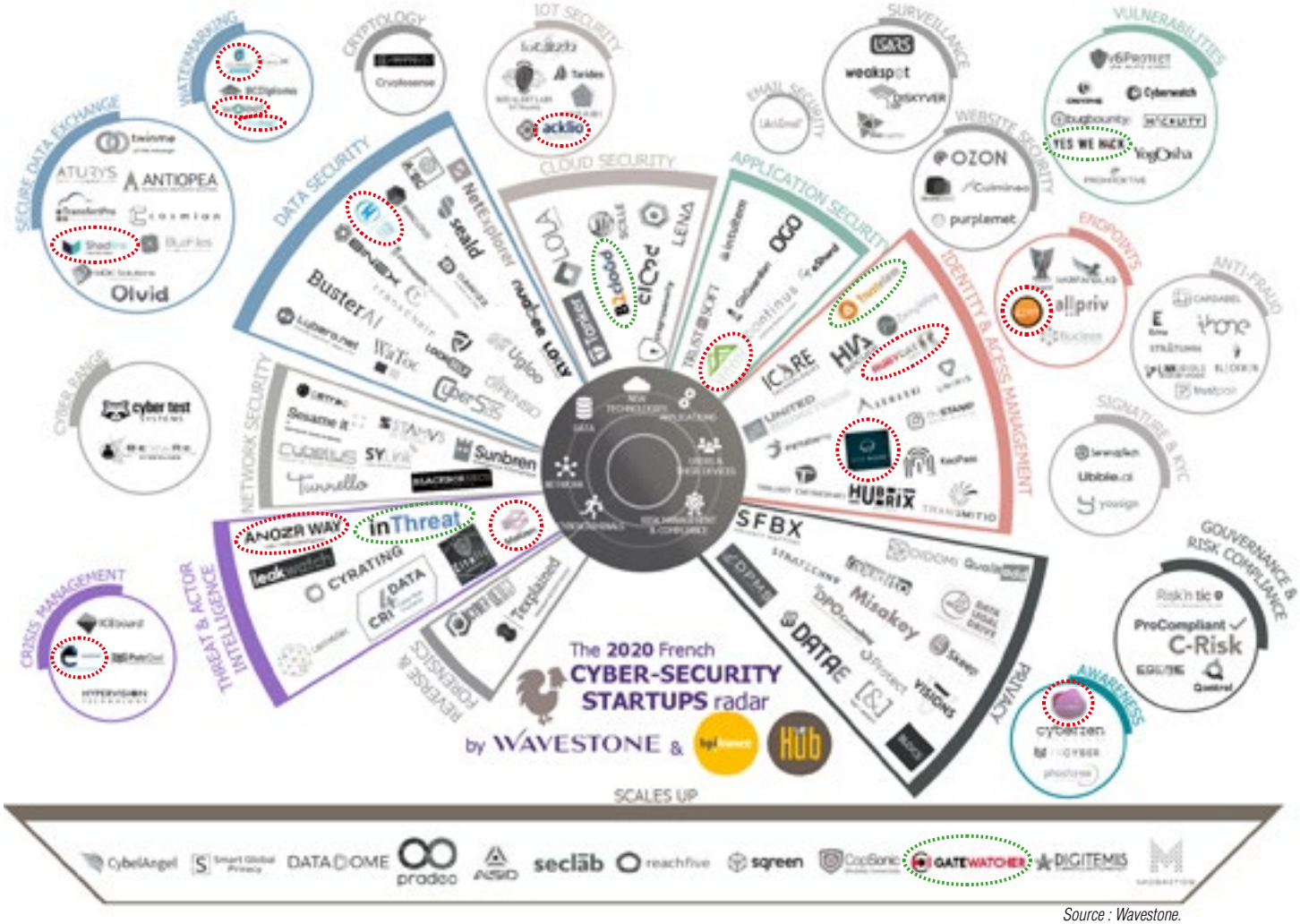
En 2020 comme en 2019 et 2018, Rennes se classe comme le 1er site en cybersécurité en région, avec 14 startups, devant Bordeaux et Lyon. De plus, Rennes s'inscrit comme locomotive dans un ensemble régional dynamique (18 startups au total). Paris – Île-de-France domine le palmarès et concentre plus de 60 % des startups. (Source Wavestone[1]).

Les startups rennaises sont leaders en watermarketing ou authentification numérique (Lamark, Content-Armor, Woleet), lutte contre la cybercriminalité (Easylience Nanocode Labs, Anozrway, Malizen), sécurité des data et applications (Hogo Business Services, Shadline, Yagaan), sécurité des utilisateurs, appareils et ioT (OneWave, Rubycat, Glimps, Acklio), évaluation et management du risque (Cy Mind).

LOCALISATION DES STARTUPS ET SCALE-UPS INSCRITES DANS LE PALMARÈS 2020 WAVESTONE CYBER-SECURITY



LES ENTREPRISES RENNAISES REPÉRÉES PAR WAVESTONE (PALMARÈS FRANÇAIS DE 150 STARTUPS ET 10 SCALE-UPS)



Source : Wavestone.

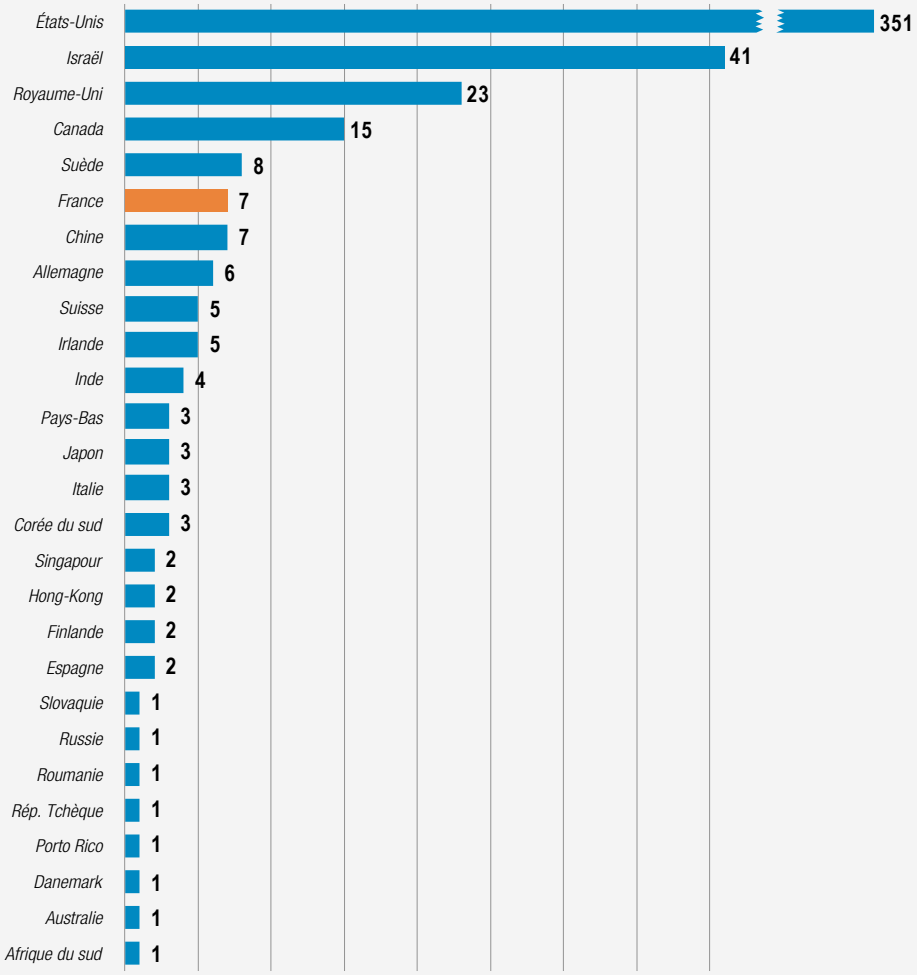
Siège à Rennes **Agence à Rennes**

1 Le radar des startups cybersécurité de Wavestone est construit selon 4 critères : siège social en France, moins de 35 salariés, moins de 7 ans d'existence et sélection de 150 entreprises environ parmi 400 sur la base de la connaissance des experts, des rencontres avec les chefs d'entreprise et les incubateurs. En outre, en 2020, 10 scale ups ont également été sélectionnées.

Benchmarking mondial : la France 6ème pays en cybersécurité

Les classements mondiaux diffèrent légèrement d'une source à l'autre (Cybersecurity Ventures[1], csoonline[2], Fortune…), mais il en ressort toujours une nette domination des USA suivi par Israël. Selon Cybersecurity 500, en 2018 les USA comptent 351 cybersecurity companies. Le 2ème pays est Israël (41 entreprises) suivi du Royaume-Uni et du Canada. La France se place au 6ème rang mondial.

TOP 500 DES ENTREPRISES DE CYBERSÉCURITÉ DANS LE MONDE



Source : Cybersecurity 500 – année 2018 - https://cybersecurityventures.com

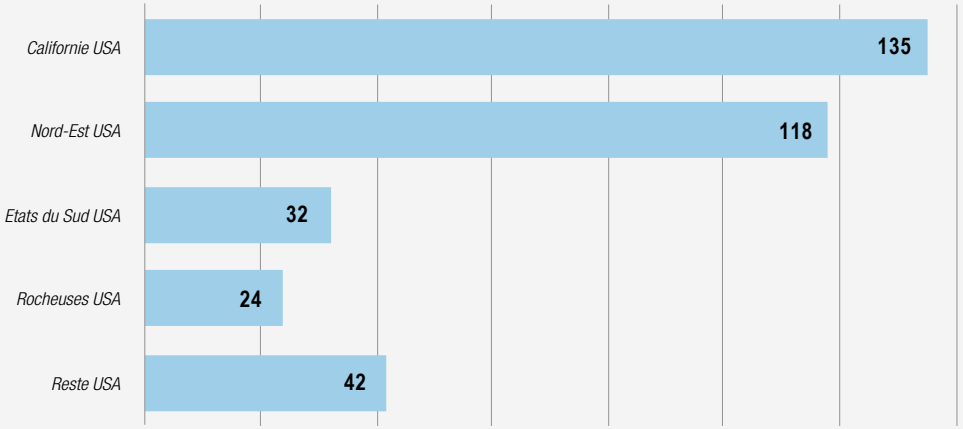
1 Les critères de sélection de Cybersecurity 500 incluent tout ou partie des éléments ci-dessous pour chaque entreprise : Produits et Problème(s) résolu(s), Clientèle, Commentaires des RSSI et des décideurs, Commentaires des évaluateurs et des conseillers en sécurité informatique, Commentaires des revendeurs à valeur ajoutée et des consultants, Financement capital-risque, Croissance de l'entreprise, Marketing d'entreprise et image de marque, Fondateur et membres de la Direction

2 https://www.csoonline.com/ https://fortune.com/2017/04/06/cyber-security-cities/

Si l'on examine les USA en grandes régions, le palmarès revient à la Silicon Valley (et San Diego : siège du US Navy's Space and Naval Warfare Sytems Command 150 entreprises 8 500 emplois en cyber Cyber Center of excellence) suivie de la Côte Est (New York City : protection des institutions économiques et financières comme Wall Street ; Washington DC : protection du gouvernement des USA, de ses agences et du Pentagone ; Boston : présence du Massachusetts Institute of Technology et son essaimage ; Maryland : siège de la NSA).

© Audiar.

LES 351 ENTREPRISES AMÉRICAINES DU TOP 500 DES ENTREPRISES DE CYBERSÉCURITÉ DANS LE MONDE



Source : Cybersecurity 500 – année 2018 - https://cybersecurityventures.com

D'autres territoires français positionnés sur la cybersécurité

Lille et les Hauts de France : la renommée du Forum International de la Cybersécurité (FIC)

Depuis 2007, Lille accueille le Forum International de la Cybersécurité (FIC), évènement de référence en matière de sécurité et de confiance numérique. Son originalité est de mêler un forum favorisant la réflexion et l'échange au sein de l'écosystème européen de la cybersécurité et un salon dédié aux rencontres entre acheteurs et fournisseurs de solutions de cybersécurité.

La Région Hauts-de-France s'est dotée d'un plan régional cybersecurité en direction des entreprises. Un « cluster » régional sera ainsi développé en partenariat avec EuraTechnologies et l'ensemble des acteurs concernés (clubs, donneurs d'ordre, startups, organismes de formation…). Par ailleurs, avec Nord France Invest (NFI), l'agence de promotion économique internationale des Hauts de France, une démarche de promotion des atouts de la Région sur ce secteur et de recherche d'investisseurs internationaux sera lancée. [1]

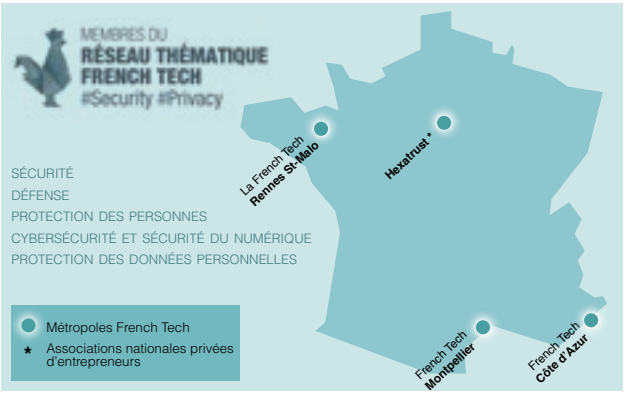
Deux autres territoires se positionnent sur le champ de la French Tech #Security #Privacy : Montpellier et la Côte d'Azur

La métropole montpelliéraine accueille sur son territoire une douzaine de spécialistes de cybersécurité dont Seclab, Tixeo, ZiWit SAS et Pradeo. La lisibilité de la French Tech Côte d'Azur est moins immédiate. L'animation de son réseau local cybersécurité est portée par Phonesec, spécialisée dans le management des risques numériques. [2]

Lyon : cybersécurité des systèmes industriels et urbains

La Métropole de Lyon s'engage avec les grands acteurs du territoire dans la création d'un collectif dédié à la cybersécurité des systèmes industriels et urbains. Une initiative soutenue notamment par la DIRECCTE et l'ANSSI, pour lesquels les enjeux portés par la sécurité des systèmes industriels sont majeurs et identifiés de longue date, notamment chez les opérateurs d'importance vitale (OIV) et leurs fournisseurs. [3]

Sont présents dans le collectif local : des fabricants d'équipements (Siemens, Schneider, Alstom, Sorhea), des éditeurs de solutions (Sentryo, ESI Group, Cybersprotect, Stormshield), des intégrateurs (Automatisme et Industrie, EKIUM, Assystem, Axians, Actemium), des acteurs globaux de la cybersécurité (ATOS, Thales), un Centre d'évaluation de la sécurité des technologies de l'information (CESTI) et des opérateurs de systèmes industriels et urbains. [4]



1 *https://www.hautsdefrance.fr/plan-regional-cybersecurite/*
2 *https://securityprivacy.lafrenchtech.com/*
3 *https://www.ssi.gouv.fr/actualite/lyon-le-premier-collectif-europeen-pour-la-securite-des-systemes-industriels/*
4 *http://www.economie.grandlyon.com/actualites/lyon-cree-le-premier-collectif-en-europe-dedie-a-la-cybersecurite-des-systemes-industriels-et-urbains-2274.html*

Zoom sur Beer-Sheva, au cœur de l'écosystème de la cybersécurité israélienne – une trajectoire possible pour Rennes ?

Depuis 10 ans, les acteurs israéliens civils et militaires, privés et publics, économiques et académiques bâtissent à Beer-Sheva un écosystème performant en cybersécurité. Or, cette ville a des similitudes de développement économique avec la métropole de Rennes (hors contexte géopolitique) : une présence forte de la défense nationale, une concentration de startups en cybersécurité et numérique, un outil d'enseignement supérieur et de recherche puissant, autant de points communs qui peuvent mener à imaginer une trajectoire similaire de Cybercapitale pour Rennes ?

Une idée à instruire d'autant que la France travaille à se doter d'un hub dédié à la cybersécurité. Le Premier ministre Edouard Philippe a confié à Michel Van Den Berghe, directeur général d'Orange Cyberdéfense une mission pour préparer la création d'un campus réunissant les forces vives de la cybersécurité françaises. « Inspiré par le cyberpark israélien de Beer-Sheva, ce campus rassemblera à la fois des équipes opérationnelles de grands groupes, des startups et également des chercheurs. » [1]

Beer-Sheva est une ville Israélienne à la lisière du désert du Neguev. Les autorités de ce pays y bâtissent la Cyber Valley israélienne, en y réunissant des entreprises du numérique, des bases de l'armée israélienne spécialisées dans la cybersécurité et une université renommée appelée « Ben Gourion ».

Son ambition est de devenir la capitale de la cybersécurité, un secteur où l'État hébreu est considéré comme l'un des pays les plus en pointe dans le monde car particulièrement menacé. En effet, Israël a pour voisins des pays contre lesquels il est ou a été en guerre. Selon les experts, avec plus de 1 000 cyberattaques par minute, Israël est l'une des cibles favorites des hackers dans le monde. Il impose d'ailleurs à ses opérateurs d'importance vitale de consacrer 8 % de leur budget à la sécurité (contre 3 à 4 % en France).

Le pays s'est donc doté en 2011 d'un National Cyber Bureau (Bureau national de la cybersécurité), rattaché au Premier ministre, qui porte notamment le projet visant à développer une cybercapitale, liée à la défense militaire et civile. Selon l'institut de recherche IVC, Israël compte 400 sociétés spécialisées dans le secteur de la sécurisation des données. Deux des 10 plus importantes sociétés au monde en cybersécurité, sont israéliennes : Checkpoint (1,5 Md$ de CA) et CyberArk. Le Pays attire dans ce domaine 20 % des investissements mondiaux, en seconde position derrière les États-Unis, et plus de 30 multinationales ont déjà installé leur centre de R&D cyber en Israël. Les cybersociétés israéliennes lèvent plus de 500 millions de dollars par an et de nombreuses pépites se sont vendues à des géants comme Microsoft ou Salesforce, pour un montant de 1,3 milliard de dollars (700 millions en 2014).

1 Michel Van Den Berghe planche sur le campus cybersécurité, 24/07/2019, Le Monde informatique.

Beer-Sheva, cité de 207 500 habitants (+14 100 habitants entre 2008 et 2017), a connu un fort développement. À l'origine de cette transformation, une volonté nationale d'établir un écosystème de proximité, « ce qui permet une interaction physique entre les responsables de la sécurité nationale, de l'université, des startups et de l'industrie, qu'ils soient israéliens ou étrangers. Ils se rencontrent, ils se parlent, ils créent ensemble » (Premier ministre israélien Benjamin Netanyahu). Des startups, ainsi qu'une kyrielle d'entreprises israéliennes et étrangères comme Lockheed Martin, Deutsche Telekom, Oracle, EMC, PaypPal ou IBM se sont installées dans deux complexes ultra-modernes bâtis dans le parc industriel CyberSpark.
1 500 techniciens, ingénieurs et chercheurs spécialisés en cybersécurité y travaillent déjà. Ils étaient moins de 400 dans la région de Beer-Sheva en 2011.

Côté université, 12 laboratoires spécialisés dans la cryptographie, l'ingénierie graphique, la vision par ordinateur, la robotique…, forment des promotions d'étudiants qui sont ensuite recrutés localement pour plus d'un tiers.
D'ici 2022, 30 000 militaires, dont 7 000 officiers de carrière, vont s'installer dans les nouvelles bases et campus technologiques qui seront construits sur 100 hectares. Ce transfert va concerner deux composantes : l'IT (3 000 soldats et officiers) et l'unité de renseignement de l'armée israélienne, en charge notamment des écoutes, du décryptage de codes, de la cyberdéfense et des cyberattaques « 8-200 ISNU » (8 000 personnes), qui aurait créé le virus Stuxnet, célèbre pour avoir infecté des systèmes d'information de centrales nucléaires en Iran.
Pour accompagner le personnel, le gouvernement projette une prime de 18 000 dollars (16 500 euros) pour les officiers célibataires et de 50 000 dollars (46 000 euros) pour les familles acceptant de vivre au moins cinq ans à Beer-Sheva.

Le gouvernement soutient également le secteur privé avec des avantages fiscaux. Depuis 2016, il accorde une subvention équivalant pendant trois ans à 20 % du montant des salaires des employés embauchés par les entreprises s'installant à Beer-Sheva dans le secteur de la cybersécurité. Ces aides soutiennent un secteur-clé de l'État hébreu.

La Bavière : un territoire pour tisser des coopérations ?

La présence de compétences issues de la recherche, de l'enseignement, de l'industrie, des startups et des multinationales en Bavière donne vie à un écosystème intéressant en matière de cybersécurité.

Les instituts de recherche majeurs dans le domaine de la cybersécurité sont l'institut Fraunhofer de la sécurité appliquée et intégrée (Fraunhofer Institut für Angewandte und Integrierte Sicherheit - AISEC) et le centre de recherche informatique CODE entourant l'université de la Bundeswehr. Les associations Sicherheitsnetzwerk München et Bayerisches IT-Sicherheitscluster sont chargées d'assurer des échanges réguliers au sein du secteur et d'initier des coopérations et débats de manière ciblée.
Le territoire accueille le centre de contact en cas de cybercrimes (Ansprechstelle für Cybercrime) (ZAC), ainsi que le centre Cyber-Allianz-Zentrum (CAZ). Le Cyber-Allianz-Zentrum (CAZ) de l'Office bavarois de protection de la Constitution conseille les entreprises et les instituts de recherche ainsi que les exploitants d'infrastructures critiques dans la prévention et l'analyse des cyber-attaques ciblées. Dans son rôle d'interlocuteur confidentiel, cette unité de gestion et de coordination nationale centrale officie dans les domaines du cyber-espionnage et du cyber-sabotage. Lors de l'analyse des attaques, le CAZ travaille en étroite collaboration avec l'Office fédéral de protection de la Constitution (BfV), l'Office fédéral pour la sécurité en matière de technologies de l'information (BSI) et d'autres autorités de sécurité fédérales et régionales. Les résultats sont analysés au CAZ et exploités en interne. Outre l'entreprise concernée, d'autres entreprises susceptibles d'être touchées par une attaque similaire obtiennent également des informations de façon anonyme.

Le nouveau centre de technologie informatique en matière de sécurité de l'État (ZITiS Zentrale Stelle für Informationstechnik im Sicherheitsbereich) a dernièrement été transféré à Munich. De surcroît, il est prévu de créer à Nuremberg une agence régionale de cybersécurité qui emploiera environ 200 experts en informatique d'ici 2025.
L'aéroport de Munich propose aussi depuis peu son Information Security Hub (ISH), un centre d'essai et d'entraînement consacré à la cybersécurité. Les entreprises, pouvoirs publics et autres institutions peuvent y former et développer des experts en sécurité pour leur organisation et passer au banc d'essai les technologies et méthodes.
Par ailleurs, la Bavière a formalisé sa stratégie relative à la cybersécurité (Bayerische Cyber-Sicherheitsstrategie). Elle accueille régulièrement des évènements dédiés à la cybersécurité. La Munich Cyber Security Conference (MCSC), qui se déroule tous les ans, met l'accent sur les échanges entre les décideurs de l'économie, de la recherche et de la politique. Les Tech Days Munich proposent une plateforme vivante aux startups, scientifiques, entreprises et industriels. Par ailleurs, l'it-sa à Nuremberg est un salon consacré à la cybersécurité.

Méthodologie

Sources de recensement des établissements

Sont recensées ici les entreprises dont le cœur de métier est majoritairement ou exclusivement la cybersécurité.
Les entreprises ont été identifiées par la veille entreprises effectuée par l'AUDIAR et par les partenaires de l'étude : Rennes Métropole, DGA-Maîtrise de l'information, ministère des Armées, Pôle d'excellence cyber. L'étude s'appuie également sur les annuaires en ligne de BDI et de réseaux thématiques (Syntec Numérique, ANSSI, GICAT, GIFAS…).

Sources d'identification des emplois

Phoning auprès des entreprises

Insee : Fichier Sirene

BVD : Fichier Diane-Astrée

ACOSS-URSSAF

Les effectifs affichés sont ceux des entités économiques dans leur totalité.
Il ne s'agit pas d'équivalents temps plein mais d'effectifs présents à la date de déclaration de l'établissement.

Cybersécurité : de quoi parle-t-on ?

Si le terme de cybersécurité évoque pour chacun une certaine idée de sécurité numérique, il demeure un domaine d'activités complexe aux contours encore incertains. Dans cette étude, le périmètre de cybersécurité est utilisé comme un terme englobant, recouvrant cyberprotection, cyberdéfense et cyberrésilience (référentiel du Pôle d'excellence cyber, janvier 2018). Les grands constitutifs de la cybersécurité étant :

- la cyberprotection : ensemble des mesures techniques, physiques et organisationnelles mises en place pour bâtir des architectures les plus robustes possibles face aux menaces portant sur la disponibilité, la confidentialité et l'intégrité des informations ou des services ;
- la cyberdéfense : ensemble des mesures techniques ou organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face à des attaques (cybercriminalité) ;
- la cyberrésilience : capacité des systèmes à continuer à fonctionner en mode dégradé lorsqu'ils sont soumis à des agressions.

Contact
Hélène Rasneur
02 99 01 85 12
h.rasneur@audiar.org

L'Audiar remercie les partenaires qui ont collaboré à ce diagnostic :

AGENCE D'URBANISME ET DE DÉVELOPPEMENT INTERCOMMUNAL DE L'AGGLOMÉRATION RENNAISE

3 rue Geneviève de Gaulle-Anthonioz
CS 40716 - 35207 RENNES Cedex 2
T : 02 99 01 86 40 www.audiar.org
@Audiar_infos

2020-037-EXT-092