NOTE RAPIDE
DE L'INSTITUT PARIS REGION N°827

ÉCONOMIE
Décembre 2019 • www.institutparisregion.fr

6,6 Mds d'€
C'EST LE CHIFFRE D'AFFAIRES DE LA CYBERSÉCURITÉ EN FRANCE (PRODUITS + SERVICES) EN 2019.

+10% par an
C'EST LA CROISSANCE DU MARCHÉ DE LA CYBERSÉCURITÉ EN FRANCE (2013-2018).

6 000 postes
DANS LA CYBERSÉCURITÉ RESTENT NON POURVUS EN ÎLE-DE-FRANCE (2019).

Sources : Comité stratégique de filière industrie de sécurité, DÉCISION Études & Conseil, Fongecif Île-de-France.

ceis
STRATÉGIE
INTELLIGENCE ÉCONOMIQUE
CYBERDEFENSE

L'INSTITUT PARIS REGION

LA CYBERSÉCURITÉ : DE LA MAÎTRISE DES RISQUES AU DÉVELOPPEMENT DES TERRITOIRES

LES RÉSEAUX ET SYSTÈMES D'INFORMATION JOUENT UN RÔLE FONDAMENTAL DANS NOTRE ÉCONOMIE ET NOTRE SOCIÉTÉ. DANS LE CONTEXTE ACTUEL DE RÉVOLUTION NUMÉRIQUE, LEUR PROTECTION RELÈVE TOUT AUTANT D'UNE QUESTION DE SOUVERAINETÉ POUR LES STRUCTURES ÉTATIQUES, QUE DE COMPÉTITIVITÉ POUR LES ENTREPRISES ET D'EFFICACITÉ POUR LES SYSTÈMES URBAINS. LA STRUCTURATION D'UN ÉCOSYSTÈME PERFORMANT DE CYBERSÉCURITÉ REVÊT AINSI UN ENJEU DE POIDS POUR LES TERRITOIRES ET SES ACTEURS.

Le coût estimé de la violation d'un système de sécurité s'élève en moyenne à plusieurs centaines de milliers d'euros. Celui d'un détournement de données se chiffre en millions d'euros. Et si les cyberattaques de grands groupes font la une des journaux, ce sont souvent les PME qui sont les plus ciblées, car plus vulnérables. Mais loin de se limiter aux acteurs économiques, ces attaques peuvent aussi mettre en péril le fonctionnement même des villes, comme ce fut le cas en juillet 2019, lors d'une attaque au *ransomware* (encadré « Lexique ») chez un fournisseur d'électricité de Johannesburg : une grande partie de la métropole fut plongée dans le noir. Ces attaques révèlent la vulnérabilité accrue de nos sociétés et économies, due à leur dépendance aux réseaux de télécommunications et systèmes d'information. Ces derniers ont aujourd'hui le rôle d'infrastructure systémique dans des secteurs d'activité d'importance capitale : santé, transports, services publics, commerce, etc. La question de leur sûreté se pose ainsi avec une acuité inédite et fait de la cybersécurité une priorité stratégique mondiale.

LA SÉCURISATION DES DONNÉES : UN MARCHÉ EN PLEINE EXPANSION

Portée initialement par des objectifs de confidentialité des données stockées ou transmises, puis des objectifs de disponibilité, la sécurisation concerne aussi aujourd'hui l'intégrité et le bon fonctionnement de systèmes d'information, dorénavant mis en réseau. Autrefois simple système de gestion, le système d'information est devenu progressivement un système opérationnel et demain industriel. La cybersécurité désigne cette sécurité globale des systèmes d'information et, plus particulièrement, « l'ensemble des outils, politiques, concepts de sécurité, mécanismes

LES START-UP FRANCILIENNES DE LA CYBERSÉCURITÉ

En janvier 2019, lors de la dernière édition du Forum international de la cybersécurité (FIC) – salon référence de la filière, organisé depuis onze ans à Lille par CEIS, en partenariat avec la Gendarmerie nationale –, les start-up franciliennes spécialisées se sont particulièrement illustrées, puisque sur 30 entreprises en compétition, trois ont obtenu une distinction majeure :

- DataDome (Paris) : vainqueur du prix 2019 ;
- Yogosha (Boulogne-Billancourt) : prix du jury 2019 ;
- LOKLY Secured by design (Massy) : coup de cœur 2019.

La prochaine édition du FIC aura lieu du 28 au 30 janvier 2020, à Lille.
https://www.forum-fic.com/accueil.htm

de sécurité [...], formations, bonnes pratiques, garanties et technologies, qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs »[1].

Historiquement structuré autour des besoins des acteurs de la défense et de l'aéronautique, le marché de la cybersécurité s'est élargi et enregistre une croissance exponentielle pour atteindre, selon les projections, un chiffre d'affaires mondial de 150 Md€ en 2020[2] (contre 3,1 Md€ en 2004 à 75 Md€ en 2015). En France, ce marché génère quant à lui entre 3 et 6 Md€ de chiffre d'affaires suivant le périmètre retenu, en progression annuelle de plus de 10 %[3]. Cette tendance se justifie notamment au regard du coût croissant des cyberattaques, estimé à 600 milliards de dollars sur l'économie mondiale en 2017[4].

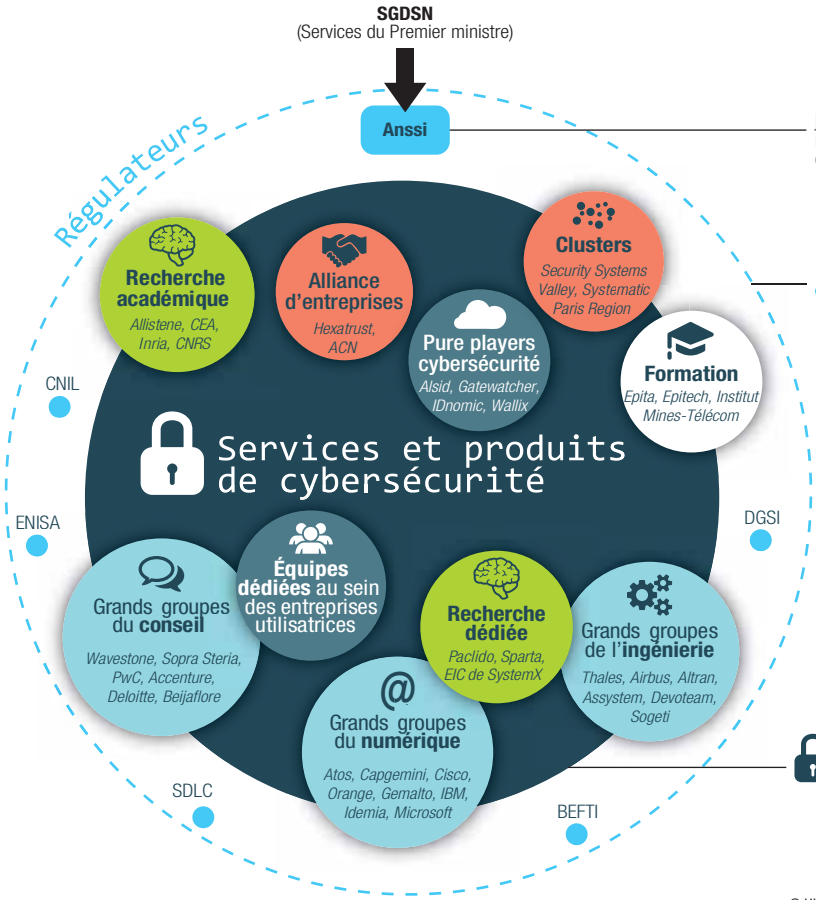
Dans un contexte où les systèmes d'information et les données deviennent des actifs stratégiques, les préjudices d'une rupture d'accès ou d'une défaillance du système d'information deviennent financièrement très importants, menaçant jusqu'à l'existence même des entreprises. Les conséquences d'une cyberattaque ne sont pas uniquement financières, mais peuvent aussi porter atteinte à la réputation d'une entreprise victime.

Autre moteur de la croissance de ce marché, le cyberespace à défendre ne cesse de s'étendre à mesure que la transformation digitale se diffuse à tous les secteurs d'activité et pénètre nos habitudes de vie. L'industrie repose ainsi de plus en plus sur l'hybridation de systèmes industriels, qui mêlent mécanique, automatisation et informatique. Le développement massif annoncé de l'Internet des objets (IoT) dans notre quotidien ne fera qu'amplifier les besoins en cybersécurité dans les années à venir. Le dernier moteur provient des obligations réglementaires et normatives, qui s'imposent non seulement aux opérateurs d'importance vitale (OIV)[5], mais aussi à l'ensemble des entreprises dépositaires de données *via* le règlement général sur la protection des données (RGPD). Entré en vigueur en mai 2018, ce règlement européen prévoit une mise en conformité des systèmes d'information et oblige les entreprises dépositaires de données à investir dans des outils et processus de sécurisation de ces dernières.

NAISSANCE D'UN ÉCOSYSTÈME

Par l'exercice de ses fonctions régaliennes, l'État occupe une place centrale dans l'écosystème de la cybersécurité (schéma ci-dessous). De ce fait,

UNE SYNERGIE ENTRE START-UP, RECHERCHE ET GRANDS DONNEURS D'ORDRES



Anssi : Agence nationale de la sécurité des systèmes d'information.
Befti : brigade d'enquêtes sur les fraudes aux technologies de l'information.
Cnil : Commision nationale de l'informatique et des libertés.
DGSI : direction générale de la sécurité intérieure.
EIC : projet Environnement pour l'interopérabilité et l'intégration en cybersécurité de l'Institut de recherche technologique Systemx.
Enisa : Agence européenne chargée de la sécurité des réseaux et de l'information.
Epita : École des ingérieurs en intelligence informatique.
Epitech : École pour l'informatique et les nouvelles technologies.
Paclido : réseau de recherche protocoles et algorithmes cryptographiques légers pour l'Internet des objets.
SDLC : sous-direction de la lutte contre la cybercriminalité (ex-Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication/OCLCTIC).
SGDSN : secrétariat général de la défense et de la sécurité nationales.
Sparta : réseau et projet collaboratif pour coordonner la recherche, l'innovation, et la formation en matière de cybersécurité au sein de l'Union européenne.

Source : L'Institut Paris Region

L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ EN ÎLE-DE-FRANCE

Tissu économique

- Concentration des emplois liés à la cybersécurité
- Autre localisation préférentielle des entreprises de la cybersécurité

Principaux acteurs de la cybersécurité

- Structure étatique
- Structure de recherche
- Structure de formation

Fond de plan

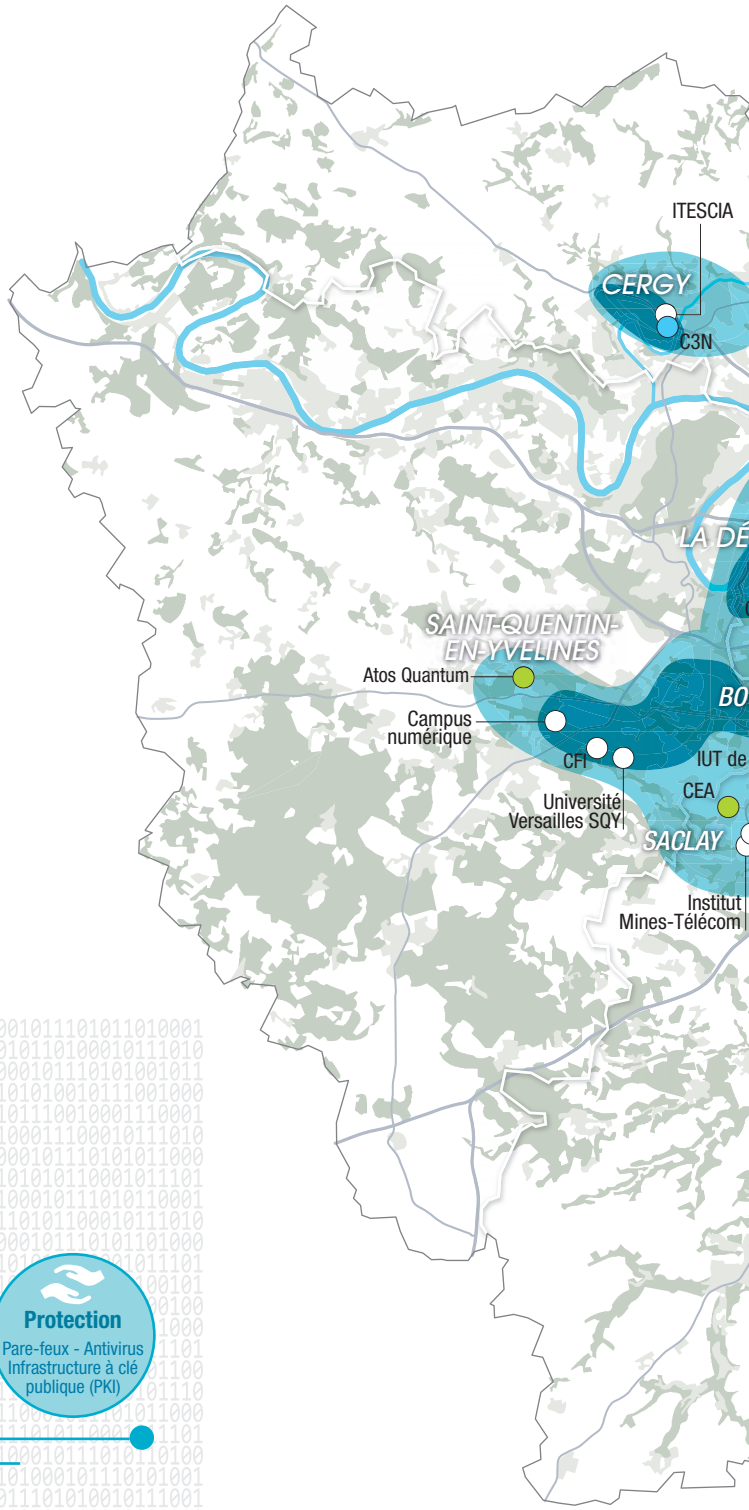
- Espace urbain
- Espace boisé
- Réseau routier principal
- Hydrographie principale

Méthodologie

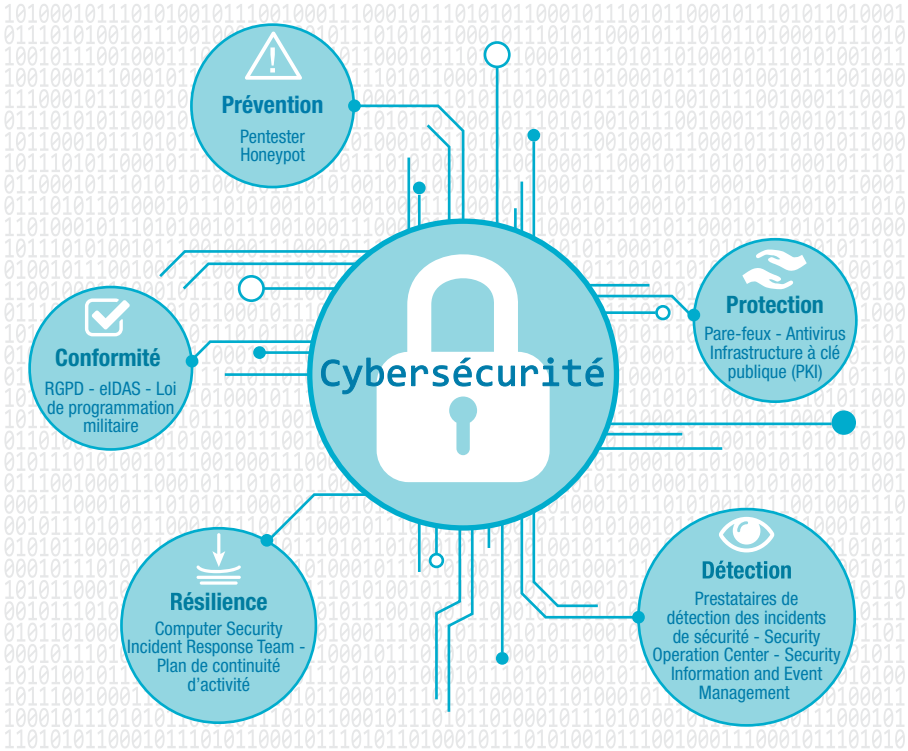
Les activités liées à la cybersécurité ne sont pas identifiées en tant que telles dans la statistique publique. La quantification à partir des codes d'activité principale des entreprises ne peut donc qu'être indirecte.
À partir des principaux secteurs d'activité engagés dans la fourniture de services et de produits de cybersécurité, à savoir le secteur du conseil, de l'ingénierie et du numérique, les codes NAF suivants ont été retenus :

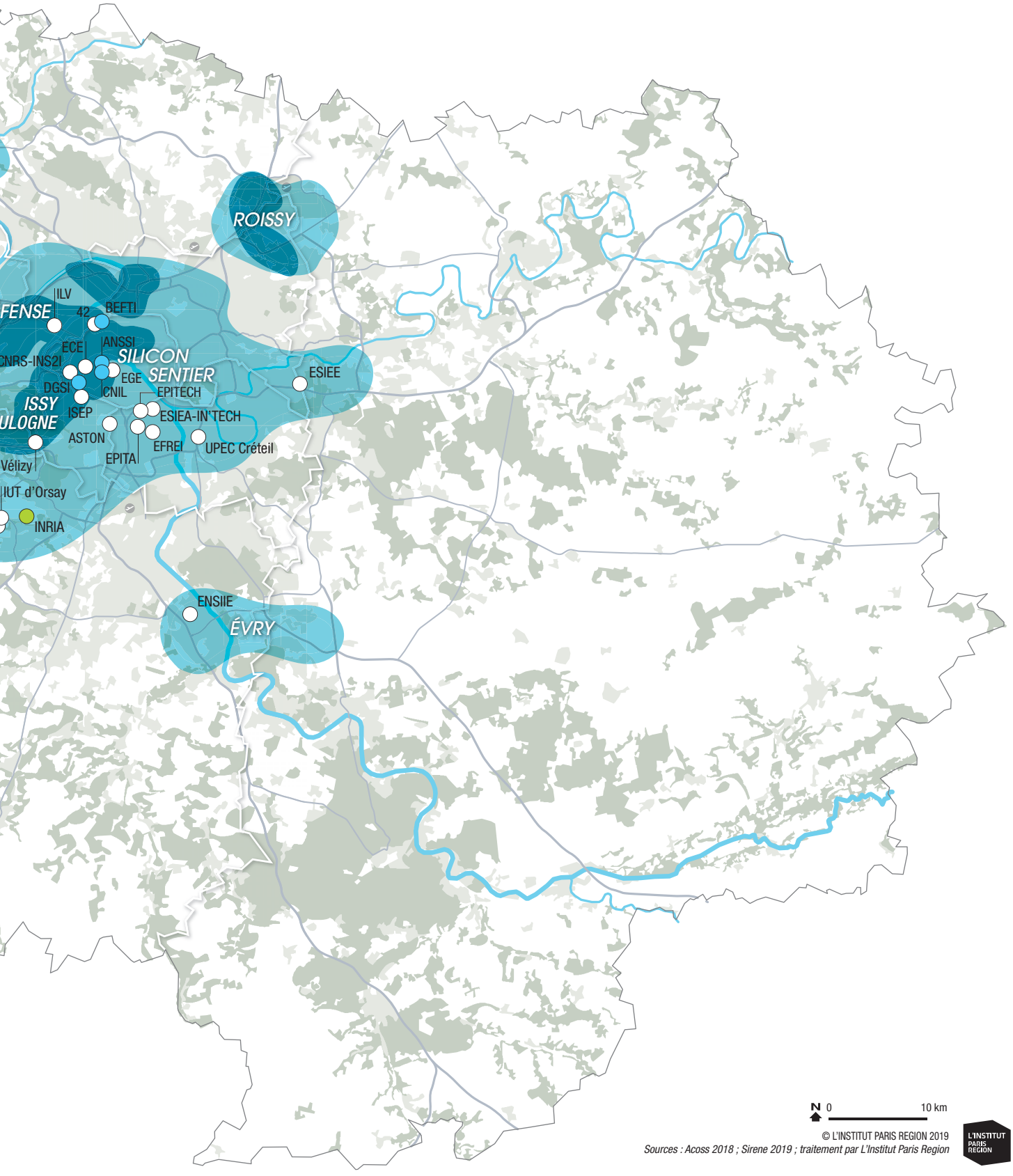
58.29A, 58.29B, 58.29C, 61.10Z, 61.20Z, 61.30Z, 61.90Z, 62.01Z, 62.02A, 62.02B, 62.03Z, 62.09Z, 63.11Z, 63.12Z, 70.22Z, 71.12B, 71.20B et 74.90B.

Par ailleurs, postulant que les grandes entreprises mobilisent en interne des compétences de cybersécurité, seuls les établissements de plus de 500 salariés ont été identifiés.
Le croisement des secteurs d'activité retenus et des grands établissements permet de calculer des densités d'emplois et ainsi d'obtenir une image des territoires de la cybersécurité en Île-de-France.



Services et produits de la cybersécurité





Sources : Acoss 2018 ; Sirene 2019 ; traitement par L'Institut Paris Region

il est prescripteur de normes, autorité régulatrice et force d'impulsion afin de moins dépendre des solutions étrangères. Au cœur du dispositif étatique, l'Agence nationale de la sécurité des systèmes d'information (Anssi) joue un rôle pivot en matière de régulation, de certification, et d'animation des acteurs de l'écosystème cybersécurité. Elle élabore notamment les règles de protection des systèmes d'information auxquelles doivent se conformer les OIV et se pose en acteur de la certification des services, produits et formations de cybersécurité du marché.

De plus, afin de fédérer les acteurs de la cybersécurité et développer les potentialités de ce marché, un comité stratégique de filière (CSF) dédié aux industries de sécurité (dont la cybersécurité) a été mis en place en 2018. La création d'un campus de la cybersécurité, inspiré du modèle israélien de Beer-Sheva, doit être annoncée d'ici à la fin de l'année 2019. L'objectif de ce campus est de permettre aux acteurs de la cybersécurité de mutualiser une partie de leurs outils, compétences et données.

Ce marché jeune et en forte croissance est plutôt dominé par les grandes entreprises de services du numérique (ESN), du secteur du conseil, et par les spécialistes historiques de l'ingénierie liée à l'aéronautique et la défense. Progressivement, les grands comptes du secteur (Atos, Capgemini, Thales, Orange, etc.) se portent acquéreurs de PME ou d'entreprises de taille intermédiaire (ETI) spécialisées.
À leur côté, un écosystème de PME/ETI s'est structuré en apportant une agilité en termes d'innovation et d'expérimentation, complémentaire à l'action des grands groupes. Pour pallier leur manque de visibilité, et dans un souci d'offrir une expertise globale, ces entreprises sont parfois amenées à se regrouper sous forme d'alliance, à l'image d'Hexatrust.

L'écosystème de la cybersécurité est un domaine à forte composante d'innovations et de technologies de rupture (intelligence artificielle, *blockchain,* cryptographie quantique, etc., encadré « Lexique »). Il travaille en étroite relation avec les établissements de recherche de pointe (CEA, Inria, etc.), notamment sous la forme de réseaux dédiés de recherche, tels Sparta ou Paclido.

LE TERRITOIRE FRANCILIEN EN PREMIÈRE LIGNE

L'environnement de la cybersécurité comprend aujourd'hui 1 500 à 2 000 entreprises au niveau national, qui génèrent environ 50 000 emplois [ACN, 2019]. Il faut y ajouter les fonctions de cybersécurité internalisées par les grandes entreprises, et notamment les OIV.
L'Île-de-France est un lieu de concentration des centres de décision, et des entreprises du secteur du numérique, du conseil et de l'ingénierie. Elle se positionne donc naturellement comme une région clé du dispositif français de cybersécurité. Les territoires couvrant l'axe partant de Saint-Quentin-en-Yvelines, jusqu'au nord-est de l'agglomération, en passant par Paris, la Défense et Boulogne-Issy-les-Moulineaux, constituent les localisations recherchées pour l'implantation de nouvelles entreprises de la filière cybersécurité.

D'autres territoires comme ceux de Cergy et du plateau de Saclay se caractérisent davantage par la présence de structures de formation en lien avec la cybersécurité. La montée en puissance de cette offre de formation est d'ailleurs un enjeu important pour l'Île-de-France, dans un contexte où les besoins de main-d'œuvre dans ce secteur sont estimés à 3 500-4 000 nouveaux postes à pourvoir chaque année, à l'horizon 2021[6]. Pour remédier aux manques en matière de recrutement, des entreprises créent leurs propres filières de formation[7], tandis que certaines collectivités territoriales travaillent au développement de nouvelles offres, comme l'illustre l'initiative de campus numérique à Saint-Quentin-en-Yvelines.

La région Bretagne a été une des pionnières en termes de structuration territoriale d'un écosystème de cybersécurité, mais plusieurs démarches de ce type sont également à l'œuvre en Île-de-France. Le pôle de compétitivité Systematic Paris Region et le cluster Security Systems Valley portent ainsi des actions fortes visant à fédérer la filière et concourent à valoriser les expérimentations en cours sur le territoire.

La Région Île-de-France apporte en outre son soutien à la filière par le financement de programmes de recherche, illustré récemment par la construction du laboratoire de R&D d'Atos, et par l'accompagnement de start-up. Cet accompagnement passe aussi par l'organisation de « challenges » ou défis intrusifs dans le domaine de la cybersécurité, qui se multiplient ces dernières années. Le recours à ce type d'événement est un bon moyen de favoriser les synergies entre start-up et grands donneurs d'ordres, à l'image du Paris Region Cybersecurity Challenge.

VERS UN NÉCESSAIRE DÉVELOPPEMENT DE LA CULTURE CYBER

Malgré ces initiatives, les entreprises françaises ne consacrent encore aujourd'hui que 4 à 5 % de leur budget de technologies de l'information à la cybersécurité, quand l'Anssi en préconise 10 %. Il reste donc une forte marge de progression pour diffuser la culture cyber au sein des entreprises. Parallèlement aux efforts déployés par l'État et la Région pour structurer et renforcer la filière, il est indispensable d'encourager plus globalement le développement d'une « culture de la cybersécurité », tant auprès des acteurs publics que des entreprises, en particulier les TPE-PME.
Cette démarche doit s'articuler autour de trois axes stratégiques. En premier lieu, il s'agit de développer et de promouvoir une offre de formation spécialisée

UN PÔLE D'EXCELLENCE CYBER EN BRETAGNE

L'écosystème breton de la cybersécurité s'appuie sur l'implantation historique de centres étatiques : direction générale de l'armement-maîtrise de l'information (DGA-MI), École des transmissions, École navale, Écoles de Saint-Cyr Coëtquidan, sur la présence d'acteurs privés majeurs du secteur, et sur un tissu dense de centres de formation et de recherche civils et militaires. La création du pôle d'excellence cyber en Bretagne en 2014 a conforté cette spécificité régionale, et en a consacré la portée nationale.

Bretagne Développement Innovation (BDI), l'agence de développement économique, anime la filière de 130 entreprises et 8 000 emplois. Pour répondre aux besoins des entreprises bretonnes, les universités forment près de 3 000 étudiants par an. L'université de Bretagne Sud, à Lorient, a récemment ouvert un master en cybersécurité des systèmes embarqués (automobile, médecine et téléphonie). Une chaire de cyberdéfense navale a également été lancée par l'École navale à Brest, avec le soutien de Naval Group, Thales et l'école d'ingénieurs IMT Atlantique.

dans les métiers de la cybersécurité, à destination d'un public de lycéens, d'étudiants et de cadres en reconversion. Parallèlement, la sensibilisation des entreprises et des collectivités aux risques de cyberattaques doit être renforcée. Enfin, un accompagnement dans la mise en place d'actions et d'outils de protection doit venir compléter cette démarche.

De manière opérationnelle, plusieurs pistes d'actions sont à envisager pour décliner ces orientations stratégiques permettant un développement plus efficient de la culture cyber sur les volets suivants :

- **la formation :** il s'agira au préalable de bâtir un référentiel régional des métiers de la cybersécurité, d'identifier les emplois non pourvus au sein des bassins d'emploi, et de recenser les compétences dont les entreprises ont besoin. Suite à cela, des actions pourraient être lancées visant à renforcer les liens entre les organismes de formation (initiale et continue) et les entreprises du secteur. Enfin, la labélisation d'établissements de formation ou de masters spécialisés est à explorer ;
- **la sensibilisation :** elle est nécessaire pour les acteurs relevant des trois grandes fonctions publiques (État, hospitalière et territoriale) et les élus sur les enjeux cyber, en particulier ceux liés à la protection des données personnelles ;
- **l'appui aux entreprises :** les collectivités locales – et tout spécifiquement la Région Île-de-France qui a la compétence en matière de développement économique – pourraient soutenir et accompagner les PME dans la réalisation d'audits sécurité IT, la formation de leurs salariés à la cybersécurité, et la montée en compétences d'une fonction de responsable de la sécurité des systèmes d'information (RSSI). De la même manière que certaines régions financent des prestations de conseil en intelligence économique pour leurs PME et ETI stratégiques, il s'agirait ici d'appuyer les entreprises dans la réalisation de diagnostics de référentiel de sécurité (politique de sécurité, politique de sauvegarde, gestion des incidents, etc.), de tests d'intrusion (*pentest, hacking,* reconnaissance, analyse des vulnérabilités, exploitation, gain et maintien d'accès, etc., « Lexique »), ou encore de plans d'action correctifs et propositions d'ajustement du référentiel de sécurité.

L'essor rapide de l'écosystème de la cybersécurité est une conséquence de la multiplication des menaces numériques qui concernent désormais tous les pans de notre économie et notre société. La structuration de cette filière est une opportunité en termes de développement économique, tant son potentiel de croissance de marché est fort et ses gisements d'emplois importants. Aux côtés des actions de sensibilisation et de formation, cet écosystème participe aussi au développement de la confiance aux espaces numériques. À l'heure de la numérisation des services publics et de la volonté de faire émerger des projets de *smart city,* cette confiance ressort comme une condition nécessaire et indispensable. ■

Renaud Roger, économiste
département Économie *(Vincent Gollain, directeur)*
Alexandre Mot, Basile de la Ménardière,
consultants Développement des territoires, CEIS

1. Définition donnée par l'Union internationale des télécommunications, *via* la recommandation UIT-T X.1205.
2. Source Gartner.
3. L'observatoire de la filière de la confiance numérique, ACN, 2019.
4. Source McAfee pour l'année 2017.
5. Art. 22 de la loi de programmation militaire.
6. Source Katalyse.
7. L'École by Capgemini.

RESSOURCES

- *L'Observatoire de la filière de la confiance numérique,* Alliance pour la confiance numérique (ACN), 2019.
- Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, *État de la menace liée au numérique en 2019. La réponse du ministère de l'Intérieur,* rapport n° 3, mai 2019.
- *Présentation générale de la cybersécurité, recommandation UIT-T X.1205,* Union internationale des télécommunications, avril 2008.
- *Livre blanc. Cybersécurité & confiance numérique,* Hexatrust, Systematic Paris Region, janvier 2017.
- « Cybersécurité en Bretagne : l'enjeu des compétences », *Les études de l'emploi cadre de l'Apec,* Bretagne Développement Innovation (BDI), Apec, n° 25, juin 2017.

LEXIQUE

***Blockchain* :** technologie de stockage et de transmission d'informations sans organe de contrôle, composée d'une chaîne de blocs numériques dont tous les échanges sont enregistrés sous forme d'empreintes numériques. Elle pourrait révolutionner les modes de transactions entre pairs, qui permettraient de fluidifier aussi bien l'économie (finance, immobilier, assurance), la démocratie (vote, protection des données, cadastre), que la vie courante (partage et location d'objets et de services). Présentée comme un élément de disruption aussi fort qu'Internet, la technologie numérique de la *blockchain* pourrait transformer les villes et les territoires.

Cryptographie quantique : protocole qui vise à rendre inviolables les échanges entre deux interlocuteurs en utilisant non plus les propriétés mathématiques de cryptage, mais celles de la physique, grâce à une clé quantique utilisant les particules de la lumière (les photons).

Cyberespace : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques (source Anssi).

***Hacking* :** piratage.

***Pentest* :** test d'intrusion pour évaluer le niveau de sécurité d'un système informatique, d'un réseau, d'une application.

***Ransomware* :** ou rançongiciel consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

DIRECTEUR DE LA PUBLICATION
Fouad Awada
DIRECTRICE DE LA COMMUNICATION
Sophie Roquelle
RÉDACTION EN CHEF
Isabelle Barazza
MAQUETTE
Jean-Eudes Tilloy
INFOGRAPHIE/CARTOGRAPHIE
Noémie Le Grand,
Pascale Guery

MÉDIATHÈQUE/PHOTOTHÈQUE
Inès Le Meledo, Julie Sarris
FABRICATION
Sylvie Coulomb
RELATIONS PRESSE
Sandrine Kocki
33 (0)1 77 49 75 78

L'Institut Paris Region
15, rue Falguière
75740 Paris Cedex 15
33 (0)1 77 49 77 49

ISSN 1967-2144
ISSN ressource en ligne
2267-4071

www
institutparisregion.fr