MICHEL VAN DEN BERGHE

CAMPUS CYBER

FÉDÉRER ET FAIRE RAYONNER L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ

Pour un nouveau centre de gravité de la sécurité et de la confiance numériques en France et en Europe.

Sommaire

Préface

Mon expérience d'entrepreneur m'a appris qu'on ne pouvait réussir seul et qu'il était imprudent de ne pas préparer l'avenir. C'est dans cet état d'esprit que j'ai accepté la mission que m'a confiée le Premier ministre en juillet 2019 afin de faire en sorte que les technologies numériques qui irriguent désormais les entreprises, les administrations et nos usages du quotidien puissent se déployer dans les meilleures conditions de sécurité.

Cette ambition exige de pouvoir s'appuyer sur des prestataires de confiance, des technologies performantes et des experts de haut niveau.

Le projet de Campus Cyber est une solution pleinement opérationnelle face à des cybermenaces changeantes. Mes rencontres avec les décideurs économiques – tant les professionnels de la cybersécurité que les entreprises utilisatrices de leurs services – m'ont confirmé que les mentalités avaient changé. Ces sociétés sont désormais prêtes à coopérer dans un lieu unique pour mettre en commun leurs savoir-faire, discuter des technologies nouvelles et identifier les meilleures pratiques pour protéger les bénéfices d'une numérisation accrue de leurs organisations et de leurs activités.

Les métiers de la cybersécurité connaissent une pénurie de candidats : les formations spécialisées existent, mais elles peinent encore trop souvent à faire le plein d'inscrits, faute de vocations suffisantes. De même, les entrepreneurs ne manquent pas pour proposer des services innovants, mais l'accès aux grands comptes leur permettant de passer à l'échelle industrielle est encore trop limité. Enfin, face à une menace cyber en constante évolution et très opportuniste, les capacités de détection peuvent rapidement atteindre leurs limites. Conscient de toutes ces contraintes, je suis persuadé qu'il nous faut revoir notre mode de réponse à ces écueils qui mettent en péril notre prospérité économique future.

Eu égard à l'avance prise par certains de nos compétiteurs outre-Atlantique ou en Asie, il convient de doter rapidement l'Europe du cadre propice à la création de cette communauté cyber. C'est la raison pour laquelle j'insiste sur la nécessité d'avancer sans tarder sur la constitution de ce Campus Cyber, qui devrait pouvoir débuter ses activités au cours du premier semestre 2021.

La localisation du Campus, à Paris ou en première couronne Ouest de Paris, s'est imposée au fil de la soixantaine d'auditions menées à partir de septembre 2019. Paris intra-muros étant même posé comme condition indispensable par tous les dirigeants de start-up auditionnés lors de la mission. En effet, les experts de la cybersécurité sont très attachés à la qualité de leur environnement professionnel et à l'accessibilité de leur lieu de travail. Ils en font un des critères prioritaires pour choisir leur employeur. L'ambition de faire du Campus une vitrine de l'offre cyber en France à l'intention des marchés internationaux plaide également pour une installation dans la capitale ou dans ses environs très proches, afin de bénéficier de l'attractivité de Paris comme centre de décision économique et politique.

Il ne s'agit certainement pas d'exclure le reste du territoire. La réussite de la région rennaise dans le domaine de la Défense montre que les expertises verticales peuvent susciter des regroupe-

ments très profitables. C'est ainsi que des satellites du Campus dans d'autres régions, où se développent de véritables ruptures technologiques, par exemple les Pays de la Loire, les Hauts-de-France ou en Auvergne-Rhône-Alpes ont à terme toute leur légitimité pour accueillir leurs propres Campus Cyber autour de spécialités de pointe comme la e-santé, la sécurité industrielle ou les villes intelligentes. La démarche francilienne doit démontrer la viabilité d'un tel montage qui réunira une diversité d'entités : compétiteurs économiques, services de l'État, sociétés utilisatrices, centres de recherche et de formation… Une fois ce modèle éprouvé, il est certain que des équivalents pourront émerger dans le pays afin de ne surtout pas verser dans un jacobinisme qui assécherait les nombreux talents et initiatives existants en France.

Ma proposition de Campus vise à doter la France et l'Europe d'un cadre optimal pour développer l'écosystème de la cybersécurité. Celui-ci doit être ouvert sur le monde. C'est la raison pour laquelle le site sera accessible à des partenaires technologiques de toutes nationalités. Avec naturellement des règles de gouvernance appropriées pour que la confidentialité et la préservation des intérêts de chacun soient assurées.

Ce lieu totem ne doit pas être une galerie marchande où les entités commerciales se contenteraient de cohabiter. Je suis persuadé de la valeur ajoutée apportée par la colocalisation d'équipes avec des plateaux-projets constitués pour travailler sur des chantiers précis. Le Campus sera ainsi le lieu idoine pour accueillir les équipes transverses travaillant sur des domaines stratégiques par exemple la sécurité des véhicules connectés ou la protection des communications. Les entités participant au Campus pourront accéder à une base commune de Threat Intelligence composée par les indices de compromission assemblés par les différents partenaires. De même, le Forum du CSF réunissant des acteurs publics/privés pourrait y être hébergé ainsi que d'autres de ses initiatives comme l'alliance des industriels français engagés pour assurer la cybersécurité des Jeux olympiques de Paris 2024. De plus, le Grand Défi « Automatisation de la cybersécurité » grâce à l'intelligence artificielle ou le projet de « Cloud de confiance » initié par la France trouveraient naturellement leur place au sein du Campus.

Nombre de grandes entreprises disposent de personnels ayant une longue expérience dans le domaine informatique. Des cursus de formation adaptés leur permettraient d'acquérir les connaissances utiles en matière de cybersécurité, contribuant ainsi à valoriser leur expertise professionnelle. Il est donc primordial d'intégrer au sein du Campus les centres de formation continue à même de délivrer ces enseignements techniques. La même démarche devra être conduite avec des formations initiales qui pourront utilement rejoindre les rangs des sociétés présentes sous forme de stages, d'apprentissages ou d'alternances.

Les relations entre les entreprises et le monde de la recherche gagneraient sans doute à plus d'interactions. L'installation d'équipes de chercheurs spécialisés en cybersécurité sur le site du Campus sera de nature à favoriser ces partages et l'élaboration de travaux communs. Avec une capacité accrue à exprimer des besoins concrets et à identifier des axes d'innovation. La proximité des laboratoires académiques et des services opérationnels des entreprises constituera le creuset *ad hoc* pour faire émerger des réponses technologiques inédites. Le dialogue quotidien des personnes réunies sur une même plateforme sera générateur de créativité par des avancées conçues lors d'échanges informels. Il ne faut pas sous-estimer les gains futurs de ce croisement des compétences.

Ce projet de Campus Cyber est tout à la fois technique, économique, humain et stratégique. Il porte en lui les outils de notre souveraineté future, en investissant sur le cadre propre à stimuler les talents qui bâtiront les technologies de demain. C'est la combinaison des investissements et du savoir-faire du monde économique, des capacités de la communauté scientifique et de l'expertise des instances étatiques qui dotera la France et l'Europe des moyens nécessaires à la durabilité de son organisation numérique.

L'incroyable capacité d'évolution rendue possible par les technologies de l'information oblige à penser de nouvelles formes de création de valeur. Le Campus Cyber peut jouer ce rôle de catalyseur afin que notre pays dispose demain des capacités pour occuper pleinement sa place dans cet environnement numérique en mutation constante.

Enthousiaste à l'idée de concrétiser ce projet ambitieux, je suis naturellement à la disposition du Premier ministre pour assurer désormais sa phase d'opérationnalisation.

Michel Van Den Berghe

7 janvier 2020

Proposition de modèle opérationnel

Le Campus Cyber en 10 points clés

1 **Un tiers-lieu opérationnel pour co-localiser** start-up, PME, industriels de la cybersécurité et du numérique, services de l'État, laboratoires de la recherche, utilisateurs, acteurs de la formation, capital-risque.

2 **10 000 m²** – avec une possibilité d'extension à 15 000 m² – pour plus de 700 spécialistes au lancement.

3 **Un lieu totem pour l'écosystème français, connecté aux dynamiques régionales** – dont le pilier rennais de cyberdéfense – **nœud central d'un futur réseau de campus satellites régionaux**, à commencer par les Hauts-de-France et les Pays de la Loire.

4 **Localisation à Paris ou petite couronne Ouest, pour l'attractivité des spécialistes** – condition d'engagement de beaucoup d'entités – l'attractivité internationale et la proximité du quartier d'affaires de la Défense.

5 **Un lieu conçu pour stimuler les synergies** entre entités autour de plateaux projets, un auditorium et un centre de séminaires, des espaces de *coworking* et de convivialité.

6 **Le point d'entrée incontournable en Europe** à la rencontre de l'écosystème de cybersécurité et de la confiance numérique, pour faire rayonner l'excellence scientifique, technique et industrielle de la France et de l'Europe.

7 **Une ouverture aux entités du monde entier, pondérée par une logique de cercles de confiance**, permettant des zones, projets et infrastructures d'accès restreint.

8 **Une société par actions simplifiée** (SAS) pour opérer et animer le Campus au quotidien.

9 **Un budget de lancement estimé à 11 000 euros d'investissement par poste puis un autofinancement** par les loyers payés par les membres et les prestations du Campus.

10 Un lancement rapide : **ouverture au 1er semestre 2021.**

ÉTUDE D'OPPORTUNITÉ

Des défis en commun

Porté par des technologies dont on peine encore à percevoir l'impact, le numérique continue de transformer profondément la vie de nos concitoyens, le fonctionnement des entreprises et des services publics. De nouvelles opportunités voient quotidiennement le jour, notamment en matière d'éducation et de formation, de santé, de transports et d'aménagement des territoires.

Dans un contexte de menace croissante, ces transformations ne pourront se faire qu'en confiance. Or à mesure que l'ensemble des activités humaines dépendent toujours plus de l'outil numérique, les attaques informatiques sont désormais susceptibles de porter atteinte à la vie de nos concitoyens, à notre économie, à notre sécurité et à notre défense nationale.

Face à cet enjeu, les pouvoirs publics ont très tôt contribué à l'émergence d'un modèle original de cybersécurité. Cette organisation a notamment permis de voir éclore des capacités privées de détection et de traitement des attaques informatiques, contribuant à hisser la France au rang des nations les plus actives en la matière.

Plénière, matinée spéciale Campus Cyber, 28 novembre 2019
Crédits : Marc Rees (licence CC-BY-SA)

L'effort a également été porté au niveau européen, l'Union européenne et les États membres partageant cette nécessité de renforcer la sécurité du marché unique du numérique.

Pour assurer la sécurité et la confiance dans le numérique, pour garantir notre sécurité économique, notre défense et notre sécurité nationale, pour construire notre souveraineté numérique en France et en Europe, **il s'agit désormais de relever collectivement plusieurs défis :**

- **Un défi scientifique, technique et industriel :** dans un contexte de compétition internationale exacerbée, dans lequel les géants numériques nord-américains occupent une position dominante et alors que se profile la concurrence d'acteurs asiatiques, un positionnement décisif est indispensable afin de garantir la souveraineté de la France et de l'Europe face aux ruptures technologiques à l'œuvre et à venir, en particulier au regard de leurs implications en matière de sécurité. Les réseaux 5G et demain 6G, l'internet des objets, l'intelligence artificielle, l'informatique quantique sont autant de défis technologiques à l'égard desquels la France et l'Europe doivent disposer d'une offre innovante et compétitive.

- **Un défi d'ouverture :** les communautés académique et de la recherche, l'État, les acteurs de l'innovation et les industriels de la cybersécurité et du numérique doivent travailler ensemble afin d'anticiper ces développements, faire émerger les solutions et les ruptures qui permettront à la France et l'Europe de progresser dans le peloton de tête de l'in-

Restitution des ateliers collaboratifs, matinée spéciale Campus Cyber, 28 novembre 2019

novation numérique mondiale. À l'heure de l'intrication croissante des offres numériques et de sécurité, les acteurs français et européens spécialisés dans la cybersécurité doivent, en particulier, se rapprocher des offreurs de produits et de services numériques. Ils doivent également travailler plus étroitement avec les bénéficiaires de la transformation numérique, afin de garantir une prise en compte des attentes et des contraintes des métiers.

Un défi opérationnel : face à la progression du nombre, de la sophistication et de l'impact des attaques informatiques, qu'elles soient ciblées ou de masse, souvent très difficiles à détecter, les acteurs publics et privés doivent développer leur capacité à travailler ensemble et à imaginer des solutions nouvelles. Au sein de mêmes secteurs d'activité et entre secteurs, les entreprises doivent, en particulier, développer les échanges d'information. Les offreurs de services et l'État doivent également partager davantage, notamment en matière de données relatives à la menace (*Threat intelligence*) afin de contribuer au renforcement de la capacité de chacun à anticiper, détecter et remédier aux attaques informatiques. Le développement des synergies entre les acteurs contribuera également à orienter l'innovation technologique et à accroître les chances de succès opérationnels.

Un défi autour de la donnée : valoriser la donnée pour la cybersécurité constitue aujourd'hui une opportunité unique pour enrichir et démultiplier les capacités d'action des acteurs du secteur, notamment en matière de détection grâce aux potentiels de l'intelligence artificielle. Relever le défi de la donnée — de la constitution de bases ou de « lacs de données » à leur standardisation — nécessite que les acteurs de l'écosystème puissent expérimenter des solutions de traitement innovantes. C'est notamment l'ambition fixée au Grand Défi « Automatisation de la cybersécurité » choisi par le Conseil de l'innovation.

Un défi humain : former des spécialistes en cybersécurité est nécessaire pour couvrir les besoins des industriels comme ceux des utilisateurs. Plus largement, le triptyque (1) sensibilisation au numérique et à ses enjeux de sécurité dès le plus jeune âge, (2) enseignement supérieur et (3) formation tout au long de la carrière constitue un préalable à toute ambition accrue dans le domaine de la sécurité et la confiance numériques.

Un défi en termes d'imaginaire : attirer des vocations pour les métiers de la cybersécurité et obtenir une plus large mobilisation de la communauté nationale et européenne, dépend, pour finir, d'une évolution maîtrisée de l'imaginaire collectif autour des enjeux de sécurité numérique.

Tout cela nécessite une impulsion majeure. La création d'un Campus dédié, souhaitée par le président de la République, est de nature à constituer une évolution décisive pour l'écosystème français de la sécurité et de la confiance numériques.

Une capacité désormais incontournable des grandes nations de la cybersécurité

1 Une capacité émergente : Israël, Royaume-Uni, Russie, États-Unis, Chine…

La prise en compte croissante des risques pour la transformation numérique a été à l'origine d'efforts importants de la part des États européens – au premier rang desquels la France, le Royaume-Uni et l'Allemagne – **et extra-européens**, dont les États-Unis, la Chine, la Russie et Israël.

La création d'agences nationales publiques dédiées à la cybersécurité, l'adoption de réglementations encadrant la sécurité des opérateurs les plus critiques, le développement d'une expertise à l'état de l'art et de capacités opérationnelles au sein de l'État et du secteur privé, le soutien à la recherche et à l'industrie constituent un socle capacitaire commun.

Les États-Unis, Israël, la Russie et la Chine ont cependant franchi un cap supplémentaire avec la création, soutenue au plus haut niveau politique, **de campus industriels et technologiques ambitieux.**

Pensés pour renforcer les synergies entre start-up, industriels, financeurs, acteurs publics et monde de la recherche, **ces campus ont fait le pari du rapprochement géographique d'acteurs divers en vue de stimuler l'innovation et permettre des succès industriels pérennes**. Ces parcs technologiques constituent également **des vitrines internationales** de l'excellence scientifique et technique des écosystèmes nationaux.

En complément des recherches de cette mission, l'étude réalisée par la direction générale du Trésor du ministère de l'Économie et des Finances des initiatives développées par plusieurs pays a permis de préciser les forces et les faiblesses de ces différents modèles (voir synthèses en annexe). Une rencontre entre la mission et la fondation de Skolkovo en Russie est venue compléter ce panorama par une plongée inspirante au cœur du parc technologique russe.

Il en ressort tout d'abord que **ces campus diffèrent dans leurs périmètres et les modalités de leurs développements**. À titre d'exemple, si le CyberSpark israélien de Beer Sheva ambitionne de se spécialiser sur la cybersécurité, le numérique ne constitue que l'une des dimensions du parc technologique russe de Skolkovo.

Global Cyber Center, Cyber NYC, New York, Etats-Unis – *Crédits : SOSA*

Cyber Spark, Beer Sheva, Israël — *Crédits : Michael Doron*

Le succès variable de ces initiatives semble toutefois reposer sur des facteurs communs :

- Le rôle central des acteurs privés et académiques de l'innovation, des start-up, des centres de recherche et des industriels à maturité ;
- Une ambition très forte d'attirer de jeunes talents, rendue possible par le positionnement central des campus au cœur ou au plus près des capitales (ex. Skolkovo à 20 minutes en train de Moscou, le Cyber NYC à Manhattan, New York). Le Cyber Spark israélien situé à Beer Sheva est réputé moins attractif en raison de son enclavement ;
- Le soutien et la facilitation des pouvoirs publics – positionnés autour et non pas au centre de l'écosystème –, soit par un soutien politique fort soit par la présence d'agences publiques spécialisées ;
- Des facilités fiscales, voire des subventions publiques, destinées à inciter les entreprises à s'installer, et la création de « zones franches » juridiques favorables à l'expérimentation ;
- La présence importante du capital-risque pour financer les start-up et entreprises plus matures dans leurs développements ;
- Des infrastructures communes adaptées au développement de synergies entre les acteurs en présence ;
- De véritables vitrines internationales de l'écosystème cyber ou plus largement technologique.

2 Une place encore vacante en Europe

Des initiatives similaires émergent en Europe. C'est notamment le cas au Royaume-Uni ou en Allemagne où des acteurs de la recherche et de l'innovation tendent à se réunir, souvent autour des universités.

Pour autant, il n'existe encore en Europe aucun « campus » proprement dédié à la cybersécurité qui soit aussi divers dans sa composition, ambitieux et tourné vers l'international que Beer Sheva en Israël ou le futur Cyber NYC.

Si l'UE affiche une ambition importante pour l'intelligence artificielle ou les technologies quantiques, elle ne saurait toutefois relever ces défis sans affirmer le même niveau d'ambition pour ce qui est des enjeux de sécurité associés.

Au sein d'une UE dont l'avenir s'écrira bientôt à 27, le lancement d'un Campus Cyber en France apparaît, à cet égard, comme une opportunité tant pour la France que pour l'UE, qui manquent d'un lieu mobilisateur, d'une vitrine internationale de l'excellence scientifique, technique et industrielle de leurs écosystèmes de cybersécurité.

Israël : le Cyber Spark de Beer Sheva, dans le désert du Néguev

FOCUS : CYBERSÉCURITÉ

Prenant appui sur des interactions historiques facilitées entre les domaines militaires et civils et entre le secteur public et le privé, **le Cyber Spark de Beer Sheva mise sur la concentration d'acteurs clés de cet écosystème et vise à doter Israël des capacités opérationnelles et techniques nécessaires à sa cybersécurité**. Le campus est également la vitrine internationale du secteur destinée à favoriser son exportation.

« Cybercapitale » proclamée du pays, Beer Sheva peut compter sur l'expertise de l'Université Ben Gurion établie sur place, de l'agence publique de cybersécurité – *Israeli National Cyber Directorate* (INCD) – d'incitations financières et d'un très fort soutien politique. Comme le reste de l'écosystème, Beer Sheva bénéficie également du rôle clé de l'armée dans la formation des élites du pays en matière de cybersécurité, souvent futurs entrepreneurs. La dynamique de l'écosystème, permise par la colocalisation d'acteurs de natures diverses, la mutualisation et le partage au travers d'évènements dédiés (*meet up, cybertech, cyberweek*), la présence d'entreprises et d'investisseurs internationaux, l'existence de facilités fiscales pour les entreprises présentes sur place, sont également des éléments du succès de Beer Sheva, tel que mis en avant par les autorités israéliennes.

Suite à une réunion organisée à l'ambassade de France dans le cadre de cette mission, il ressort qu'en dépit des incitations financières, **la localisation de Beer Sheva dans le désert du Néguev constitue toutefois une limite importante à son attractivité**, par rapport à Tel-Aviv ou Jérusalem. Des entreprises peineraient à attirer des talents, en particulier les plus confirmés et certaines auraient d'ores et déjà pris la décision de se relocaliser à Tel-Aviv. Les entreprises présentes sur le campus souffriraient également d'un déficit de proximité avec leurs clients ainsi que des fonctions supports, notamment juridiques.

Russie : le parc technologique de Skolkovo à 20 minutes en train de Moscou

FOCUS : NUMÉRIQUE (INCL. CYBERSÉCURITÉ), ÉNERGIE, ESPACE, BIOMÉDICAL, NUCLÉAIRE.

Campus technologique et industriel né il y a dix ans de la volonté politique de Dmitri Medvedev, actuel président du gouvernement de la Fédération de Russie, **Skolkovo réunit sur plusieurs kilomètres carrés des industriels, des instituts technologiques et une université (Skoltech), des incubateurs et un accélérateur géant pour les start-up**, des habitations et des lieux de vie, avec pour objectif le développement de l'innovation russe dans les domaines du numérique, de l'énergie, de l'espace et de la santé. Au sein du volet numérique, plusieurs start-up et entreprises de cybersécurité sont installées ou ont été incubées à Skolkovo avant leur essor international.

Outre son infrastructure, **Skolkovo permet l'accès à des financements et offre des facilités fiscales et douanières**. La Fondation Skolkovo, qui anime l'ensemble du site, organise au quotidien la vie de ce campus vivant et opérationnel, en veillant, en particulier, à encourager les synergies entre les acteurs sur place.

Le campus dans lequel 10 milliards de dollars ont été investis depuis sa création compte déjà plus de 2 000 start-up ayant généré 1,4 milliard de dollars en 2018 et suscité 30 000 créations d'emplois et plus de 1500 brevets. 150 entreprises, russes et

internationales avec plus de 6 300 salariés, ainsi que 45 centres en recherche et développement (R&D) sont installés sur le campus. Skolkovo peut également compter sur une très forte présence d'investisseurs et une jeune université à l'ambition internationale, Skoltech. Extrêmement sélective, celle-ci ambitionne de former l'élite scientifique et technologique russe, grâce à des partenariats avec d'autres universités comme le Massachusetts Institute of Technology (MIT) et des entreprises, fournissant aux étudiants les projets de recherche sur lesquels ceux-ci planchent dans leurs laboratoires de recherche.

À moins de 20 minutes en train de Moscou, Skolkovo est proche de la ville. De grandes entreprises russes de la cybersécurité, dont la première d'entre elles, Kaspersky, demeurent néanmoins principalement localisées dans Moscou.

États-Unis : Cyber NYC au cœur de Manhattan, New York

FOCUS : CYBERSÉCURITÉ.

La ville de New York souhaite devenir l'épicentre de la cybersécurité et de l'innovation avec la création du Cyber NYC. Annoncé en 2018, celui-ci dispose d'un investissement public-privé de 100 millions de dollars et ambitionne d'atteindre 10 000 emplois issus de start-up présentes sur le site.

Placé au cœur de Manhattan, le Cyber NYC comprend un Centre cyber de 1300 m² développé par l'entreprise SOSA dans le quartier de Soho avec comme activités des challenges pour le développement de nouvelles technologies (*Cyber security Moonshot Challenge)*, un *boot camp*, des initiatives en matière de formation et d'innovation ainsi qu'un incubateur et accélérateur géré en partenariat avec le fonds de capital-risque de la *Jérusalem Venture Partners* (JVP).

En soutien d'un secteur très actif — selon *New York City Economic Developement Corporation*, le secteur de la cybersécurité représente une industrie de plus d'un milliard de dollars pour la ville, avec plus de 100 entreprises et 6 000 employés — l'objectif est de créer un lieu fédérateur, au plus près de cinq écoles et universités, de l'agglomération (CUNY, NYU, Columbia University, Cornell Tech, iQ4) pleinement associées à ce projet et des bénéficiaires.

Des programmes de formations initiale et continue y seront également proposés afin de répondre au déficit de talents dans l'agglomération. Par ailleurs, des entreprises étrangères comme Wavestone pour la France, participent à la mise en place du Cyber NYC.

Chine : les parcs dédiés à la cybersécurité de Pékin et Wuhan.

FOCUS : CYBERSÉCURITÉ.

Priorité nationale depuis son arrivée au pouvoir en 2012, le Président Xi préside une commission interministérielle qui définit la politique publique nationale de cybersécurité. Dans le cadre de cette politique et à côté des « académies d'excellence » à vocation internationale, des parcs industriels dédiés à la cybersécurité sont installés dans de grandes métropoles de l'est du pays. Quatre de ces parcs sont succinctement présentés ici.

Créé en 2014, le parc de Tianjin, situé à une heure de Pékin, a une vocation opérationnelle

et de souveraineté. Y sont concentrés un CERT national et des centres de recherche sur les virus informatiques, l'alliance des entreprises contre les logiciels malveillants, l'alliance internationale pour la sécurité du cloud, le projet de microprocesseur « Tengfei » et de système d'exploitation « Kylin » conduit par la *National University of Defense Technology* destinés à se substituer à l'offre américaine. Dans le même esprit, un nouveau parc « de rang national » a été inauguré à Pékin en janvier 2019. Il est destiné à occuper une place centrale au sein du « plan de développement national de l'industrie de la cybersécurité ». Une trentaine d'entreprises ont annoncé s'y installer.

Plus au sud, à Wuhan, un parc industriel constitue la « base nationale d'innovation et des talents — sécurité des réseaux de l'information ». Il accueillait 75 entreprises en 2018 — dont ATOS, 41 autres entreprises ayant manifesté l'intention de s'y relocaliser.

Le parc de Tai'an est destiné à la coopération internationale. Présenté comme Sino-israélien, ce parc a été inauguré en décembre 2018.

Royaume-Uni : la Tech City de Londres et le LORCA britannique, accélérateur d'entreprises à 30 minutes de Covent Garden

FOCUS : NUMÉRIQUE (INCL. CYBERSÉCURITÉ)

« London Office for Rapid Cybersecurity Advancement », le programme LORCA a été lancé en 2018 avec un budget de 13,5 M£ sur trois ans pour accompagner le développement de plus de 72 entreprises dans le secteur de la cybersécurité. En rassemblant des acteurs du secteur privé, public et académique au sein de ses murs, LORCA espère accélérer l'innovation britannique en matière de cybersécurité ainsi que la commercialisation de nouvelles solutions pour générer de la croissance.

Le projet implique plusieurs partenaires, dont Plexal, qui met à disposition l'espace physique d'incubation au sein du *Queen Elizabeth Olympic Park* à Londres, Deloitte et la *Queen's University* de Belfast. Les start-up qui souhaitent participer au projet doivent candidater au sein d'une des catégories choisies chaque année par LORCA (ex. : confidentialité et confiance, cyber menaces dans les services publics, etc.). Ces catégories permettent un alignement stratégique de la demande et de l'offre du marché de la cybersécurité, phénomène renforcé par la proximité des grands groupes et des start-up lors de l'exécution du programme. Les start-up sélectionnées bénéficient en effet d'un accompagnement personnalisé et de l'expertise des entreprises partenaires de LORCA.

Les entreprises accélérées par LORCA sont relativement matures dans la mesure où elles sont déjà dans une phase de commercialisation. Sur les trente-deux entreprises accélérées par LORCA jusqu'à présent, huit ont d'abord participé au programme d'accélération du *NCSC Cyber Accelerator*.

Un écosystème français prêt à se mobiliser

1 Un engouement pour la démarche

Entre septembre et novembre 2019, la mission a organisé plus de 60 auditions avec des représentants de haut niveau de l'industrie du secteur de la cybersécurité, de fédérations d'entreprises utilisatrices des solutions et services de cybersécurité, du monde de la recherche, du capital-risque, de la communauté numérique, de la société civile et des pouvoirs publics.

« Le Cyber Campus est extrêmement important pour nous. On compte s'impliquer ardemment et placer des équipes sur place pour faire de ce projet un grand succès ! »

Hugues Foulon
Directeur de la stratégie et des activités de cybersécurité, ORANGE

En complément, une matinée spéciale organisée le 28 novembre 2019 en présence du secrétaire d'État chargé du numérique Cédric O, a permis la consultation de plus de 150 responsables de l'écosystème, via des ateliers collaboratifs organisés autour de quatre thèmes : la recherche et l'innovation, la coopération opérationnelle, la formation et les communs de la cybersécurité.

Ces temps d'échanges et la réactivité des interlocuteurs consultés ont permis d'apprécier l'intérêt extrêmement fort de l'écosystème pour une initiative française comparable aux expériences internationales précitées.

Lors de ces échanges, **l'opportunité de colocaliser des acteurs publics, privés, académiques et associatifs est apparue comme une évidence.**

Les acteurs rencontrés ont, pour beaucoup, manifesté très tôt un intérêt pour la démarche, au regard d'objectifs pouvant varier (voir « Déclarations de soutien ») :

- Pour les industriels en croissance, le Campus constitue une opportunité de déployer leurs ressources et leurs équipes au plus proche de potentiels partenaires : industriels, services de l'État, de recherche, voire de leurs utilisateurs ;
- Pour les start-up et PME, le Campus est l'occasion de se rapprocher d'acteurs plus matures susceptibles d'accompagner leur accélération, par exemple en testant à l'échelle leur solution ou en l'incluant dans leur catalogue ;
- Pour tous, le Campus est l'opportunité de tester de nouvelles synergies, d'évoluer dans un environnement porté par une ambition commune au travers d'évènements dédiés, de débats d'idées, d'exercices, de challenges ;
- Pour tous, le Campus est l'opportunité de développer la formation en matière de cybersécurité, grâce à la présence de centres de formation, d'écoles ou en mutualisant les efforts de formation continue d'entreprises privées ;
- Pour tous, le Campus peut constituer une vitrine européenne et internationale unique pour leurs activités.

Cette mobilisation dessine également les contours du modèle économique d'un Campus, ayant vocation à réunir des membres, dont le retour sur investissement sera propre à chacun.

Déclarations de soutien au Campus Cyber en présence de Cédric O, secrétaire d'État chargé du Numérique, matinée spéciale Campus Cyber, 28 novembre 2019

2 Les conditions de la mobilisation

Les conditions de la mobilisation sont également ressorties de ces échanges, en particulier :

- **La très haute attractivité de la localisation du Campus**, indispensable pour attirer des talents réputés exigeants et capitaliser sur un écosystème principalement établi en Île-de-France. **La majorité des interlocuteurs nous ont ainsi vivement invités à rechercher une localisation parisienne ou en petite couronne Ouest, faisant de la localisation une condition à leur engagement**. L'accessibilité des transports en commun apparaît par ailleurs comme un critère non négociable ;

- **L'engagement de l'État, en particulier de l'ANSSI, dans le Campus**. L'État a été tout à la fois évoqué comme garant de l'intérêt général, catalyseur nécessaire pour développer des synergies entre acteurs concurrents, source d'expertises, de ressources et d'outils uniquement disponibles au sein de la sphère publique de la cybersécurité ;

- **La capacité du Campus à renforcer les échanges, les synergies, le partage** — notamment de données — entre acteurs publics, privés et académiques, et les opportunités qu'offrira le campus, au travers de la conception du lieu et de son animation. Outre des lieux de travail et de convivialité communs, le Campus devrait notamment disposer d'un centre de conférences permettant d'accueillir des évènements, colloques, réunions, ateliers et formations ;

- **La portée internationale du Campus**, tant dans l'ouverture au travers de projets, que dans sa visibilité à l'international. Le Campus devrait être, en tant que tel, un espace de démonstration vivant de l'excellence scientifique et technologique de l'écosystème français et européen et un point de passage obligé en Europe pour aller à sa rencontre ;

- **La confiance que le Campus devrait permettre de développer**, y compris, lorsque cela sera nécessaire en sanctuarisant des espaces pour des entités, projets ou communs – telles que des données – nécessitant un degré de protection et des modalités d'accès particuliers.

Un contexte favorable en France et en Europe

Outre l'intérêt manifeste de l'écosystème pour le Campus Cyber, ce projet bénéficie d'un contexte favorable en France et en Europe, renforçant ses chances de succès.

Un contexte favorable sur le plan industriel, grâce à un tissu dynamique et compétitif d'industriels et de petites et moyennes entreprises qui s'exporte déjà en Europe et à l'international. De nouvelles start-up viennent par ailleurs grossir les rangs de l'offre française de produits et de services de sécurité numérique chaque année.

D'après l'Observatoire 2019 de la confiance numérique, la France, en 2018 comptait, 2 088 entreprises dans le domaine, dont 65 grandes entreprises, 75 entreprises de taille intermédiaire et 636 PME. 16,9 milliards d'euros de chiffre d'affaires étaient, la même année, générés dont 9,1 milliards à l'international. Selon le radar 2019 des start-up en cybersécurité en France publié par Wavestone, le nombre de start-up en cybersécurité a également augmenté de 18 % depuis janvier 2018 et les levées de fond ont significativement progressé. Choisissant d'innover dans des domaines matures de la cybersécurité telle que la sécurité de la donnée, la gestion des identités et des accès ou encore la gestion des vulnérabilités, les start-up françaises misent de manière croissante sur l'international.

On soulignera, en particulier, le dynamisme du pôle rennais, avec le soutien de la Région et l'implication décisive du ministère des Armées ayant permis de fédérer autour de problématiques de défense nationale des start-up, PME et acteurs industriels innovants, ainsi que de formations en cybersécurité.

Un contexte favorable sur le plan de la structuration de la filière par le Comité Stratégique de Filière Industries de sécurité au sein du Conseil national de l'industrie, labellisé le 22 novembre 2018. Rouage essentiel du soutien à la filière de cybersécurité, le CSF et ses membres, acteurs privés et publics, porteront des projets d'intérêt commun pour la filière, notamment dans le domaine de la cybersécurité. Ces projets feront l'objet d'engagements dans un contrat de filière avec l'État et trouveront souvent un débouché naturel dans le Campus.

Un contexte favorable sur le plan de la recherche et de l'innovation, grâce à un maillage national riche de centres et instituts de recherche spécialisés dans le numérique et, de manière croissante, dans la cybersécurité. Deux projets de grande envergure incarnent, en particulier, cette dynamique.

Premièrement, le Grand Défi « Automatisation de la cybersécurité », l'un des cinq grands défis choisis par le Conseil de l'innovation et financés à hauteur de 30 M€ par an par le Fonds pour l'innovation et l'industrie, en vue de répondre à des enjeux sociétaux dans des domaines stratégiques nécessitant la levée de barrières technologiques.

Deuxièmement, le consortium SPARTA, nouveau réseau de compétences en cybersécurité, soutenu par le programme Horizon 2020 de l'UE, ayant pour objectif de développer et de mettre en œuvre des actions collaboratives de recherche et d'innovation de haut niveau. Piloté par le CEA, SPARTA rassemble un groupe équilibré de 44 acteurs au sein de 14 États membres de l'UE, incluant pour la France Thales, YesWeHack, l'ANSSI, l'Institut Mines-Télécom et Inria, à l'intersection de l'excellence scientifique, de l'innovation technologique, et des sciences sociales dans le domaine de la cybersécurité.

> **« Le Campus pourra être un débouché et une vitrine pour des projets structurants portés dans le cadre du comité stratégique de filière industries de sécurité »**
>
> **Marc Darmon**
>
> *Président du Comité stratégique de filière (CSF) dédié aux industries de sécurité, directeur général de l'Activité Systèmes d'Information et de Communication Sécurisés, THALES*

Un contexte favorable sur le plan de la formation. Malgré le déficit d'experts maintes fois pointé, la France dispose sur

l'ensemble de son territoire de nombreuses formations d'excellence en mathématiques, en ingénierie ainsi que dans d'autres disciplines, reflétant la diversité des profils et des métiers de la sécurité numérique, de la réglementation, du conseil ou la gestion et la communication de crises.

Près de soixante formations universitaires supérieures, d'ingénieur et mastères spécialisés, incluant un volet ou portant à titre principal sur la cybersécurité ont notamment reçu le label SecNumEdu délivré par l'ANSSI.

Un contexte favorable sur le plan européen, avec le projet de règlement européen visant l'établissement d'un « centre de compétences et d'expertise en cybersécurité » et des relais nationaux dont l'objectif est d'optimiser et mieux orienter le financement de la recherche et de l'innovation dans le domaine de la sécurité et de la confiance numériques au sein des écosystèmes nationaux.

Un contexte favorable, également, grâce à la mise en place du cadre européen de certification de sécurité numérique adopté en 2018, par l'agence européenne pour la cybersécurité (ENISA) et les États membres, qui permettra de valoriser en Europe et à l'international les offres de solutions de sécurité de qualité pour tous les niveaux, de futures réglementations et orientations politiques structurantes (5G, cloud, IOT, etc.).

Innovation Center, Skolkovo Technopark, Moscou, Russie

PROPOSITION

Vision et dimensions du Campus

1 Objectifs : bâtir un centre de gravité de la cybersécurité et de la confiance numérique en France et en Europe

Compte tenu des éléments d'opportunité et des contextes favorables évoqués précédemment, il est proposé d'établir un Campus Cyber, opérationnel au 1er semestre 2021 destiné à :

- **Fédérer la communauté de la sécurité et de la confiance numériques**, incluant les industriels de la cybersécurité et du numérique, la communauté académique, les acteurs de l'innovation, les services concernés de l'État, acteurs de la formation ou encore des financeurs ;

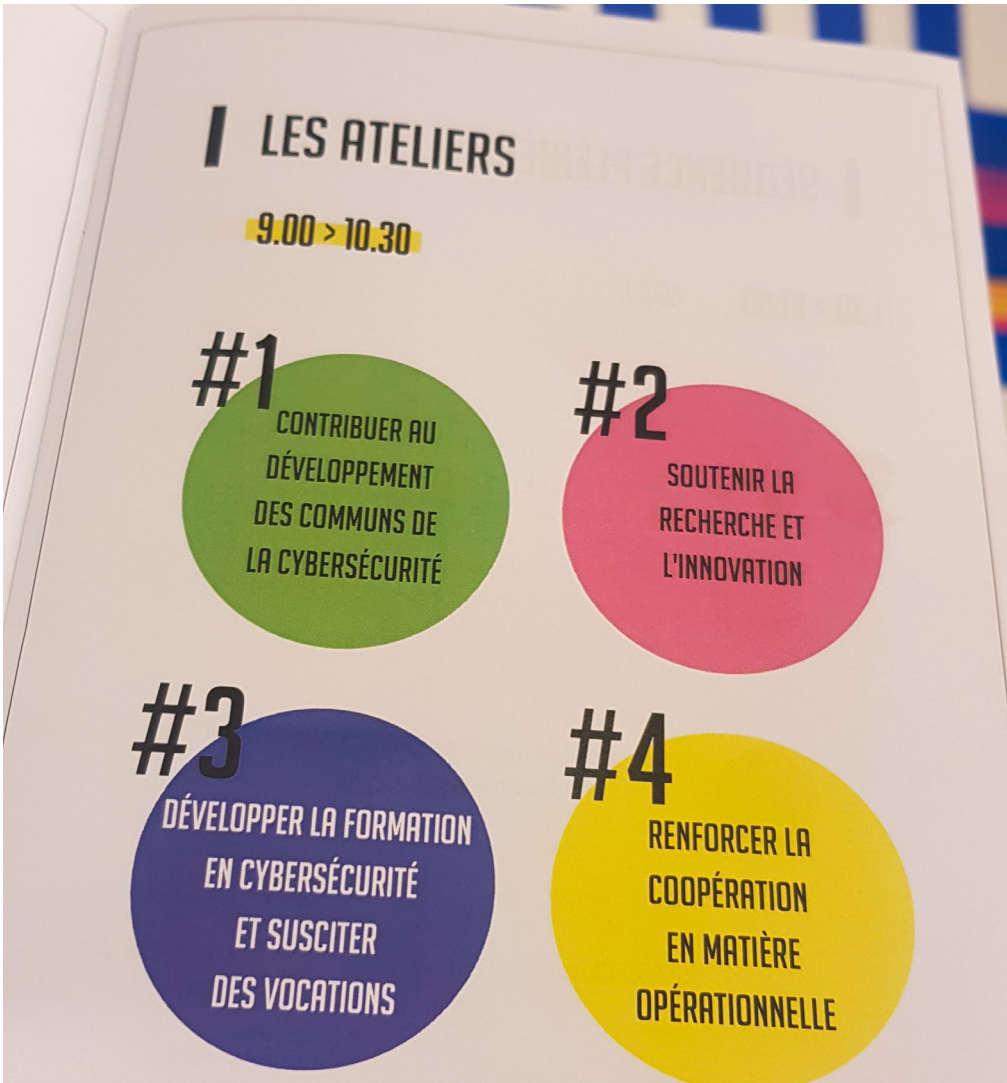
- **Renforcer les synergies entre l'ensemble des acteurs volontaires de la communauté au sein d'un tiers lieu opérationnel et ouvert**, nouveau centre de gravité pour les spécialistes français et européens, qui travailleront côte à côte au quotidien et autour de projets de recherche et d'innovation ;

- **Faire rayonner l'excellence scientifique, technique et industrielle française, en dotant pour la première fois la France et l'Europe d'un point d'entrée incontournable vers l'écosystème** de la sécurité et de la confiance numériques. Cette dimension sera amplifiée par la scénarisation du site, la rencontre des spécialistes et de démonstrations. Le Campus Cyber français sera dès le départ ouvert à la participation d'acteurs européens souhaitant s'inscrire dans la démarche ;

- **Être également un lieu totem et un levier pour le réseau national d'initiatives actuelles et futures en région, partageant les mêmes visions et ambitions**, à l'instar du pôle rennais, écosystème dynamique créé autour des enjeux de la cyberdéfense. Le Campus pourra, en outre, stimuler des logiques de réseau entre ces initiatives et bâtir un maillage territorial de Campus en Région ;

- **Relever collectivement le défi de la concurrence internationale dans le domaine des technologies et des usages numériques au regard des enjeux de sécurité qu'ils suscitent.**

Thèmes des ateliers collaboratifs, matinée spéciale Campus Cyber, 28 novembre 2019



Atelier collaboratif, matinée spéciale Campus Cyber, 28 novembre 2019

2 Missions : faciliter les projets multipartites et développer les communs de la sécurité et de la confiance numérique

DES PROJETS MULTIPARTITES

Visant à rapprocher des entités d'horizons différents et développer les synergies entre elles – à l'inverse d'un modèle en silos – **le Campus favorisera le mode projets impliquant plusieurs entités**, publiques, privées, académiques dans des domaines tels que :

> **« Atos, en tant que leader mondial de la cybersécurité, souhaite être un contributeur majeur du Campus Cyber. Ce projet va mettre en valeur les capacités exceptionnelles de la France dans ce domaine, de décupler les synergies et d'établir un écosystème structuré pour répondre à des enjeux de sécurité digitale toujours plus complexes. »**
>
> **Pierre Barnabé**
>
> *Senior Executive Vice President, Head of Big Data & Security Division chez Atos*

La recherche et l'innovation au travers de programmes communs qui rassembleront industriels, start-up et chercheurs selon un système partenarial et décloisonné. La conduite de travaux portant sur les logiciels libres, la cybersécurité industrielle, la cryptographie quantique et la cryptographie post-quantique, ou encore la connectivité et la sécurisation de la voiture autonome sont autant de pistes de projets associant différentes entités du Campus.

L'innovation de rupture pourrait également être soutenue grâce à un fonctionnement sur le modèle des grands défis. Le développement de la recherche partenariale permettra de développer les doctorats en la matière ainsi qu'une culture de la création et de l'innovation.

L'Anticipation et la détection des menaces informatiques : plusieurs entités souhaitent y positionner leurs CERT (*Computer Emergency Response Team*). Dans le respect d'un partage sécurisé et choisi de l'information, la localisation de ces équipes dans un même lieu permettra de renforcer pour tous ces acteurs leur capacité de veille, de détection et de traitement de la menace.

Une base de *threat intelligence* sera, sur cette base, développée, selon une logique de cercles de confiance, afin de mutualiser la connaissance de la menace numérique au bénéfice de tous.

La formation et l'entraînement : des programmes communs de formation et d'entraînement pourraient être mis à disposition au sein du campus, afin de répondre au besoin actuel de développer le capital humain en matière de cybersécurité. Ces formations pourraient être dispensées par des écoles ou centres de formation, de manière pérenne ou *ad hoc*.

DÉVELOPPER LES COMMUNS DE LA SÉCURITÉ ET DE LA CONFIANCE NUMÉRIQUES

Pratique historique devenue domaine de recherche philosophique, sociologique ou encore juridique, **l'idée des « communs » a déjà influencé de nombreux domaines et secteurs**, tels que l'environnement, les transports, le numérique, la connaissance, à l'initiative d'acteurs publics, de citoyen(ne)s ou encore d'acteurs privés.

Renvoyant à la **gestion collective d'une ressource partagée par une communauté** pouvant aller d'un groupe d'individus à la communauté humaine, **l'idée des communs oppose l'ouverture et l'intelligence collective à l'accaparement et au risque de duplication**. Les communs emportent également une conception différente de la gouvernance d'une ressource partagée, au travers de l'auto-organisation et de l'agilité.

Innovation Center, Skolkovo Technopark, Moscou, Russie

Des projets ambitieux, centrés sur le partage et l'exploitation commune des données, voient actuellement le jour et peuvent servir d'inspiration pour le Campus comme :

- Le « Health Data Hub » établi en 2018 par le gouvernement français, avec pour objectif de favoriser l'utilisation et de multiplier les possibilités d'exploitation des données de santé ;

- La Fabrique des mobilités, réseau ouvert de personnes, de compétences et de ressources, premier accélérateur de projets dédié à l'innovation dans les nouvelles mobilités, ayant placé les communs au cœur de sa démarche et disposant à cet égard d'une plateforme dédiée, accessible à toutes les personnes ayant participé à produire la ressource, légitimes pour en déterminer les règles d'accès.

L'idée des communs peut apparaître, en revanche, comme contre-intuitive en matière de cybersécurité, notamment au regard de la sensibilité des informations et des données associées à ces métiers. Pourtant, comme l'ont confirmé les échanges entre les participants à l'atelier collaboratif organisé par la mission le 28 novembre 2019, des communs peuvent être envisagés selon plusieurs thématiques :

- **Données, en particulier en matière opérationnelle :** dans ses modes opératoires et dans les vecteurs numériques dont elle tire parti avec agilité, la mise en commun de données relatives à la menace permettrait également de renforcer la capacité de chaque acteur, public ou privé, à être plus efficace dans leurs missions et leurs métiers. Les travaux menés autour du Grand défi « Automatisation de la cybersécurité » pourraient ainsi donner lieu à la création de communs, notamment autour des données ;

- **Expertises, en particulier en matière scientifique, technique et industrielle :** face à une compétition internationale en matière d'innovation et aux ruptures technologiques qui la nourrissent, développer le partage d'expertise, de connaissances et de données et la co-construction au sein de l'écosystème de sécurité et de confiance numériques en France et en Europe permettrait de renforcer fortement la sécurité des solutions produites et d'accélérer considérablement leur développement ;

- **Outils en licences libres :** pour accompagner, au moyen de logiciels Floss (free libre open source software dans la terminologie européenne), la co-construction d'outils élaborés, adaptés aux besoins de la communauté, pouvant faciliter les missions des spécialistes métiers et enrichir les offres de produits et de services, voire favoriser l'éclosion d'entreprises ;

- **Formation et sensibilisation :** face au défi de la formation, des ressources matérielles et immatérielles pourraient être partagées : expertises en matière d'ingénierie des formations en cybersécurité ou numérique ; organisation d'évènements, de camps d'été spécialisés, défis et compétitions communs à l'écosystème pour permettre la sensibilisation et développer les vocations chez les plus jeunes ; fédérer des offres de formation lorsque cela est pertinent, par exemple en matière de formation continue entre entreprises privées ;

- **Innovation :** à l'instar du partage de la connaissance sur les moyens, les outils de financement, d'incubation et d'accélération des start-up ; au travers d'évènements communs à l'écosystème, pour encourager les rencontres entre ces acteurs, de défis, de concours pour valoriser les solutions innovantes ;

- **Idées et connaissances :** en faisant émerger une capacité collective à penser les développements du numérique, tant sur le plan des technologies que sur celui des usages et de leurs conséquences dans tous les aspects des sciences humaines et sociales, sur les plans national, européen et international.

Penser les communs ne saurait toutefois signifier la fin de toute forme de compétition, mais offrir un espace dans lequel, la coopération et la co-construction puissent générer des opportunités durables pour tous, des opportunités qu'une trajectoire seulement individuelle n'aurait pas permis d'atteindre.

La cybersécurité des évènements de la Nation

Communauté associant l'ensemble des acteurs de la sécurité du numérique, le Campus pourrait constituer une plateforme privilégiée de préparation et d'accompagnement d'évènements ou de projets nationaux ou internationaux au regard de leur portée vis-à-vis des enjeux de sécurité et de confiance numériques.

À titre d'illustration, les trois évènements suivants seraient potentiellement susceptibles de bénéficier du soutien du campus :

- **Les Jeux olympiques de 2024 :** le numérique y jouera un rôle de premier plan — notamment en matière de sécurité — dans un Paris devenu « ville intelligente ». Pendant la durée des Jeux, le Campus pourrait participer à héberger l'alliance des industriels français engagés pour assurer la cybersécurité des Jeux olympiques de Paris 2024, dans le cadre du CSF.

- **La présidence française du Conseil de l'UE de 2022 :** la communauté académique associée aux autres acteurs du Campus, appuierait, en tant que de besoin, le travail des cabinets et administrations en charge de la préparation de cette présidence.

- **L'Appel de Paris pour la confiance et la sécurité dans le cyberespace :** le Campus pourrait contribuer aux travaux d'expertise qui découlent de la démarche engagée par l'appel lancé par le Président de la République en 2018, ou accompagner sa manifestation annuelle au long cours.

The London Office for Rapid Cybersecurity Advancement (LORCA), Plexal innovation centre, Queen Elizabeth Olympic Park, Londres, Royaume-Uni

3 Structure : un tiers lieu opérationnel pour travailler, rapprocher et innover

UN TIERS-LIEU DE TRAVAIL

Le Campus devra être un espace de travail partagé et de rencontres pour l'ensemble de ses parties prenantes. Il devra être adapté à la diversité des métiers de la cybersécurité et du numérique et de ses acteurs, publics ou privés, jeunes ou matures.

« Capgemini est enthousiaste à l'idée de réunir dans un même lieu la diversité des acteurs publics et privés, de toutes tailles. Cela permettra d'accélérer le développement des compétences, de gagner en efficacité, de créer plus de synergies entre les acteurs clés de la cybersécurité et ainsi de permettre à la France d'être à la pointe de la recherche et de l'innovation dans le domaine. »

Hélène Chinal

DG Capgemini Technology Services – Head of operations BU France

Visant à rapprocher des acteurs d'horizons divers, **l'aménagement du Campus sera conçu selon un double objectif :**

- **Accueillir des entités souhaitant conduire leurs activités dans le Campus ;**
- **Stimuler les effets de réseaux et la co-construction au travers de lieux propres à chaque entité.**

DES ESPACES EN PROPRE ET DES ESPACES PARTAGÉS

Afin de développer les synergies et aider à développer les communs, le Campus devra en particulier comprendre :

- **Des plateaux projets**, pouvant être réservés à titre temporaire par plusieurs membres du Campus et leurs éventuels partenaires extérieurs ;
- **Un auditorium** permettant l'organisation d'évènements d'ampleur nationale, de conférences, remises de prix, etc ;
- **Des espaces permettant d'accueillir des cycles de formation ;**
- **Des espaces dédiés à l'innovation collaborative**, permettant d'organiser des ateliers, hackathons, évènements d'accompagnement de l'innovation (talent fair, scale up fair, challenges, etc.) ;
- **Des espaces de coworking** ;
- **Des lieux de convivialité** (cafés, restauration)

UNE STRUCTURE D'ANIMATION

Une structure dédiée au Campus Cyber sera créée afin de :

- **Faire fonctionner au quotidien la structure Campus** en gérant, par exemple, l'allocation des espaces, la collecte des loyers et des montants des prestations, la gestion de l'infrastructure et des services partagés (ex. sécurité) ;
- **Animer la vie du Campus pour développer les synergies et les effets de réseau** entre entités (évènements, rencontres, vie numérique, etc.) ;
- **Développer les relations du Campus avec d'autres initiatives en Région ou à l'international.**

À titre de comparaison, l'équipe d'animation de la Station F – 34 000 m² – est composée d'une trentaine de personnes, sans compter les prestataires.

Atelier collaboratif, matinée spéciale Campus Cyber, 28 novembre 2019

4 Participants : le point de rencontre pour des acteurs et des métiers de tous horizons

UNE DIVERSITÉ D'ENTITÉS

Pensé pour favoriser les effets de réseaux dans une logique d'inspiration mutuelle et d'intérêt commun, le Campus Cyber réunira **des acteurs d'horizons divers :**

- **Start-up, PME et acteurs de l'accompagnement de l'innovation**, apportant avec eux l'agilité et la créativité nécessaires à la transformation des idées et parfois des ruptures technologiques, gage des conquêtes industrielles futures ;

- **Industriels de la cybersécurité et du numérique**, apportant avec eux la maturité, le rayonnement international et la capacité à porter des projets d'envergure, dont ils pourront faire bénéficier les acteurs plus jeunes ;

> **« L'ANSSI est convaincue de l'intérêt majeur d'implanter une partie de ses activités au cœur de l'écosystème qui se fédérera au sein du Campus »**
>
> **Guillaume Poupard**
> *Directeur général, ANSSI*

- **Centres et instituts de recherche**, en particulier Inria, acteur central de la recherche et de l'innovation publique, apportant la recherche fondamentale et appliquée ;

- **Utilisateurs ou associations ou fédérations professionnelles**, apportant la connaissance sectorielle des attentes et des contraintes de la transformation numérique des métiers ;

- **Centres de formation initiale et continue, publics, académiques ou privés**, pouvant établir tout ou partie de leurs activités d'enseignement en lien avec la cybersécurité, de manière pérenne ou *ad hoc*. La proximité des étudiants, des centres de recherche et d'acteurs industriels permet également d'envisager la mobilisation des premiers au profit des autres. À terme, la formation sur le Campus de futurs ingénieurs et autres spécialistes pourrait faciliter des démarches de création de start-up.

La transformation de la voie professionnelle, annoncée par le ministre de l'Éducation nationale et de la Jeunesse Jean-Michel Blanquer, est une réelle opportunité pour répondre aux nouveaux besoins de compétences pour les métiers de demain, en particulier les métiers du numérique. Cette transformation se traduit par l'ouverture en 2021 de la famille « Métiers du numérique et de la transition énergétique » et par la promotion des campus comme lieux par excellence d'attractivité de la voie professionnelle. La rénovation de la filière de formation au numérique est engagée dans cette voie : elle va donner lieu à la création de nouveaux diplômes, en particulier en cybersécurité. Grâce à l'installation du Campus Cyber, les jeunes en formation bénéficieront ainsi d'un environnement entrepreneurial et technique au plus proche de leur futur métier ;

- **Les services concernés de l'État et en particulier l'ANSSI**, mais également les ministères des armées et de l'Intérieur, dont la présence est considérée comme un facteur clé de succès du Campus et pour certains un prérequis à leur installation. Facilitateur, l'État pourra faire office de catalyseur et de fédérateur autour des projets d'intérêt commun, par exemple à partir des données. Il constituera également une ressource en expertise, en outils et en données, participant à la montée en compétences de l'ensemble de l'écosystème ;

- **Le capital-risque**, apportant le financement nécessaire au lancement des start-up, mais aussi à l'accélération internationale de PME prometteuses, souvent en déficit d'accompagnement au moment le plus critique où elles ont besoin de faire passer leur activité à l'échelle ;

- **Les représentants du champ des idées et des perceptions**, pour collectivement mieux anticiper et répondre aux défis de la sécurité et de la confiance numériques, notamment eu égard aux enjeux géopolitiques et aux ruptures technologiques actuelles et à venir ;

- **Des entités européennes et internationales ;**

- **Des acteurs du monde du numérique ou d'autres secteurs.**

La diversité des entités représentées devra également s'incarner dans le fait qu'aucune d'entre elles ne dispose d'une position excessivement prépondérante dans le Campus, en s'accaparant, par exemple, une part trop conséquente de la surface du lieu pour un nombre de spécialistes trop important.

Campus : un modèle pour l'accélération des start-up

Le Campus réservera une place particulière aux start-up et aux PME, forces émergentes d'un écosystème en perpétuel développement.

Alors que la France compte déjà de nombreuses pépinières et incubateurs susceptibles d'accompagner efficacement les start-up en phase de lancement – à l'instar de la Station F – leur colocalisation au sein d'un Campus spécialisé avec des acteurs académiques, publics et industriels de premier plan favorisera leur développement en France et à l'international.

Les start-up qui seront amenées à interagir avec le Campus bénéficieront, en particulier, d'une dynamique d'accélération grâce à leur positionnement auprès des grandes entreprises et d'entreprises de taille intermédiaire, avec qui elles travailleront et qui pourront notamment accroître la visibilité de leurs offres. Les solutions ainsi testées et approuvées verront leur développement facilité sur le marché du numérique, y compris au niveau européen et international. La présence d'organismes de conseil, de financement et d'accompagnement participera à cette dynamique écosystémique.

Afin de garantir leur capacité à s'installer aux côtés d'acteurs plus matures, **une part du loyer des start-up sera prise en charge par les entreprises plus matures**. Les start-up pourront également bénéficier de formes de mécénat privé ou de subventions publiques afin de faciliter leur installation.

UNE DIVERSITÉ DE MÉTIERS

Au-delà de la diversité des acteurs présents dans le Campus, **la diversité des métiers de la sécurité et de la confiance numériques a vocation à être représentée**, sans toutefois aucun caractère contraignant à l'égard des entités souhaitant rejoindre le Campus.

À titre d'exemple et sans caractère d'exhaustivité :

- Laboratoires de recherche publics et privés ;
- Capacités de gestion de crise et d'entraînement, dont un *cyber range* [1] ;
- Capacités de supervision – tels que les SOCs [2] – et de détection ;
- Capacités de réponse opérationnelle aux cyberattaques – tels que les CSIRTs [3] (équipes de réponse à incidents) ;
- Développement de produits et de services ;
- Cycles de formation initiale et continue ;
- Activités de conseil ;
- Incubateurs, accélérateurs ;
- Activités associatives ;
- Groupes de réflexion.

UNE OUVERTURE À L'EUROPE ET L'INTERNATIONAL

Parce que le succès de l'écosystème français de cybersécurité et de confiance numérique passera par son étroite connexion avec les développements, l'innovation et les marchés internationaux, **l'ouverture à l'international du Campus Cyber passera par la capacité de ce dernier à accueillir des entités du monde entier.**

Future plateforme internationale pour l'innovation en cybersécurité, **le Campus Cyber devra néanmoins permettre l'activité d'entités traitant d'enjeux de sécurité nationale.**

À cette fin, l'ouverture internationale du Campus s'effectuera dans une logique de cercles de confiance, permettant des zones, projets et infrastructures d'accès restreint.

1 Plateforme d'entraînement.
2 Security Operations Center.
3 Computer Security Incident Response Teams.

Localisation, forme juridique et financement

1 Un Campus attractif à Paris ou dans la petite couronne Ouest

Différents scénarios d'installation géographiques – à court terme, dans une logique de lancement rapide – ont été envisagés, autour de trois options principales :

1/ Une installation nouvelle en Région dans une logique de dynamisation d'un territoire ;

2/ Une installation en Île-de-France (grande et très grande couronne) auprès d'acteurs, notamment académiques, déjà implantés ;

3/ Une installation dans Paris intra-muros ou petite couronne Ouest, proche de la Défense, accessible par les transports en commun.

> **« Depuis notre implantation sur la Défense, nous avons multiplié notre taux d'attractivité par 2 et réduit notre turnover de 35 % »**
>
> **Ludivine DE LAVISON**
> *DRH Orange Cyberdefense*

Une installation à Paris ou dans sa proximité immédiate s'impose comme la meilleure des options de l'avis général des interlocuteurs rencontrés dans le cadre de la mission. C'est même, pour certains, notamment les start-up, un prérequis à leur engagement dans le Campus.

Trois raisons principales conduisent à privilégier cette option :

1/ L'enjeu critique de l'attractivité des talents au sein du Campus, dans un contexte de rareté en termes d'ingénieurs et d'autres spécialistes de la cybersécurité et du numérique. À la différence de Beer Sheva, dont l'éloignement géographique constitue une limite observée, la proximité du Campus d'un centre urbain, rapidement et facilement accessibles en transports en commun et sa localisation dans un environnement vivant et dynamique, constitue un élément du succès des campus et parcs technologiques internationaux récemment établis. **Les entreprises rencontrées, en particulier les start-up et industriels de la cybersécurité ont, à cet égard, unanimement soutenu l'établissement du Campus Cyber à Paris ou dans la petite couronne Ouest ;**

2/ La nécessité de tirer parti au maximum d'un écosystème de cybersécurité et de la confiance numérique, particulièrement développé et divers à Paris ou à proximité de la capitale, qu'il serait contre-productif de déplacer ;

3/ La pertinence d'une localisation au cœur des nœuds de communication français, européens et des flux internationaux des spécialistes scientifiques et techniques, industriels et financiers ainsi qu'à proximité des pouvoirs publics français ou européens. Placer le Campus ailleurs qu'à Paris ou en Île-de-France reviendrait à faire le choix impossible de déplacer un écosystème principalement établi au sein et proche de la capitale de la France.

Compte tenu des manifestations d'intérêts formulées par les entreprises, instituts et acteurs étatiques rencontrés, **la taille du Campus devrait atteindre plus de 10 000 m²**. Ce chiffre devra être ajusté à la réception des engagements formels.

Un totem pour un réseau national d'initiatives en Région

La France comprend déjà des bassins de recherche et d'innovation dans de nombreux domaines scientifiques et techniques. En matière de cybersécurité, on peut citer, sans caractère d'exhaustivité, le dynamisme des régions Bretagne, Pays de la Loire, Auvergne-Rhône-Alpes, Hauts-de-France, Nouvelle Aquitaine (voir en annexe les propositions reçues de la part de la Métropole européenne de Lille, de la Région des Pays de la Loire et du Pôle d'excellence cyber de Rennes).

Le Campus ne pourra pas accueillir et fédérer en son sein l'ensemble des acteurs pertinents en France.

C'est pourquoi le développement de Campus Cyber régionaux, à partir d'initiatives existantes ou nouvelles, permettrait de démultiplier les effets de réseaux à l'échelle du territoire, en tirant parti des forces des différents écosystèmes et en développant les expertises dans des domaines spécialisés tels que la e-santé, la sécurité industrielle, les villes intelligentes ou les objets connectés.

L'ensemble de ces initiatives pourraient être regroupées au sein d'une « entité ombrelle » (ex. fondation, fonds de pérennité, association, etc.).

2 Un Campus financé par ses membres, disposant d'une gouvernance agile

STRUCTURE JURIDIQUE

La structure juridique qui portera le projet de Campus doit permettre, par une gouvernance agile et un fonctionnement collaboratif, de rassembler les acteurs de l'écosystème de la sécurité du numérique. Celle-ci doit, en particulier, permettre des collaborations opérationnelles visant l'industrialisation et la rentabilisation des projets, qui seront portées de manière autonome par les différents partenaires sur la base de conventions *ad hoc*.

Afin de favoriser la coopération des parties prenantes, le montage juridique de pilotage doit être prévu comme support à la mise en œuvre effective du Campus autour de plusieurs axes : les coopérations opérationnelles [4], la gestion des communs [5], la logistique et, enfin, la recherche et les travaux académiques. Ce montage doit être doté de la personnalité juridique adaptée à la prise d'actes de gestion relatifs à ces activités.

Agissant dans un domaine concurrentiel en forte croissance, cette structure devra offrir un cadre juridique propice à une gestion souple et agile entre des parties prenantes de natures et aux finalités diverses, essentiellement privées, mais également publiques.

Projet porté par le secteur privé, la présence publique devra être minoritaire (instituts ou établissements de recherche, administrations, potentiellement des collectivités territoriales, etc.) et le contrôle étatique limité (administratif, financier et comptable).

La structure doit également pouvoir bénéficier de ressources et moyens nécessaires à son fonctionnement, visant à terme une autonomie financière : apports en numéraire, investissements, absence de subventions publiques directes en dehors, éventuellement, des projets de coopérations.

Un fonctionnement sur le modèle de cercles de confiance est, pour finir, souhaité en fonction des projets et du type d'informations traitées.

Sur la base des critères précédents, certaines structures ont été écartées et d'autres apparaissent comme adaptées pour le projet de Campus.

4 Gestion des infrastructures communes, location des locaux aux parties prenantes, gestion des accès sécurisés, opérabilité des ressources informatiques ouvertes (cloud, data center), animation du campus, etc.

5 Outils open source, plateformes de données, un bouquet de services en guichet, formations, etc.

LES SOLUTIONS ÉCARTÉES POUR LE PILOTAGE DU CAMPUS

STRUCTURES ÉCARTÉES :

Groupement d'intérêt public et l'établissement public
Structures publiques avec une gouvernance publique inadaptée à un projet porté par des acteurs du secteur privé.

Groupement d'intérêt économique
Structure qui peut présenter un risque juridique et financier en raison de la responsabilité illimitée et solidaire des membres.

Structure peu souple quant à son objet et inadapté au projet de Campus puisque les activités d'un GIE sont nécessairement auxiliaires à celles de ses membres) et à ses modalités de financement

Fondation reconnue d'utilité publique
Structure qui nécessite une procédure de création complexe pour obtenir la reconnaissance d'utilité publique, qui n'est pas assurée au regard de l'objet du Campus et de ses activités.

Structure avec une gouvernance non adaptée à la logique de cercles de confiance.

Autres types de fondations
Structure dont les conditions de création et de gouvernance ne correspondent pas aux caractéristiques du projet :

> la fondation abritée qui n'a pas la personnalité morale ;
> la fondation d'entreprises dont l'Etat ne peut être directement membre et exclurait de fait certaines entités publiques ;
> le fonds de dotation tant pour son objet uniquement d'intérêt général que pour ses modalités de fonctionnement ;
> la Fondation de coopération scientifique qui a un objet spécifique trop restreint pour l'ensemble du projet Campus : la recherche et la formation.

Association
Structure envisagée, mais écartée au profit de la SAS en raison de la plus grande flexibilité laissée par la SAS sur la nature des activités exercées.

Société anonyme
Structure qui pourrait correspondre aux caractéristiques du projet, mais qui présente l'inconvénient d'une gouvernance peu souple.

LA SOLUTION RECOMMANDÉE POUR LE PILOTAGE DU CAMPUS

L'approche retenue vise à articuler le pilotage du campus autour d'une structure juridique de type société anonyme simplifiée – SAS dans laquelle l'Etat n'a pas vocation à devenir l'actionnaire majoritaire.

La SAS présente l'avantage de l'agilité et de répondre aux critères définis pour le projet.

Cette SAS aurait pour objet de gérer la logistique et l'animation du Campus.

Sous réserve d'un feu vert donné à la préfiguration opérationnelle du Campus Cyber, le montage juridique d'ensemble et particulièrement le détail de l'actionnariat de la SAS fera l'objet d'un examen attentif à l'issu de la remise du présent rapport, en lien avec les entreprises et les services concernés de l'État.

FINANCEMENT ET BUDGET

Le financement du Campus inclut deux phases importantes :

1/ La phase de lancement : impliquant un financement initial, nécessaire au déploiement des infrastructures et services indispensables au fonctionnement du futur Campus.

Basée sur le coût d'une réhabilitation et d'un aménagement récent selon la localisation géographique correspondant aux préconisations de ce rapport (10 000 m² pour 700 postes dans l'Ouest parisien), l'estimation budgétaire nécessaire à l'installation du campus est de 11 000 euros d'investissement par poste environ.

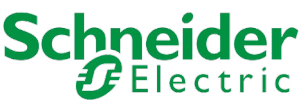
Ce montant pourrait être financé par les acteurs privés aux côtés de l'État et des collectivités territoriales, dont la région Île-de-France qui a déjà fait part de son intérêt pour le projet. **La structuration budgétaire de ce financement pourra être précisée dans la phase d'opérationnalisation du projet.**

2/ La phase de fonctionnement normal du Campus : afin d'être viable financièrement dès le démarrage et notamment ne pas dépendre de subventions publiques, les coûts liés au fonctionnement et à l'animation du Campus seront ensuite autofinancés sur la base des loyers versés par ses membres et de la facturation des prestations de service associées au lieu (ex. auditorium, salles de formation, etc.). À titre de comparaison, le coût de fonctionnement annuel de Station F est estimé à 7 à 8 millions d'euros.

Au-delà du financement du lancement du Campus Cyber parisien, des collectivités sont prêtes à investir pour le développement de Campus régionaux, à l'instar de la Région Pays-de-Loire et de la métropole européenne de Lille, comme en attestent les courriers en annexe.

Déclarations de soutien

Secteur privé



Secteur public

Organismes de formation

Associations

CESIN

CLUSIF

PÔLE D'EXCELLENCE CYBER

FRANCE DIGITALE

System X
INSTITUT DE RECHERCHE TECHNOLOGIQUE

syntec numérique

Entités européennes et internationales

CISCO

data iku

FORTINET

IBM

kaspersky

Microsoft

ORACLE

pwc

SIEMENS

TREND MICRO

VARONIS

vmware

ANNEXES

Annexe 1 – Liste des entités auditionnées

ACE Management
François LAVASTE & Quentin BESNARD

Advens
Alexandre FAYEULLE

Airbus Cybersecurity
Frédéric JULHES

Airbus Defence & Space Cybersecurity
Romain QUEINNEC

Alsid
Emmanuel GRAS

Alstom
Stephane DETRUISEUX

Ambassadeur français pour le numérique
Henri VERDIER

ANSSI
Guillaume POUPARD

Atos
Pierre BARNABE & Philippe DULUC

Beijaflore
Maxime DE JABRUN

BNP Paribas
Bernard GAVGANI

Bpifrance
Pascal LAGARDE & Guillaume CALI

Capgemini
Hélène CHINAL & Édouard JEANSON

CEA
Bruno CHARRAT

CEIS
Guillaume TISSIER & Clément RIOU

CESIN
Mylène JAROSSAY & Alain BOUILLE

CIGREF
Jean-Claude LAROCHE

Citalid
Maxime CARTAN

CLUSIF
Jean-Marc GREMY & Luména DULUC

Comité stratégique de filière pour les industries de la sécurité
Marc DARMON & Jean-Noël DE GALZAIN

Cybermalveillance.gouv.fr
Jérôme NOTIN

EDF
Olivier LIGNEUL, Christophe SALOMON & Valérie DEROUET

ENEDIS
Jean-Claude LAROCHE

EPITA
Joël COURTOIS

France Digitale
Marianne TORDEUX

Gatewatcher
Jacques DE LA RIVIERE

Gendarmerie nationale
Colonel Éric FREYSSINET

IBM
Nicolas SEKKAKI

Ikare & CCEF Israël
Anna BAER

INRIA
Bruno SPORTISSE

Kaspersky
Tanguy DE COATPONT

L'Oréal
Etienne AUBOURG & Alain BERNARD

Métropole européenne de Lille
Cathy BUQUET

Microsoft
Bernard OURGHANLIAN

Ministère des Armées
Général Didier TISSEYRE, Vice-amiral Arnaud COUSTILLIERE, ICA Frédéric VALETTE & Martin BRIENS

Ministère de l'Éducation nationale et de la Jeunesse
Édouard GEFFRAY

Ministère de l'Enseignement supérieur de la Recherche et de l'Innovation
Nicolas CASTOLDI

Oodrive
Édouard DE REMUR

Oracle
Philippe ROUSSET & Matis PELLERIN

Orange
Hugues FOULON

Pôle d'excellence cyber
Philippe VERDIER

Police judiciaire
Catherine CHAMBON

Préfecture de Meurthe-et-Moselle
Éric FREYSSELINARD

Région des Pays de la Loire
Christelle MORANÇAIS & Patrick LANGRAND

Région Ile de France
Valérie PECRESSE & Othman NASROU

Rennes Métropole
Paul-André PINCEMIN

Saint-Quentin en Yvelines
Anne FAHY

Schneider Electric
Christel HEYDEMANN

SGPI
William LECAT

Shushane & Co
Nelly SOUSSAN

Siemens France & Benelux
Nicolas PETROVIC

Simplon
Frédéric BARDEAU

Skolkovo Foundation
Arkady DVORKOVICH

Sopra Steria
Arnaud CAILLEAU & Jean-Luc GIBERNON

Start-up Nation Central
Jérémie KLETZKINE

Syntec Numérique
Émilie DUMERAIN & Philippine LEFEVRE

Thales
Hervé DERREY & Marc DARMON

TransformIT
Stéphane AYACHE

Ville de Boulogne Billancourt
Pierre-Christophe BAGUET

Ville d'Issy Les Moulineaux
Direction de l'urbanisme

VMware
Anthony CIROT, Pierre ARDICHVILI & Dahlia KOWNATOR

Wavestone
Pascal IMBERT

Yes We Hack
Guillaume VASSAULT-HOULIÈRE

Annexe 2 – Lettre de mission

Le Premier Ministre

1133/19/SG

Paris, le 16 JUIL. 2019

Monsieur le président-directeur général,

À l'heure où les cyberattaques sont susceptibles de porter atteinte aux intérêts vitaux de la Nation et de remettre en cause la soutenabilité des usages numériques, il est nécessaire d'organiser la montée en puissance des acteurs du numérique et de l'innovation sur les enjeux de cybersécurité.

Si les capacités et l'engagement de l'État demeurent essentiels, le renforcement du niveau de sécurité numérique s'obtiendra par une association étroite des différents acteurs nationaux publics et privés. Pour garantir la sécurité de la transformation numérique et garder la maîtrise de notre souveraineté dans l'espace numérique, l'État doit pouvoir s'appuyer sur un tissu industriel fort, en complément de son action. Cette dynamique vertueuse entre secteurs public et privé est également nécessaire pour faire de nos entreprises du secteur des leaders mondiaux, y attirer les meilleurs talents et soutenir leur capacité à créer des emplois en France. Il s'agit d'une attente forte des acteurs industriels.

La France tient la comparaison internationale. Elle dispose d'acteurs industriels de premier plan, de startups, petites et moyennes entreprises innovantes et d'une recherche dynamique. Cet écosystème est toutefois fragmenté et il pâtit de synergies insuffisantes entre ces différents acteurs, d'une part, et le monde du numérique et de l'innovation, d'autre part. D'autres pays ont fait le choix de politiques ambitieuses pour fédérer leurs écosystèmes nationaux. Israël, en particulier le CyberSpark à Beer-Sheva, se distingue sur le plan international et constitue de ce point de vue un exemple inspirant.

Fort de ces constats, le Gouvernement a engagé, avec les acteurs industriels, un chantier de structuration de la filière, par la labellisation, le 22 novembre 2018, du comité stratégique de filière (CSF) « Industries de sécurité » au sein du conseil national de l'industrie. Ses membres, acteurs privés et publics, finalisent actuellement les projets structurants d'intérêt commun pour la filière, notamment dans le domaine de la cybersécurité, qui feront l'objet d'engagements dans un contrat de filière avec l'État.

Monsieur Michel VAN DEN BERGHE
Président directeur général
Orange Cyberdefense
54, place de l'Ellipse

92983 PARIS LA DÉFENSE

Dans ce contexte, le Président de la République a souhaité qu'une dynamique soit engagée pour mettre en place un « campus cyber », porté par les acteurs industriels et fédérant l'écosystème français de cybersécurité. Dédié à la recherche de synergies, un tel projet devrait étroitement associer le monde académique et le secteur public et poursuivre l'objectif de renforcer nos capacités d'innovation, en alliant nos atouts spécifiques dans le secteur de la cybersécurité à ceux dont nous disposons plus généralement dans le monde du numérique et de l'innovation.

Trois grands acteurs privés impliqués en matière de cybersécurité – Orange, Thales et Atos – se sont rapidement mobilisés pour répondre à cet appel à l'élaboration d'un tel projet de « campus cyber ». Fort de la détermination de ces trois entreprises et considérant votre longue expérience d'entrepreneur et votre connaissance très fine des acteurs de la cybersécurité, je souhaite recueillir votre avis sur l'opportunité, la faisabilité, le périmètre souhaitable et les conditions de réussite de ce projet, notamment s'agissant de sa viabilité économique, sa gouvernance et de son financement.

En s'appuyant sur l'expérience française des pôles de compétitivité, vos réflexions pourraient notamment permettre d'évaluer l'intérêt d'une plateforme de mutualisation de données sectorielles et de partage de connaissances sur l'état de la menace. Vous pourriez également proposer plus largement les mises en commun de moyens, physiques ou numériques qui pourraient être constitutives du « campus cyber ». La possibilité de développer les parcours croisés entre les secteurs public et privé pourrait également être envisagée. Il est indispensable que la valeur ajoutée de ce projet soit réelle et clairement identifiée, par rapport aux démarches existantes ou envisagées par ailleurs, aux niveaux européen, national et local.

Je souhaite que vos travaux puissent se faire en étroite concertation avec le CSF « Industries de sécurité » et, en particulier, avec son président, Marc Darmon. La question se pose notamment de l'opportunité d'intégrer cette nouvelle initiative dans le cadre du CSF ou, dans le cas contraire, des modalités d'articulation entre les deux projets permettant de capitaliser sur la dynamique de structuration du secteur déjà engagée par le CSF.

L'agence nationale de la sécurité des systèmes d'information (ANSSI) vous apportera tout le soutien nécessaire pour mener à bien cette mission. La direction générale de l'armement (DGA), la direction générale des entreprises (DGE), les services du ministère de l'enseignement supérieur, de la recherche et de l'innovation (MESRI), ainsi que la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), pourront également vous accompagner en tant que de besoin.

En étroite coordination avec le secrétariat d'État au numérique, vous me rendrez compte de votre mission avant la fin de l'automne 2019.

Je vous prie de croire, Monsieur le président-directeur général, à l'assurance de ma sincère considération.

Philippe

Édouard PHILIPPE

Annexe 3 – Lettre de la Maire de la Ville de Lille, du Président de la Métropole Européenne de Lille et du Président du Conseil régional des Hauts-de-France

ville de Lille

MEL MÉTROPOLE EUROPÉENNE DE LILLE

Région Hauts-de-France

Réf. DC/

Monsieur Edouard PHILIPPE
Premier ministre
Hôtel Matignon
57 rue de Varenne
75007 Paris

Lille, le 13/12/2019

Monsieur le Premier ministre,

Par décision du 23 juillet 2019, vous avez confié à M. Michel VAN DEN BERGHE la mission de préfigurer un grand campus de la cybersécurité afin de doter la France d'un écosystème de première importance pour renforcer la stratégie de défense et de lutte contre les cyber-menaces.

Ce campus s'organiserait autour d'un campus central à Paris et de campus satellites, le tout ayant vocation à favoriser la montée en puissance des acteurs du numérique sur le sujet, à développer l'innovation et la collaboration entre entreprises et laboratoires, à renforcer la formation pour combler le déficit d'experts.

Eu égard aux enjeux et de leur capacité à contribuer au positionnement de la France comme leader européen de la cybersécurité, des acteurs de la métropole dont en premier lieu Advens, Orange CyberDefense, OVH, Stormshield, Thales Six, Vadesecure, l'Université de Lille, le centre Inria Lille-Nord Europe se joignent à nos trois collectivités pour proposer un campus satellite résolument positionné sur la cybersécurité des territoires, des personnes, des entreprises et des collectivités.

Le campus intègre :

- des capacités de Recherche, de Recherches technologiques, de R&D ;
- un espace d'analyse et de prospective notamment pour la compréhension des signaux faibles et, en réponse, la mise en place d'actions de R&D avec les entreprises mais aussi avec des startups qui se sont positionnées comme offreuses de solutions sur l'ensemble de la chaîne de valeur.

Ces objectifs sont :

- de développer des capacités d'expérimentation grande échelle et d'innovation sur tous les segments de la chaîne de valeur ;

- de renforcer la place à l'international des entreprises éditrices de solutions cybersécurité ;
- d'accompagner les PME, PMI et ETI et les communes pour qu'elles soient moins vulnérables aux attaques cyber ;
- de favoriser le développement des technologies et leur maîtrise par les entreprises en s'appuyant sur les centres techniques et de transfert présents sur le territoire ;
- de structurer et rendre lisible un corpus de formations et de développer des outils pédagogiques à destination des très jeunes et des publics non avertis pour qu'ils deviennent des acteurs avisés de la sûreté numérique ;
- d'assurer l'ouverture nord-européenne du campus France au regard de notre proximité avec Bruxelles, Londres et le quartier général du commandement allié Opérations (ACO) de l'OTAN à Mons.

En termes de thématique, le campus définit son positionnement en appui du retail, de la santé, du sport et de la sûreté et la résilience urbaine dans une démarche :

- intégrant :
  - la protection des données personnelles ;
  - l'analyse par l'IA des informations et données pour la détection comportementale d'anomalies ;
  - la résilience des systèmes de gestion de transports, de distribution de l'eau et de l'énergie, de la gestion de la voirie et des déchets, etc…
- induisant des solutions allant de la collecte et du transport de l'information jusqu'au stockage, la valorisation et l'exploitation de la donnée.

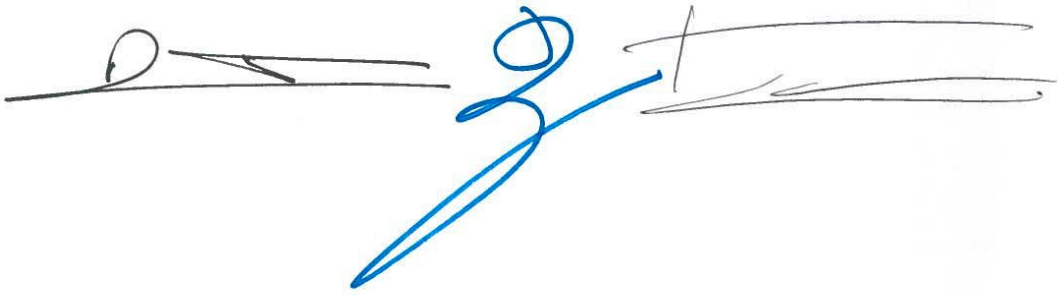
En appui, nous proposons deux lieux d'accueil, tous les deux emblématiques du numérique et de la recherche en métropole :

- le parc d'activités de la Haute Borne (140 ha, 310 000 m² de bureaux), à proximité immédiate de l'Université de Lille et des centres de recherches de l'Inria et du CNRS et site d'implantation d'entreprises déjà engagées sur les marchés de la cybersécurité et de sièges sociaux de groupes utilisateurs de solutions ;
- Euratechnologies au sein des Rives de la Haute Deûle (38 ha), lieu « totem » de notre écosystème numérique et de la Capitale French Tech Lille.

Compte tenu de l'importance du projet pour notre territoire, nous comptons sur votre soutien et restons pleinement à disposition de vos équipes et de M. VAN DEN BERGHE pour tout échange que vous jugerez utile dans la proximité de la décision gouvernementale.

Nous vous prions de croire, Monsieur le Premier ministre, à l'expression de notre haute considération.

La Maire de la Ville de Lille	Le Président de la Métropole Européenne de Lille	Le Président du Conseil Régional des Hauts de France
Martine AUBRY	Damien CASTELAIN	Xavier BERTRAND



Annexe 4 – Lettre de la Présidente de la Région des Pays de la Loire

RÉGION DES PAYS DE LA LOIRE

La Présidente

Nantes, le 6 - DEC. 2019

DGAE2I/CD/2019-12

Monsieur VAN DEN BERGHE
Directeur Général d'Orange
Cyberdéfense
54 Place de l'Ellipse
92 983 PARIS LA DEFENSE

Monsieur,

Je souhaitais vous remercier pour la qualité de notre échange du 15 novembre dernier et l'attention que vous avez portée à notre réseau de Technocampus.

A cet égard, j'ai le plaisir de vous transmettre une note synthétique précisant le maillage et l'offre de services de ces plateformes technologiques d'excellence. Ce document met également en exergue ce que je considère être de véritables atouts pour accueillir dans un futur proche un campus de la cybersécurité en Pays de la Loire.

Je vous prie d'agréer, Monsieur, l'expression de ma considération distinguée.

Bien Cordialement

Christelle MORANÇAIS

Région
PAYS DE LA LOIRE

La Région des Pays de la Loire se mobilise pour accueillir le futur campus de la cybersécurité

L'ambition d'un « smart territoire régional »

Dans le cadre de la transition numérique qui bouleverse nos organisations et la vie de nos concitoyens, la Région des Pays de la Loire a adopté en 2017 une stratégie numérique ambitieuse pour un « smart territoire régional » au service de tous, posant la « donnée » au cœur de cette transformation pour concevoir, gouverner et gérer différemment notre service public régional.

Au cœur de cette stratégie, deux axes sont priorisés : le **soutien au renforcement des compétences numériques** et **l'accompagnement à la transformation numérique des entreprises ligériennes**.

Afin **d'assurer une solidarité face à des défis techniques majeurs** sur l'ensemble de notre territoire régional, le numérique a été intégré au sein des politiques publiques, visant à accompagner les territoires dans cette mutation mais aussi à mutualiser au niveau régional un certain nombre d'infrastructures et services numériques à destination des collectivités (e-collectivité Vendée, Gigalis, ICP, etc..), des entreprises et des citoyens des Pays de la Loire. Cette mutualisation permet de positionner la Région des Pays de la Loire et ses territoires en position d'excellence dans le domaine de l'innovation numérique. Plus de 85 acteurs numériques sont mobilisés sur le territoire, au premier rang desquels ADN Ouest, un cluster majeur du numérique avec plus de 600 adhérents. Enfin, de nombreux tiers lieux sont conçus pour favoriser l'acculturation numérique ainsi que la sécurité numérique.

Dans ce contexte, **la Région des Pays de la Loire entend se mobiliser pour accueillir le campus de la cyber sécurité sur son territoire** en s'appuyant sur un écosystème engagé, une excellence scientifique incarnée par près de 300 chercheurs spécialisés en informatique et cybernétique, notamment en cybersécurité et intelligence artificielle, réunis au sein d'ATLANSTIC 2020 et un réseau de Technocampus.

La Région des Pays de la Loire est prête pour accueillir un campus de la cyber sécurité

Notre région dispose d'atouts incontestables pour accueillir un campus de la cyber sécurité : plus faible taux de chômage de France, un écosystème de l'innovation mature, des pôles de compétitivité, un IRT reconnu, des acteurs académiques (laboratoires de recherche, les enseignements supérieurs), l'expérience pour développer des filières émergentes et les animer de façon pérenne (Energies Marines Renouvelables, Hydrogène, ...)

La Région regroupe un écosystème industriel diversifié et pour lequel la Cybersécurité est indispensable. Le premier secteur employeur de la Région est **l'aéronautique** avec deux usines Airbus et de nombreux co-traitants. Avec la présence de Naval Group ou des Chantiers de l'Atlantique, la Région accueille les fleurons de **l'industrie navale et fluviale**. Thalès, basé à Cholet, Laval et Nantes, vient d'ouvrir une nouvelle ligne de production pour les radios « Contacts » de l'armée (contrat de plus d'un milliard d'euros) et regroupe des ressources significatives (300 experts en cyber sécurité). Le secteur **agricole et agro-alimentaire** est également très actif avec des coopératives telles LDC, Terrena ou des entreprises comme Sodebo ou Fleury Michon. Sur le plan de la **e-santé**, la métropole nantaise accueillera un QHU avec une attention particulière portée sur les données santé. **L'électronique et les objets connectés** sont également représentés avec des PME et ETI.
Enfin, la Région s'engage aux côtés de la French Fab à travers un plan pour l'Industrie du Futur et a réuni les acteurs de la Tech et de la Fab pour renforcer les effets de synergie entre ces communautés. Ces ETI, PME et PMI innovantes constituent un vivier industriel dynamique et diversifié. Les assureurs mutualistes viennent compléter ce paysage.

La Région Pays de la Loire se mobilise également au niveau européen. A cet égard, elle souhaite intégrer le réseau ECSO (European CyberSecurity Organisation) et suivra de près les appels à projets du programmes Horizon 2020 spécifiques sur ce sujet. En particulier, via son Bureau à Bruxelles, la Région étudie les opportunités offertes dans le cadre du programme PERS (Programme Européen de Recherche dans la Sécurité) et du futur cluster « Sécurité civile pour la société ». Enfin, **la Région est impliquée dans une démarche pour constituer un DIH - Digital Innovation Hub** - point d'entrée unique en région pour permettre aux entreprises d'avoir accès à tous les outils pour leur transformation numérique – tests, conseils, lien avec des experts – sur les grands défis que sont l'intelligence artificielle, les super calculateurs et la cybersécurité. L'Europe prévoit de co-financer ces DIH à hauteur de 50% dans le cadre du futur programme européen Digital Europe. Les acteurs régionaux ont pour le moment identifié la thématique IA comme la plus en lien avec l'écosystème, avec une attention qui devra également être portée sur la cybersécurité.

Enfin un réseau de Technocampus complète le paysage pour soutenir la montée en compétences de nos industriels.

Les Technocampus : des plateformes d'excellence au service de notre industrie

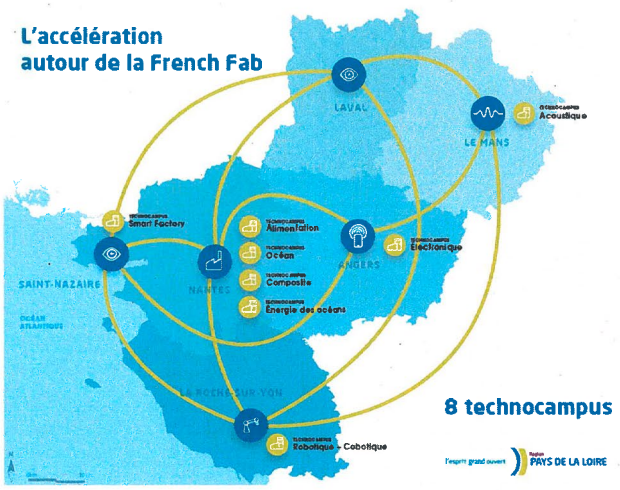
Pour accompagner les entreprises vers l'innovation, la Région a développé depuis 2008 - en partenariat avec l'Etat, les collectivités locales, les entreprises, les académiques et les acteurs de l'innovation - des Technocampus, plateformes d'excellence, maillant l'ensemble du territoire régional.

Un Technocampus est une plateforme technologique qui colocalise et fédère acteurs académiques et industriels (entreprises et centres techniques) pour mutualiser équipements et expertises. Chaque Technocampus est dédié à une thématique phare de l'Industrie du Futur avec une ambition de rayonnement national et international. Les Technocampus sont organisés, en réseau, pour créer des synergies entre chaque domaine d'innovation stratégique.

Quatre briques de services constituent le socle de ces plateformes :

- **Etudes industrielles** : préséries, études et essais pour concevoir un produit ou procédé avant son déploiement ;
- **Recherche & Développement** : preuves de concept, (valorisation, prototypage, démonstrateurs), mise en visibilité des expertises/ équipements académiques, alimentent les feuilles de route académiques à partir des besoins industriels ;
- **Formation** : offre de formations continues multi-acteurs, mise à disposition d'équipements pour des formations initiales ;
- **Animation** : services résidentiels, animation technologique et valorisation du pôle d'excellence.

Huit Technocampus couvrent un large spectre de domaines d'innovation.



Composite, Bouguenais, 2008
Smart Factory, St Nazaire, 2014
Océan, Bouguenais, 2015
Alimentation, Nantes, 2017
Electronique / IoT, Angers, 2019
Cobotique / Robotique, La Roche sur Yon, 2020
Réalité virtuelle / augmentée, Laval, 2020
Acoustique, Le Mans, 2022

3

Un programme « initiative Cyber Région » dévoilé en 2020

La Région a également consulté les acteurs économiques du territoire pour lancer un **programme « initiative Cyber Région »** dévoilé en 2020 autour de 6 axes :

- Sensibiliser et accompagner les entreprises à travers des dispositifs existants comme le diagnostic de Cybersécurité ou l'organisation d'ateliers experts.
- Accompagner la création d'entreprise sur notre territoire pour exploiter des brevets industriels sur des technologies de protection Cyber.
- Créer des fonds ligériens pour accompagner les secteurs stratégiques dans leur cyberdéfense (Bpifrance, Caisse des Dépôts, Banque du territoires, Cyber Angel...).
- Faire connaître, avec le secteur tertiaire, la gamme d'assurance pour les entreprises de notre territoire.
- Créer des formations spécifiques en cyber pour des techniciens et des ingénieurs qui viendront renforcer les équipes des entreprises ligériennes.
- Ajouter au réseau des Technocampus existants un référent cyber sécurité avec pour mission une montée en compétence en lien avec la thématique de son site.

Ce programme prendra appui sur une démarche ciblant les usages et les besoins des Ligériens pour développer des services « plus intelligents » et plus performants, dans un objectif d'intérêt général. Les habitants, les entreprises et les « start-up », les associations et la communauté académique seront associés à ce projet sur le principe de **l'innovation ouverte**, de manière à renforcer l'efficacité des actions et des décisions. Plusieurs dispositifs participatifs seront mis en place, dont **« Les rendez-vous Cyber Région »,** des programmes collaboratifs et une plateforme citoyenne ouverte à tous.

L'aménagement numérique du territoire n'a de sens que s'il permet le développement d'usages nouveaux, créateurs de valeur dans de très nombreux domaines tels que la santé, le transport, le nautisme... Mais la réussite du déploiement de ces nouveaux usages est étroitement corrélée à notre capacité collective à créer les conditions d'un environnement protégé.

Consciente des enjeux de sécurité et des risques sous-tendus par le numérique, la Région affiche sa volonté de lancer un Plan cybersécurité en 2020 pour investir dans la protection des données de ses citoyens et entreprises. L'accueil d'un campus de la cyber sécurité sur son territoire serait non seulement un gage de reconnaissance de son engagement dans ce domaine mais également un signal fort pour l'ensemble des acteurs de l'écosystème déjà investis sur ce champ.

Annexe 5 – Lettre du Président du Pôle d'Excellence Cyber

PÔLE D'EXCELLENCE CYBER

Rennes, le 18 décembre 2019

Monsieur le Directeur Général d'Orange Cyberdéfense

Cher Michel,

Les travaux de pré-configuration du Campus Cyber, auquel le Pôle d'Excellence Cyber, a été associé, ont permis de poser les bases du futur campus autour de la constitution d'un lieu de décloisonnement et de partage siège d'une réelle activité économique et implanté dans le bassin d'emploi francilien.

Les prolégomènes retenus sont identiques à ceux qui ont présidés à la constitution du Pôle d'Excellence Cyber.

La constitution d'une filière cyber demande d'articuler dans une approche commune recherche, formation et développement économique.

Cette articulation ne peut être réussie que si les univers constitués (recherche, formation, grands groupes, ETI, start-ups…), qui disposent chacun d'une sémantique et d'un modèle économique, sont décloisonnés.

Le Pôle d'Excellence Cyber a montré la voie de la création d'un éco-système désormais installé, générateur d'innovation, d'activités économiques pérennes et siège d'un bassin d'emploi de taille significative.

Cette création a été rendue possible notamment grâce au déploiement des initiatives des membres fondateurs le Ministère des Armées et la Région Bretagne autour de la plaque Rennaises et plus largement en Bretagne.

La force du modèle repose sur un axe majeur centré sur les cas d'usages de cyber défense. Cet axe majeur s'inscrit cependant dans l'affirmation de la dualité qui permet d'intégrer toutes les forces de l'éco système à l'image de la gestion des données sensibles et de les appliquer à d'autres cas d'usage à l'image de la santé.

1

Dans ce cadre, le projet de créer un lieu dédié au décloisonnement, l'institut cyber rejoint la préoccupation du Campus Cyber de disposer d'un outil concret et opérationnel d'échange et de travail entre les univers constitués.

Ainsi, l'institut implanté sur 3000 m² vise à regrouper un appareil de formation et de recherche ainsi que les instruments de transfert de technologie. L'institut s'adosse sur deux LABEX et accueille l'école universitaire de recherche en cyber sécurité à ce jour la seule labellisée en France.

Il complète un dispositif important où figure notamment la cyberschool de Rennes basée sur une approche interdisciplinaire combinant mathématiques, sciences et technologies numériques, sciences humaines et sciences sociales, l'accord général de partenariat dédié à la recherche et la cyber defense factory du ministère des Armées, structure d'appui à la création de start-ups.

Le Pôle d'Excellence Cyber, dont l'ambition est de bâtir une filière en cybersécurité-cyberdéfense souveraine ancrée en Bretagne et d'envergure nationale, contribuant au développement européen et rayonnant à l'international, doit, pour être cohérent avec sa stratégie, s'engager dans une étroite collaboration avec le Campus Cyber.

Cette volonté entre en résonance avec celle du Campus Cyber de créer une fédération des écosystèmes cyber du pays.

Les modalités de la collaboration au sein de cette fédération sont un des vecteurs essentiels de la réussite du Cyber Campus.

Le Pôle d'Excellence Cyber propose une première version des modalités de collaboration avec le Cyber campus :

- La création d'une fédération des écosystèmes cyber demande d'installer une gouvernance dédiée garante de la transversalité et de la complémentarité des initiatives des écosystèmes. Cette fédération est constituée pour garantir le maintien des particularités propres à chaque écosystème. Le Pôle propose que l'instance de gouvernance soit constituée de l'ANSSI, du campus cyber et de chacun des écosystèmes associés à la fédération. Une représentation, *ad hoc*, des ministères dans leur domaine de compétences respectifs permettrait d'adresser les freins législatifs ou réglementaires au développement de la fédération Cyber dans les domaines de la recherche, de la formation ou encore du développement industriel.
- Le Pôle propose d'apporter au sein du Campus Cyber l'écosystème cybersécurité et cyberdéfense déjà constitué, dans ce cadre il souhaite disposer d'un hébergement au sein du Campus Cyber et propose un hébergement au Campus Cyber au sein de l'institut Cyber à Rennes.
- La coopération opérationnelle avec le Campus cyber peut notamment être mise en œuvre par :
    - la mise en place d'un comité des projets en charge d'étudier l'opportunité de projets inter écosystèmes cyber et définir l'organisation des projets retenus,
    - la communication croisée des activités des écosystèmes cyber (Travaux, Offres des membres, …),

- la définition d'outils communs (base commune d'offre d'emploi, base commune de Threat Intelligence, outils commun de gestion de crise à destination de la communauté nationale…).

J'espère que ces propositions retiendront toute votre attention et que nos futurs travaux permettront de doter notre pays d'une organisation de la filière cyber apte à se confronter aux menaces de cyber et à apporter toute sa capacité au développement économique de la nation.

Dans l'attente, je vous prie de recevoir l'expression de mon amicale considération.

Le Président du Pôle d'Excellence Cyber

Philippe VERDIER

Annexe 6 – Synthèse des études pays

Une étude a été menée sur les initiatives visant à renforcer les synergies entre les experts publics, privés, et académique dans le domaine de la cybersécurité concernant 8 pays :

- **ALLEMAGNE**
- **CHINE**
- **ÉTATS-UNIS**
- **ISRAËL**
- **ROYAUME-UNI**
- **RUSSIE**
- **SINGAPOUR**
- **SUISSE**

Pour chacun des pays étudiés, la volonté de rassembler cette diversité d'acteur est apparue comme une évidence depuis ces dernières années, avec des formes et des moyens différents.

La diversité de ces initiatives renforce l'intuition française, tant des acteurs publics, privés et académiques du besoin de créer un lieu totem qui fédérera l'écosystème français et sera le symbole de l'excellence de l'écosystème en matière de sécurité et de confiance numériques.

Cette étude permet de comprendre que la sécurité numérique est devenue l'affaire de tous, que le modèle écosystémique est essentiel pour garantir un développement national à la hauteur des innovations internationales.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

ALLEMAGNE

Le marché allemand de la cybersécurité est en pleine croissance, malgré la faible sensibilité du secteur privé aux risques informatiques. Des initiatives sont prises pour stimuler l'innovation et les capacités opératoires dans la cybersécurité, en rapprochant les différents acteurs de ce milieu, mais aussi grâce à une étroite collaboration publique et privée avec Israël et les États-Unis.

Approche et principales initiatives lancées dans le domaine de la cybersécurité

Les politiques de cybersécurité de l'Allemagne reposent sur les initiatives fédérales, celles des Régions et, dans une moindre mesure, du secteur privé.

La stratégie de **l'État fédéral** est d'une part axée sur la défense et sur la sécurité économique, notamment industrielle, et d'autre part sur la sécurité des administrations fédérales.

Après la création en 2017 d'un Office central des technologies de l'information dans le secteur de la sécurité pour servir d'appui aux services de police, a été annoncée la création pour 2023 d'une Agence pour l'innovation disruptive dans la cybersécurité (ADIC). Avec un budget de 50 M EUR par an, elle regroupera une centaine de spécialistes chargés d'identifier les technologies critiques en matière de cybersécurité. Placée sous la tutelle du ministère de l'Intérieur, l'agence permettra le développement de la recherche scientifique et de l'innovation aux côtés du *Cyber Innovation Hub* créé par le ministère de la Défense en 2016 et le centre de cybersécurité de l'armée allemande à Munich.

Le *digital hub cybersecurity* de Darmstad, dédié à la cybersécurité, est l'un des douze hubs du programme fédéral *Digital Hub Germany*. C'est un lieu, un espace de *coworking* et un réseau qui facilite la mise en relation des start-up avec les acteurs de l'écosystème : financeurs, clients, ETI de la cybersécurité, pouvoirs publics, etc.

Le développement de la cybersécurité en Allemagne fait partie intégrante du programme « entreprise 4.0 », un cadre stratégique visant à moderniser (notamment numériquement) les entreprises allemandes, qui a connu un gain d'intérêt après les attaques cyber de ces dernières années.

Les besoins de l'administration fédérale (notamment du *Bundesamt für Sicherheit in der Informationstechnik*, homologue de l'ANSSI) représentent près de 50 % du CA du marché de la cybersécurité allemand.

Les régions allemandes sont également très actives. Dans l'enseignement supérieur, 70 universités ont une formation en matière de cybersécurité. À titre d'exemple du dynamisme régional, la Bavière va créer une université consacrée aux hautes technologies, dont celles utiles à la cybersécurité, qui devrait accueillir 10 000 étudiants. Fondé en 2006, le *Bavarian IT security and safety cluster* regroupe aujourd'hui 115 membres, universités, entreprises et collectivités territoriales et promeut la coopération entre ces derniers, notamment en matière de recherche et d'éducation, de soutien au développement des start-up.

Certaines initiatives regroupent **l'État fédéral, les Régions et le secteur privé**. Ainsi, en janvier dernier le fonds d'investissement *eCapital* a annoncé la création de son premier fonds dédié entièrement à la cybersécurité à hauteur de 50 M EUR. Il a pour but de soutenir les start-up qui innovent dans la cybersécurité, et est en partie financé par le fonds de placement fédéral *Sondervermögen*, et par la NRW Bank (banque du Land de Rhénanie-du-Nord-Westphalie).

En matière de coopération internationale, l'Allemagne cherche à bénéficier de technologies élaborées aux États-Unis (Darpa notamment) ou en Israël avant même leur commercialisation. À titre d'exemple, Deutsche Telekom travaille en étroite collaboration avec des étudiants israéliens du Cyber Spark et y a créé le premier centre de recherche et développement cyber hors d'Allemagne ; l'*Institut Fraunhofer* pour la sécurisation des technologies de l'information (une des universités allemandes de pointe en la matière) et le Centre de recherche en cybersécurité de l'Université hébraïque de l'École de Jérusalem pour les sciences informatiques et l'ingénierie, se rencontrent dans le cadre de l'*Hessian*[6] *Israeli Partnership Accelerator for Cybersecurity* (HIPA), forum spécialement consacré à la coopération israélo-germanique.

Toutefois, si la réussite de ces parcs industriels repose sur l'intégration et la mise en place de collaborations entre l'ensemble des parties prenantes de l'écosystème de la cybersécurité, il existe deux dynamiques concurrentes : d'une part la volonté de spécialisation des territoires à la faveur de ce type d'initiatives au sein des *länder* et de l'autre un objectif d'égalisation des territoires. Cette dernière vision explique l'implantation de l'ADIC dans une autre région que les centres de recherche avec lesquels elle doit coopérer, au détriment de la centralisation des compétences en un même lieu.

Trois obstacles semblent susceptibles d'entraver les efforts allemands : la faible conscience des risques dans le secteur privé, l'opposition des Verts (*Die Grünen*) aux initiatives de cybersécurité et enfin la contrainte budgétaire portée par le *Schwarze null* qui interdit à l'Allemagne les 0,35 % de déficit structurel et pourrait empêcher les investissements nécessaires.

6 La Hesse est le *Land* (région) de Francfort, région disposant des plus importantes infrastructures numériques allemandes, en particulier en raison de la présence des banques allemandes et des interconnexions internet les plus rapides au monde.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

CHINE

Dès l'arrivée au pouvoir de Xi Jinping, en 2012, la sécurité de l'information et du cyberespace a été instituée au rang de priorité nationale. La cybersécurité fait l'objet d'une promotion nationale importante à l'égard du grand public et des entreprises. Différentes mesures d'initiatives gouvernementales sont concomitamment mises en place afin de renforcer le niveau de compétence sur l'ensemble du territoire, l'émancipation du pays des technologies étrangères et la présence des entreprises chinoises à l'international.

I / La cybersécurité, priorité nationale des dirigeants chinois

En février 2014, un « leading small group sur la cybersécurité et l'informatisation » dirigé par Xi Jinping en personne a tenu sa première réunion à Pékin. Ce *leading small group* s'est transformé en « Commission » à la faveur de la réorganisation administrative intervenue en mars 2018. Toujours dirigée par Xi Jinping, cette commission réunit également le Premier ministre et plusieurs ministères (sécurité publique, industrie, sciences et technologies, affaires étrangères, commission centrale militaire) en vue de définir les orientations générales de la politique à tenir en la matière. Le 1er juin 2017, une Loi sur la cybersécurité est en outre entrée en vigueur. Elle impose de fortes obligations à tout « opérateur de réseau », dont les entreprises.

Depuis 2014, la cybersécurité fait l'objet d'un effort de promotion nationale à l'égard du grand public dans le cadre de la *Cybersecurity week* organisée annuellement au mois de septembre (à Tianjin en 2019, Chengdu en 2018, Shanghai en 2017, etc.).

La prévention des risques cyber fait également l'objet d'une promotion auprès des entreprises chinoises. Une « commission de promotion de la cybersécurité » a ainsi été créée en 2016, sous l'égide du ministère de l'Industrie et des technologies de l'information (MIIT). Cette commission est rattachée au « C entre pour le développement de l'industrie de la sécurité de l'information » du ministère avec pour mission : participer à l'élaboration des lois et de la règlementation touchant les entreprises du secteur ; promouvoir les technologies et produits de sécurité informatique ; stimuler les entreprises afin qu'elles sécurisent davantage leurs systèmes et leurs infrastructures informatiques ; réaliser des audits réguliers des entreprises, etc.

II / La formation de compétences, facteur clé de la souveraineté technologique chinoise en matière de cybersécurité

En 2018, d'après la *China Academy of Information and Communications Technology* (CAICT), le marché chinois de la cybersécurité était estimé à 6,6 Mds EUR, en croissance de 19,2 %, et pourrait avoir atteint 8,3 Mds EUR en 2019. Les autorités publiques sont à l'initiative des principales actions entreprises dans le domaine de la cybersécurité. Les principales entreprises du secteur sont privées (plus de 3000), mais la Chine souffre d'un manque de talents de haut niveau pour répondre aux besoins actuels en matière de recherche et d'innovations. Le déficit serait compris entre 700 000 et 1,4 million de personnes pour atteindre la souveraineté technologique dans le secteur.

Pour combler ce déficit, Xi Jinping a appelé en 2016, au cours d'une conférence organisée par la *Cyberspace Administration of China* (CAC), à « créer des académies d'excellence dans le domaine de la cybersécurité ». D'ici 2027, 11 universités devraient avoir acquis une influence internationale dans le domaine.

Ces universités ont 8 missions :

- créer des cursus spécialisés, identifier des élèves susceptibles d'être recrutés en master et envisager la création de cours de spécialité ainsi que de classes pour jeunes élèves ;
- élargir le panel de recrutement des élèves et mettre en place des cursus interdisciplinaires (physique, biologie, droit, management, etc.) ;
- établir des centres de recherche en cybersécurité en partenariat avec des entreprises ou des organismes de recherche et y conduire des recherches sur les thématiques définies par le gouvernement central ;
- mettre en œuvre des mesures afin d'attirer des personnalités ayant des connaissances et une expertise à officier en tant que professeur ; l'emploi à temps partiel d'experts et de hauts talents est encouragé ;
- organiser des détachements de professeurs au sein d'entreprises internet ou informatiques, des organismes de recherche ou des « organes étatiques » ; la coopération avec les entreprises doit être renforcée aussi bien sur le plan de la formation des talents, que des cursus proposés, des matériaux d'enseignement utilisés que des thématiques de recherche, etc. ;
- encourager les étudiants à rejoindre ou créer des start-up durant leur cursus ;
- activement développer les coopérations avec les universités, entreprises et organismes de recherche étrangers spécialisés dans le domaine de la cybersécurité. Attirer les « talents » étrangers de très haut niveau ; encourager les jeunes professeurs à étudier ou réaliser des formations à l'étranger et à participer aux « évènements d'échanges techniques » internationaux ;

- mettre en place un système d'évaluation des talents qui ne repose pas uniquement sur les résultats académiques de la personne mais prenne prioritairement en compte ses « capacités réelles » (expertise, innovation, applications pratiques).

Même si ces initiatives demeurent récentes — fin 2017 pour les académies —, les efforts portés en matière de formation semblent déjà à porter leurs fruits (en 2018, +17,7 % d'inscrits en licence et +44,4 % d'inscrits en master), avec un nombre de dépôts de brevets qui suit la même trajectoire de croissance. Ces initiatives sont en outre complétées par celles du secteur privé, comme celle du leader chinois du secteur, Qihoo 360, qui, en 2017, à Pékin a créé sa propre académie (avec des antennes à Jinan, Nankin, Xiamen, Zhengzhou, Wuhan, Xi'an et Chengdu) avec l'objectif de former 10 000 individus chaque année.

III / Les parcs industriels, soutien à la politique publique de cybersécurité

Plusieurs parcs industriels de rang national sont en cours de construction dans le pays depuis 2018. Parmi ceux référencés dans le « livre blanc » de la CAICT :

- **À Pékin**, le parc industriel « sécurité des réseaux » : inauguré en janvier 2019, il s'agit d'un parc de rang national pour lequel une trentaine d'entreprises ont manifesté leur intention de s'y installer ;

- **À Tianjin** — Binhai, *Binhai Information Security Industry Park* : inauguré en 2014. A vocation opérationnelle, le parc regroupe déjà l'alliance des entreprises anti-logiciels malveillants, l'alliance pour une informatique de confiance, l'alliance internationale pour la sécurité du *cloud*, l'alliance de l'industrie de la sécurité informatique, le centre national des réponses d'urgence en cas d'infection informatique, le centre d'inspection des produits antivirus du ministère de la Sécurité publique, le centre de recherche national des technologies de lutte contre les virus informatiques.

Ce parc possède une forte dimension « civilo-militaire » avec la présence, sur place, du centre de recherche pour l'innovation dans le cadre de l'intégration civilo-militaire ; projet de microprocesseur « Tengfei » de la *National University of Defense Technology* et de système d'exploitation « Kylin » développé par la même université, etc. Fin septembre 2019, treize nouvelles entreprises ont manifesté leur intention de s'y installer.

- **À Wuhan**, une base nationale d'innovation et des talents « sécurité des réseaux et de l'information ». Fin septembre 2018, 75 entreprises y étaient déjà installées — dont la française Atos — et 41 autres avaient manifesté l'intention de s'y relocaliser ;

D'autres parcs spécialisés ont également été inaugurés à Hechuan (Chongqing) et Chengdu (autour de l'entreprise publique CETC, conglomérat public lié à l'Armée de libération populaire), entre autres.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

ÉTATS-UNIS

En 2018, les États-Unis sont classés au 1er rang mondial en termes de capacité d'innovation et de collaboration par The Global Competitiveness Report. Il existe dans le pays une véritable culture de la recherche partenariale publique-privée et de l'innovation avec, au cœur, les universités. Au-delà d'instituts de recherche spécialisés dans la cybersécurité et la très réputée Silicon Valley, le Cyber NYC démontre le besoin de créer un lieu à vocation internationale qui permette de développer les synergies entre l'ensemble des acteurs de l'écosystème.

I / Les États-Unis, garants « par la force » de la sécurité du numérique

En septembre 2018, la Maison-Blanche publie la *National Cyber Strategy* à travers laquelle elle promeut un internet ouvert et la libre circulation des données au niveau international. Dans ce document, il a affirmé que les Etats-Unis « created the Internet and shared it with the world » et ont vocations à « assurer la paix par la force » dans le cybersespace.

Le document estime que le « protectionnisme digital » (les régulations restreignant la libre circulation des données) affecte négativement la compétitivité des entreprises américaines. Pour sécuriser cet écosystème, la Maison-Blanche estime nécessaire d'investir dans des infrastructures de communications, en mentionnant le développement de la 5G et l'utilisation de technologies émergentes comme l'informatique quantique et l'intelligence artificielle. Enfin, elle souhaite améliorer le recrutement et les compétences liés à la cybersécurité, pour s'assurer de la compétitivité du secteur des technologies.

Comme dans d'autres domaines économiques, l'Administration Trump a initialement considéré la cybersécurité comme l'opportunité de constituer un secteur d'activité d'excellence et susceptible d'exporter. Dans l'*Executive Order* 13800 de 2017 — la première orientation donnée par l'Administration Trump en la matière —, l'exécutif affirme que le développement de mécanismes de cybersécurité repose largement sur l'investissement des entreprises et non sur des fonds fédéraux. Elles sont présentées comme les mieux placées pour lutter contre les risques spécifiques, alors que le gouvernement serait plus à même d'investir dans des domaines plus fondamentaux. Dans la vision du *Council of Economic Advisers* (CEA), le développement d'un secteur d'activités concentrant des entreprises dédiées à la cybersécurité permettra aux autres entreprises américaines d'externaliser les tâches de cybersécurité.

Toutefois, l'agenda relatif à la cybersécurité est pour l'instant en retrait des ambitions affichées en 2017. Ainsi, le secteur privé a dénoncé les exigences posées par les agences fédérales américaines, notamment en ce qui concerne la mise en place de « backdoors » par le FBI, la CIA ou le NSA.

II / Le partenariat universités-entreprises, soutenu par l'État fédéral, facteur clé de succès de l'écosystème américain

Dans le secteur de la cybersécurité, il est difficile d'établir un modèle des relations entre initiatives regroupant à la fois le secteur académique, public et privé. On peut distinguer toutefois plusieurs partenariats ou relations bilatérales : le soutien fédéral aux universités « expertes » ou « d'excellence » dans la cybersécurité ; l'établissement d'un institut de recherche spécialisé, géré par le MITRE, organisme indépendant ; la multiplication des partenariats entre les grandes entreprises de la Tech avec les universités américaines.

- Les universités à l'initiative de centres de recherche sont soutenues par l'administration fédérale.

En 1999, la *National Security Agency* (NSA) et le *Department of Homeland Security* (DHS) lancent la labellisation « Center of Academic Excellence », dans le domaine de la cybersécurité (CAE-IAE) qu'elle attribue initialement à sept universités. Par ailleurs, la NSA a lancé un programme « National Centers of Academic Excellence in Cyber Operations » (CAE-CO), pour les professionnels. Le DHS et la NSA sponsorisent aujourd'hui plusieurs centaines de « colleges » et 48 universités sur le territoire américain.

L'Université de Northeastern a par exemple été désignée comme « centre d'excellence académique », notamment pour son centre de recherche « Cybersecurity and Privacy Institute de la Northeastern University ». Ce dernier collabore avec un réseau d'universités américaines ou étrangères, mais également des entreprises privées (Akamai, Airbus Group Innovaiton, AT&T, Google, IBM Research, Microsoft Research, Toyota, etc.) ainsi qu'avec le gouvernement américain (DHS, NSA) ou la Commission Européenne.

- En 2012, le *National Institute of Standards and Technology* (NIST) créé un *National Cybersecurity Center of Excellence* (NCCoE) au sein de l'Université du Maryland. Le centre de recherche, le Maryland Cybersecurity Center (MC2), établit des liens entre plusieurs partenaires privés et réunit par ailleurs des experts gouvernementaux et des universitaires. En février 2013, le Président Barack Obama publie un décret présidentiel, « Improving Critical Infrastructure Cybersecurity », qui missionne le NIST d'établir un cadre pour la cybersécurité afin que les entreprises et organisations puissent évaluer et réduire les risques. Le NIST a publié le *Framework for Improving Critical Infrastructure Cybersecurity* en février 2014.

- Les initiatives des grandes entreprises technologiques pour développer des partenariats universitaires. On peut citer l'exemple de Facebook, qui a lancé, en partenariat avec les uni-

versités, le Facebook Cyber Security University Program, qui vise à former les étudiants des grandes universités américaines. L'entreprise soutient une dizaine d'universités. Grâce à ses financements la Texas A&M University a pu construire un centre de recherche, le *Center for Information Technology and Cyber Security*, pour un montant de 63 M USD. Le programme réunit des experts de Facebook, qui permet ensuite aux étudiants de continuer leurs études dans le domaine en offrant des bourses, ainsi que des stages dans l'entreprise.

Par ailleurs, en 2017, Facebook a lancé ce même programme à destination des vétérans de l'armée américaine, Facebook Cybersecurity University for Veterans.

III / Le Cyber NYC, une initiative innovante pour conforter le leadership des entreprises américaines du secteur

La création du Cyber NYC, lancée en 2018 par la ville de New York, se démarque de ces précédentes initiatives. Il s'agit pour New York de devenir le centre international de l'innovation en matière de cybersécurité avec un investissement public-privé de 100 M USD et la mise en place d'un lieu fédérateur situé au cœur de Manhattan, au plus près de l'écosystème de la cybersécurité. Le Cyber NYC est dédié à l'innovation, avec un incubateur et un accélérateur développés en partenariat avec le fonds de capital-risque Jerusalem Venture Partners (JVP), mais aussi le développement de la formation, la mise en place d'un showroom, l'organisation challenges et d'évènements internationaux, etc.

Le Cyber NYC s'inscrit dans la dynamique internationale de création de lieux dédiés aux questions de cybersécurité, à l'image du modèle israélien. La *New York City Economic Development Corporation* (NYCEDC) qui est à l'initiative de ce projet souhaite faire de ce lieu un espace ouvert aux start-up qui pourront bénéficier de cette vitrine internationale, et du développement de l'excellence américaine en matière de cybersécurité avec 5 écoles et universités de la ville.

Ce *hub* d'innovation est créé en partenariat avec SOSA, entreprise qui, comme à Tel-Aviv ou à Londres, est spécialisée dans le développement des écosystèmes internationaux de la Tech et de leurs stratégies d'innovation. D'une manière globale aux États-Unis, les acteurs privés et les universités constituent la pierre angulaire de la politique d'innovation en matière de cybersécurité. Le Cyber NYC concrétise le besoin de rassembler physiquement l'ensemble des acteurs de l'écosystème et de catalyser sa capacité d'innovation.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

ISRAËL

Dans un contexte où Israël fait face quotidiennement à des centaines de cyber-attaques, l'approche israélienne du cyberespace est à la fois défensive et offensive ainsi qu'holistique et flexible, la frontière entre les mondes civil et militaire étant poreuse. La politique volontariste du gouvernement, couplée à l'éducation (exposition à la technologie dès l'enfance) ainsi qu'aux dispositions culturelles, sociales (valorisation de la prise de risque, hiérarchie non rigide…) et géographiques (superficie inférieure à celle de la Région Bretagne facilitant les expérimentations) constituent, entre autres, les facteurs clés du positionnement de leader occupé par Israël dans cette industrie.

I / Depuis les années 1990, l'État a accompagné le développement du secteur, devenu un enjeu économique autant que de sécurité.

Par le soutien au capital-risque puis par la consolidation d'un paysage institutionnel qui n'a cessé d'évoluer depuis 2011, date à laquelle la cyberdéfense a été érigée en priorité nationale par le gouvernement, l'objectif des autorités a été de positionner Israël parmi les 5 puissances du cyberespace. Aujourd'hui, les politiques publiques dans le domaine de la cybersécurité sont mises en œuvre par l'*Israel National Cyber Directorate* (INCD), créé en 2018 et placé sous l'autorité du Bureau du Premier ministre. L'INCD fédère ainsi les acteurs civils de la sécurité du numérique – administrations gouvernementales, entreprises, incubateurs, milieu académique – qui ont désormais un interlocuteur unique et central et joue aussi un rôle d'interface entre le civil et le militaire.

Cette politique volontariste a contribué à faire d'Israël une référence mondiale en matière de cyber- sécurité. Avec ses 450 entreprises actives et ses flux d'exportations de cyber-solutions supérieures à 5 Mds USD par an (soit le 2e exportateur mondial), la cybersécurité israélienne est performante et attractive et attire 20 % des investissements mondiaux du secteur. Néanmoins, cette politique incitative et résolument tournée vers l'international emporte une fragilité pour ce modèle qui dépend principalement de ces financements étrangers.

II / Le Cyber Spark de Beer Sheva concentre les acteurs clés (public, privé, académique, armée) de l'écosystème et constitue une vitrine pour Israël

Le campus Cyber Spark à Beer Sheva a pour vocation de devenir un pôle d'expertise de cybersécurité mondial. Le Premier ministre, Benjamin Netanyahou, a fait le choix de promouvoir Beer Sheva en tant que « cyber-capitale » avec pour objectif de désenclaver cette région du Néguev. Annoncé en 2014 et progressivement opérationnel depuis, le Cyber Spark réunit sur un même site, le CERT (Computer Emergency Response Team, rattaché à l'INCD), l'incubateur du fonds JVP, les entreprises (de la start-up à la multinationale), ainsi que le secteur de la défense (à terme). Ce campus s'adresse aussi bien aux Israéliens qu'aux étrangers.

S'il s'agit d'un « échantillon » (3 bâtiments étant opérationnels sur les 15 prévus), les incitations financières pour attirer les meilleurs chercheurs et ingénieurs sont à la hauteur des ambitions de créer 30 000 emplois à Beer Sheva au cours des 10 prochaines années (contre 3 000 actuellement).

Le Cyber Spark se veut opérationnel et répond à une notion de court terme avec la recherche de solutions opérationnelles disponibles rapidement. Le partage de connaissances et la mise en relations y sont mis en valeur.

La *Cyber Spark Industry Initiative* est une organisation à but non lucratif désignée pour être la structure centrale de coordination des activités cyber du site. L'INCD, la municipalité de Beer Sheva, l'Université Ben Gourion et les entreprises en sont membres.

Les facteurs clés de succès du Cyber Spark sont le prix de l'immobilier, les incitations financières du gouvernement (une subvention des salaires pour les entreprises s'installant dans la zone) et le vivier de jeunes diplômés de l'Université Ben Gourion.

Toutefois, comme l'ont confirmé les échanges avec les acteurs du secteur ayant eu lieu lors d'une réunion à l'ambassade, Beer Sheva semble néanmoins être moins attractif que Tel-Aviv ou Herzliya aux yeux des entreprises plus matures qui y constatent la difficulté à attirer les talents les plus confirmés, un déficit de proximité avec leurs clients, les financiers ou encore les fonctions supports (conseil, juridique, marketing).

En dehors du Cyber Spark de Beer-Sheva, certaines initiatives sont inspirantes à l'instar de l'incubateur Team8 qui figure parmi les plus réputés au monde ou encore le consortium public-privé dénommé IC3 qui regroupe multinationales israéliennes et start-up.

Une des principales volontés des « jeunes pousses » semble être de réussir leur « exit » en vendant à de grands groupes étrangers, ce qui peut freiner l'émergence d'une industrie de la cybersécurité plus « robuste ».

III / Le capital humain constitue le pilier du secteur, dans un contexte de déficit d'experts à l'échelle mondiale et auquel Israël doit aussi faire face

L'armée joue un rôle stratégique dans la formation d'experts, grâce au service militaire obligatoire (3 ans pour les hommes, 2 ans pour les femmes) et des programmes de formation spécifiques (*Talpiot* ou encore *Havatzalot*). Les cyber-compétences sont aussi développées dès le plus jeune âge, les programmes dédiés hors du cursus académique se multipliant à l'instar des *coding bootcamps*, des cours de codage et autres hackatons.

Les ONG, telles qu'Appleseeds avec Net@ou encore la *Rashi Foundation* avec le programme *Magshimim*, contribuent à mettre l'accent sur l'*inclusive innovation* qui consiste en la montée en compétences de populations peu intégrées au sein de l'écosystème *high tech* avec pour objectif de relancer la cohésion sociale. Ces programmes, soutenus par les autorités (ministère de l'Éducation, de l'Économie, de la Défense ou encore l'INCD), reposent tous sur l'idée de proposer un enseignement technique de haute qualité et exploitable rapidement par les industriels et les militaires.

Cependant, si les milieux civil et militaire sont liés, certains experts et organisations sont réticents à l'idée de travailler avec des compagnies israéliennes notamment au vu de leurs liens avec le gouvernement et les services de renseignement. Dans ce contexte, il n'est pas rare de voir des compagnies israéliennes déplacer leur siège en dehors du pays tout en maintenant leur R&D en Israël.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

ROYAUME-UNI

Le marché britannique de la cybersécurité est considéré comme le plus important d'Europe. Un nombre important d'initiatives publiques participent à renforcer ce domaine en matière de sensibilisation des entreprises, de promotion des carrières et de facilitation de collaborations entre le secteur public et le secteur privé. Éléments clés de la National Cyber Security Strategy 2016 to 2021, la coopération public-privé a permis la création de la Tech City à Londres.

I / L'initiative publique à l'origine de l'efficacité du Royaume-Uni en matière de cybersécurité

En 2016, le gouvernement britannique a publié sa deuxième stratégie quinquennale en matière de cybersécurité (*National Cyber Security Strategy 2016 to 2021*). Il y figure clairement que la coopération entre les secteurs public et privé est clé pour lutter efficacement contre la cybercriminalité. Le document est en phase avec la stratégie nationale de sécurité de 2015 (*National Security Strategy*) qui annonçait un investissement de 1,9mds£ dans le programme national de cybersécurité (National Cyber Security Programme) afin de promouvoir le développement des compétences, connaissances et capacités du Royaume-Uni en la matière.

Les autorités publiques, dont le GHCQ et le *National Cyber Security Centre* (NCSC), rattachés au Premier ministre, sont un soutien essentiel aux différentes initiatives lancées dans ce domaine éminemment stratégique. Outre les orientations stratégiques, elles apportent un soutien financier, technique, à l'export, pour la formation de talents, mais aussi pour la coordination des efforts et des ressources. 16 programmes et projets mêlant acteurs publics et acteurs privés de la cybersécurité ont été lancés ces dernières années. Tant les activités de recherche, que d'innovation, d'accélération, de formation ou encore de partage d'informations face aux risques cyber sont appréhendés.

Ces programmes, dont la plupart sont financés par le DCMS (*Department for Digital, Culture, Media & Sport*) concernent l'ensemble du champ de la cybersécurité (sécurité des systèmes d'information, lutte contre la cybercriminalité et la cyberdéfense).

À titre d'exemples, il est possible de citer les programmes suivants :

- **le Cyber Security Information Sharing Partnership** (CSIP) : partenariat lancé en 2013 par le gouvernement avec le secteur privé pour faciliter le partage d'informations en temps réel sur les cybermenaces. Concrètement, le CSIP est une plateforme en ligne qui permet à ses 4020 membres d'échanger des informations en temps réel dans un environnement sécurisé et confidentiel ;

- **le programme Active Cyber Defence** (ACD) : déployé pour la première fois en 2016, il avait alors pour objectif d'empêcher l'utilisation frauduleuse des réseaux et des marques du gouvernement britannique pour tromper les utilisateurs de services gouvernementaux. Les technologies de l'ACD, développées par le NCSC, servent désormais à identifier et bloquer les escroqueries en ligne dont sont victimes les entreprises privées et la société civile ;

- **Industry 100** est une initiative du NCSC lancée en 2017 pour intégrer à ses équipes des experts du secteur privé, détachés pour des stages de courte durée. Les volontaires au programme sont payés par leur entreprise. En contrepartie, Industry 100 permet aux grands groupes d'élargir leur réseau d'experts, de tisser des liens avec la NCSC et de promouvoir leur engagement en matière de cybersécurité ;

- **Cyber 101** a permis la mise en place de centres spécialisés par secteurs qui ont vocation à promouvoir la recherche et le développement en connectant les entreprises avec les chercheurs et universitaires britanniques ;

- **Cyber UK** est l'évènement phare en matière de cybersécurité au Royaume-Uni. Il est organisé tous les ans par le NCSC afin de faciliter les interactions entre les secteurs public et privé ;

- **Exercise in a Box** est un outil en ligne gratuit développé par le NCSC dans le cadre du programme Active Cyber Defence pour aider les organisations publiques, privées et civiles à tester leur résilience aux cyberattaques. Cela consiste concrètement en une série d'exercices qui plonge ses utilisateurs dans des scénarios de cybermenaces et évalue leur état de préparation et leurs réactions. Les participants reçoivent un rapport d'évaluation personnalisé.

II / Une initiative privée opportuniste associant acteurs publics et privés : le LORCA, campus londonien orienté entreprises et marchés

Le *London Office for Rapid Cybersecurity Advancement* (LORCA) a ouvert au sein du *Queen Elizabeth Olympic Park* à Londres, à la fois à proximité du siège du NCSC et à proximité du hub technologique de l'Est londonien. LORCA occupe les locaux initialement construits pour accueillir l'espace presse des Jeux olympiques de 2012.

À l'origine du projet, la société de promotion immobilière Delancey a candidaté à un appel d'offres de la ville de Londres. Ils ont obtenu un bail de 200 ans pour y installer leur filiale Here East, campus d'innovation créé en 2014. En 2017, Here East a créé Plexal, un incubateur qui accueille des start-up et des entités publiques de tous secteurs. Plexal se rémunère de trois façons différentes : en

louant des espaces de coworking pour des entreprises de 1 à 40 employés, en organisant et en accueillant des évènements au sein de sa structure et en mettant à disposition des entreprises son équipe d'experts en innovation.

Le DCMS a lancé un appel d'offres pour la création d'un cyber accélérateur à Londres. Plexal, en association avec Deloitte et la Queen's University de Belfast, a remporté l'appel d'offres et créé LORCA, en 2018, avec un budget de 13,5 M£ sur trois ans. Dans leur contrat avec le gouvernement, LORCA s'est engagé à accompagner 72 entreprises sur trois ans, à les aider à lever 40 M£ et à créer 500 emplois directs et 1500 emplois indirects à plus long terme.

Au quotidien, six personnes travaillent à plein temps pour LORCA. LORCA bénéficie également de l'aide d'un Industry Advisory Board (IAB), présidé par un directeur du GCHQ. L'IAB est constitué d'influenceurs internationaux dans les domaines de la technologie et de la cybersécurité.

L'Innovation Forum rassemble quant à lui des entreprises de différents secteurs. Il définit les grandes priorités de chaque promotion de LORCA et participe à la sélection des start-up qu'il accompagne tout le long du programme. Des fonds en capital-risque, private equity ainsi que des business angels font partie du Finance Forum.

Les entreprises accélérées peuvent bénéficier de :

- un an d'incubation dans les locaux de LORCA et de six mois d'accélération ;
- un accompagnement technique, juridique et commercial. Elles reçoivent également des informations sur l'écosystème pour adapter leur offre à la demande du marché ;
- un accès à un réseau d'investisseurs et à une journée de démonstration annuelle pour présenter son entreprise à un parterre d'investisseurs et partenaires potentiels ;
- au travers du *Global EPIC* (Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity), accès à un réseau international de potentiels partenaires commerciaux et investisseurs. Chaque entreprise a aussi l'opportunité de voyager à l'étranger se préparer au lancement de leurs solutions en dehors du Royaume-Uni.

Les start-up qui souhaitent participer au projet doivent candidater au sein d'une des catégories choisies chaque année. Ces catégories permettent un alignement stratégique de la demande et de l'offre du marché de la cybersécurité, phénomène renforcé par la proximité des grands groupes et des start-up lors de l'exécution du programme. Les entreprises accélérées par LORCA sont relativement matures dans la mesure où elles sont déjà dans une phase de commercialisation.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

RUSSIE

Si la Russie dispose de champions dans le secteur de la cybersécurité, en particulier Kaspersky, le marché national reste modeste. Ceci s'explique par le relatif retard du pays en matière de numérisation des entreprises et des administrations. Conscient de cet état de fait, les pouvoirs publics ont lancé des initiatives fortes en faveur de la transition numérique, qui comprennent des volets cybersécurité et un cadre règlementaire renouvelé. Le parc technologique de Skolkovo situé en périphérie de Moscou, que l'on présente également comme la « Silicon Valley russe » est le symbole de la volonté russe d'affirmer son positionnement parmi les puissances internationales du numérique.

I / L'économie numérique fait l'objet d'une attention particulière de la part du gouvernement russe, soucieux de préserver le développement d'un écosystème national.

Le développement de l'internet russe est porté à la fois par la taille du marché domestique (87 millions d'internautes, soit 71 % de la population) et le développement d'un écosystème propre, le « Ru.net ». Celui-ci repose sur des entreprises privées russes de plus en plus nombreuses (Yandex, Ozon, Mail.ru, Wildberries, Avito, Vkontakte, etc.), qui se sont développées à l'abri des *GAFAM*. Les autorités russes considèrent ainsi avoir réussi à protéger leurs plateformes numériques nationales face aux géants américains et chinois, objectif stratégique à leurs yeux pour des raisons économiques et sécuritaires.

Les documents stratégiques publiés par la Russie dans le domaine du numérique font une place importante aux questions de « souveraineté technologique ». Si l'industrie russe n'est pas à ce stade en mesure d'être compétitive face à la concurrence américaine, les autorités poursuivent néanmoins une politique industrielle volontariste en la matière. Ainsi, dans le domaine des processeurs, la Russie cherche à réduire sa dépendance vis-à-vis du duopole américain Intel/AMD, avec les gammes de processeurs Baikal et Elbrus.

Pour autant, l'économie et la société russes sont relativement peu numérisées, ce qui constitue un frein au développement du secteur de la cybersécurité. L'État russe a donc lancé, en 2010, un programme « économie numérique » afin de rattraper ce retard. Sur la période 2018-2024, 22,7 Mds EUR ont été consacrés à des projets fédéraux de transition numérique, en particulier pour l'industrie 4.0, et 419 M EUR pour la « Sécurité de l'information » afin d'augmenter la proportion de logiciels et de produits domestiques selon une stratégie de « souveraineté technologique ».

II / La Fondation Skolkovo est chargée de servir de catalyseur à la diversification de l'économie russe

Le 28 septembre 2010, le président Dmitri Medvedev promulgue la loi « Sur le centre d'innovation de Skolkovo », donnant ainsi naissance à l'entité gestionnaire du projet, la « Fondation Skolkovo » (fondation à but non lucratif).

Chargée de servir de catalyseur à la diversification de l'économie russe, la Fondation Skolkovo a pour objectif principal de créer un écosystème durable d'entrepreneuriat et d'innovation, de créer une culture de jeunes pousses et d'encourager le capital-risque. Skolkovo regroupe différentes structures : un centre d'innovation, un Technoparc, un institut de technologie de pointe (*Skoltech*) et une nouvelle université. Parmi les domaines à fort potentiel de croissance identifiés, les technologies informatiques stratégiques, et notamment la cybersécurité, apparaissent en bonne place aux côtés de l'énergie, la biomédecine, le nucléaire et le spatial.

Trente des sociétés les plus performantes au monde, parmi lesquelles Boeing, Cisco Systems, EADS, GE, Johnson & Johnson, IBM, Intel, Microsoft, Siemens, Nokia, Samsung, etc., ont signé des accords de partenariat de recherche et développement avec la Fondation Skolkovo. Les entreprises Dassault systems, Orange, Schneider Elecric et les Laboratoires Servier sont installés sur le parc ou travaillent avec les équipes de Skolkovo.

Skolkovo démontre que la création d'un « campus » qui regroupe les chercheurs, les grandes entreprises, les PME innovantes et les start-up permet de générer des économies d'agglomération et permet aux participants de bénéficier d'infrastructures de haute qualité, avec une dynamique d'émulation collective. Le parc Skolkovo aurait permis d'attirer 10 Mds USD d'investissements dont 70 % d'origine privée.

L'initiative répond également au besoin en ressources humaines avec la mise en place de formations d'excellence d'une part au sein de l'Institut de technologie de Skolkovo et d'autre part au sein de l'université de recherche de Skolkovo, couplée au MIT (*Massachusetts Institute of Technology*), mais également avec des travaux académiques en partenariat direct avec les entreprises. La Russie entend ainsi adapter son développement aux nouveaux usages et technologies (ex. : *IoT*, *Cloud*, quantique, etc.). Toutefois, les sanctions économiques imposées par l'Union européenne et les États-Unis à partir de 2014 ont eu un impact important sur la capacité de la Fondation à inviter des scientifiques, ou à amener des spécialistes et des entreprises étrangères à rejoindre des projets.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

SINGAPOUR

Plateforme commerciale, financière et juridique pour l'Asie, la cité-État de Singapour se positionne logiquement comme l'un de ses principaux hubs numériques. Près de 40 000 entreprises internationales (dont 7 000 multinationales) y ont établi leur siège, et côtoient les grandes entreprises singapouriennes, dont en particulier Singtel, deuxième opérateur téléphonique asiatique, et ST Engineering, entreprise de technologie, ingénierie et défense, ainsi que 4 300 start-up présentes dans l'écosystème. En matière d'infrastructures, Singapour est reliée aux autres continents par 17 câbles sous-marins, dispose de connexions rapides et de bonne qualité et héberge un tiers des serveurs de données d'Asie du Sud-Est.

I / Les autorités publiques ont été très proactives pour développer l'écosystème de cybersécurité à Singapour et peuvent s'appuyer sur des moyens considérables

Les autorités singapouriennes ont élaboré dès 2016 une stratégie nationale en matière de cybersécurité, suivie par l'adoption d'un cadre règlementaire en mars 2018 (ce qui n'a pas empêché une attaque informatique massive sur des données de santé en juin-juillet 2018, dont celles du Premier ministre).

Le développement d'un écosystème dynamique est l'un des grands piliers de la stratégie nationale. Trois approches ont été privilégiées :

- développer les parcours professionnels ;
- encourager l'entrepreneuriat et attirer les meilleures entreprises étrangères ;
- stimuler l'innovation.

À titre d'exemple, un « appel de l'industrie pour l'innovation » a été lancé en 2018 et à nouveau en 2019, invitant les entreprises à apporter des solutions innovantes à quatre défis identifiés ensemble avec les autorités : la préparation aux enjeux de cybersécurité, la protection industrielle contre les menaces, l'accès sécurisé des systèmes, la détection intelligente des intrusions et des anomalies). Chaque solution retenue est financée à hauteur d'1 M SGD (environ 700 K EUR).

Plus généralement, Singapour accorde une priorité stratégique à l'innovation avec un investissement massif dans la recherche et des mesures d'incitation financière pour attirer les entreprises technologiques à forte valeur ajoutée.

II / Un accélérateur spécialisé dans la cybersécurité a été physiquement ouvert tout récemment sur le grand campus de start-up de Singapour, mais les enseignements à en tirer sont à ce stade limités

Un accélérateur spécialisé dans la cybersécurité, l'*Innovation Cybersecurity Ecosystem* (ICE71), a été ouvert en mars 2018, co-fondé par l'Université nationale de Singapour (NUS) et Innov8, le fonds dédié au capital-risque de Singtel (deuxième groupe de télécommunication en Asie). L'accélérateur est soutenu financièrement par les autorités et compte comme principal sponsor l'entreprise informatique américaine CISCO. Il est géré par CyLon, un incubateur britannique privé dédié à la cybersécurité.

L'accélérateur propose trois programmes : (i) un « bootcamp » d'une semaine permettant à un public large d'avoir un premier contact avec le monde de la cybersécurité pour tester des idées et discuter de leur faisabilité et viabilité commerciale, (ii) une aide au développement de 3 mois pour les start-up « early-stage » cherchant à adapter leur produit au marché (25 entreprises à ce jour), (iii) une aide à l'expansion (« scale-up ») en Asie-Pacifique pendant 6 mois pour des start-up locales et internationales (une vingtaine d'entreprises bénéficiaires actuellement).

L'incubateur a été localisé au sein du grand campus de start-up singapourien, Block71, qui héberge plus de 800 start-up et plus de 50 capital-risqueurs. La gouvernance d'ICE71 est effectuée par les deux organismes fondateurs, NUS Enterprise et Singtel Innov8, toutes deux des entités à dominante publique. Aucune orientation stratégique n'est à ce jour imposée, bien que les autorités y réfléchissent.

Ce dispositif reste petit et récent, et les enseignements à en tirer paraissent à ce stade encore limités. Singapour dispose néanmoins d'un vrai savoir-faire en matière de priorisation stratégique, avec une administration de très grande qualité qui est systématiquement à l'initiative. Les acteurs privés, locaux comme internationaux, ainsi que les universitaires, s'alignent ensuite derrière les priorités définies, notamment grâce à de généreuses incitations financières.

Initiatives visant à renforcer les synergies entre les experts publics, privés et académiques dans le domaine de la cybersécurité

SUISSE

Le numérique est un secteur important en Suisse, et plus particulièrement le domaine de la cybersécurité qui est en forte croissance. La recherche académique active, la création de start-up, le développement de PME et de filiales de groupes internationaux mais aussi la présence d'organismes internationaux actifs dans le secteur le démontrent. Des projets fédéraux qui permettent de rassembler acteurs publics et privés ont été mis en place ces dernières années dans le pays.

I / Approche et principales initiatives lancées dans le domaine de la cybersécurité

Il s'agit avant tout d'initiatives fédérales. Deux principales structures existent en matière de cybersécurité. Le Centre de recherche et d'évaluation en sécurité biométrique de 2015 et le Center for Digital Trust mis en place en 2017. Tous deux visent à favoriser la collaboration entre la recherche académique et l'industrie avec le développement de technologies et de projets de recherche. La formation, l'organisation d'évènements ainsi que l'aide à la mise en place de projets font également partie des activités de ces deux entités.

Le *Cyber Campus-Defence* a par ailleurs été créé en 2019 pour faire la liaison entre l'administration fédérale, l'industrie et le monde académique pour la cyberdéfense en parallèle des actions menées pour le secteur de la cybersécurité. Il fait partie du plan d'action pour la cyberdéfense adopté en 2017, dont le campus vise à encourager les transferts de technologies. Il est géré et financé par l'Armasuisse, administration fédérale et a été en partie mis en place au sein de l'Innovation Park de l'EPFL à Lausanne. De nombreuses entreprises, y compris des multinationales, sont implantées sur ce parc afin d'être au plus près des équipes de recherche.

II / Éléments caractéristiques et facteurs clés de l'approche suisse

Ces différentes initiatives sont réparties en plusieurs sites sur le territoire suisse et jouissent d'une proximité tant opérationnelle que géographique. Les partenariats avec les universités et plus de cinquante entreprises démontrent le réel souci de renforcer la coopération entre les différents acteurs avec la mise en place d'une véritable communauté autour de ces enjeux numériques.

Les principaux objectifs mis en avant à travers ces récentes initiatives sont :

- Anticiper des évolutions dans le domaine (ex : ID quantique et cryptologie quantique) ;
- Mettre en relation les différents acteurs de la cybersécurité ;
- Développer la recherche, la formation et l'attraction des talents ;
- Favoriser la collaboration entre les équipes dédiées à la cybersécurité et celles dédiées à la cyberdéfense.

Les deux centres de cybersécurité font l'objet d'un financement public-privé. Le Centre de recherche et d'évaluation en sécurité biométrique offre également aux chercheurs la possibilité de proposer des projets qui sont ensuite financés et menés par ces équipes sous la direction des entreprises. Outre le financement, la recherche est un des éléments fondamentaux de la politique suisse, ce que démontre la volonté de rapprocher physiquement chercheurs et entreprises privées.

Annexe 7 – Retour sur les ateliers de co-construction du Campus

Les différentes consultations menées depuis septembre ont permis de définir les prémices de ce lieu consacré au numérique. La matinée spéciale du jeudi 28 novembre 2019 qui s'est déroulée en présence de Monsieur Cédric O, secrétaire d'État chargé du numérique a permis de **concrétiser les premières déclarations de soutien et d'engagement** pour la création du futur campus dédié à la cybersécurité de la part d'une vingtaine d'entités.

Lors de cette matinée organisée au *Liberté Living Lab* à Paris, des ateliers de co-construction réunissant plus de 80 personnes ont été organisés autour de quatre grandes thématiques :

- Renforcer la coopération opérationnelle
- Soutenir la Recherche et l'Innovation
- Développer la formation en cybersécurité et susciter des vocations
- Contribuer au développement des communs de la cybersécurité

À cette occasion, beaucoup de moments ont été consacrés aux échanges, notamment aux exemples personnels et aux retours d'expérience. La matinée a rendu tangible un réel besoin de discussions entre pairs de la cybersécurité.

Cette synthèse reprend les défis et idées qui ont convergé, après les phases d'idéation et de mise en commun, au sein de chacun des 4 groupes

1 Atelier « Renforcer la coopération opérationnelle »

Les sous-groupes ont souvent identifié les mêmes défis mais formulés différemment : ils en ont retenu collectivement 5 qui concernent différents points de la chaîne « information — action ».

Dans ce groupe, il a été particulièrement apprécié de pouvoir échanger sur des questions complexes de points juridiques, souvent source de blocage en matière de coopération.

Quels cercles de confiance créer ?

La coopération / collaboration semble essentielle à la réussite des objectifs en matière de cyber sécurité, mais le groupe s'est légitimement posé la question de la confidentialité des données et des activités sensibles. Avec **QUI** partage-t-on **QUOI ?**

Idées proposées :

- Établir une cartographie des acteurs pour définir les niveaux d'accès aux informations
- Rédiger une charte de confiance signée par tous les acteurs.

Comment partager efficacement l'information ?

Défi lié au point ci-dessus d'une part (hétérogénéité des droits d'accès aux informations), et d'autre part lié à la complexité des référentiels juridiques différents selon les pays et les types de données.

Idées proposées :

- Clarifier / exploiter le cadre juridique permettant le partage des données.
- Créer une structure légère structurant le partage d'informations.
- Promouvoir la communication transversale : séminaires sectoriels.

Comment gérer la donnée ?

Toujours d'un point de vue juridique, la question qui a beaucoup animé le groupe est celle des différents régimes de confidentialité des données.

Idées proposées :

- préciser/élaborer une segmentation/nomenclature des données, un cadre juridique pour travailler sur les mêmes référentiels (temps réel ou non, ce qui relève de la défense ou du judiciaire…).

Comment s'adresser à tout l'écosystème ?

L'enjeu est de ne pas travailler uniquement avec les grands acteurs traditionnels, souvent rompus aux appels d'offres, et d'être assez agile pour intégrer des acteurs type start-up moins identifiés et moins rôdés, et d'être capable d'écouter toutes les expertises…etc.

Idées proposées :

- Profiter d'un lieu pour organiser des évènements physiques réguliers
- Mais aussi renforcer les liens grands groupes / start-up sur des besoins

Comment rendre efficace et lisible la chaîne d'intervention ?

Quand il s'agit de réagir à une crise, comment le Campus peut-il permettre d'être plus efficace ?

Idées proposées :

- Créer un centre de crise mutualisé (war room), qui regroupe personnes et outils identifiés en anticipation.
- Faire des exercices réguliers d'entraînement à la gestion de crise.

2 Atelier « Soutenir la Recherche et l'Innovation »

Le groupe s'est mis d'accord pour faire converger les différents défis identifiés par les sous-groupes en 3 défis majeurs pour soutenir la recherche et l'innovation : collaborer, orienter, et valoriser.

Soutenir la R&I c'est avant tout mieux collaborer

Créer les conditions / renforcer la collaboration entre l'ensemble des acteurs du futur campus

Idées proposées :

- Développer des systèmes de chaires (croisées) centrées sur les métiers ou sur des expertises / besoins scientifiques spécifiques (en favorisant les échanges avec d'autres thématiques
- Consacrer au sein de ce campus un espace totem ou un « showroom interdisciplinaire » ouvert à tous les utilisateurs (avec comme objectifs l'échange et le rayonnement business international)
- Déployer une plateforme collaborative, outil numérique au service des projets et des dynamiques collaboratives (échanges, ressources, contenus, projets communs, etc.)

C'est aussi mieux orienter l'ensemble des acteurs

Identifier les priorités business, les financements, les opportunités d'industrialisation ;

Aligner recherche et innovation en diffusant des cas d'usages opérationnels : *use cases / best cases*

Idées proposées :

- Renforcement et management des connaissances mais aussi des opportunités sectorielles grâce à une veille collaborative (technique, scientifique et concurrentielle).
- Déployer une cellule de captation (et d'influence) concernant les financements européens de la recherche.
- Organiser des rencontres entre ingénieurs-chercheurs et serial entrepreneurs (montée en compétences business).
- Créer des challenges sponsorisés sur des thématiques à opportunités afin d'impulser des projets / initiatives (ex. : hackathon, programmes d'expérimentation et de partage de données).

C'est enfin mieux valoriser les dynamiques de recherche et leurs résultats

Rendre attractives les carrières dans le champ de la recherche, favoriser son rayonnement international, renforcer les liens entre recherche et industrie

Idées proposées :

- Accompagner le « *go to market* » et connecter la recherche à des débouchés économiques potentiels (aider à trouver les premiers marchés / clients).
- Renforcer le financement (européen) pour les projets *early stage* et développer des programmes spécifiques pour le *scaling*.
- Favoriser l'émergence de nouveaux champions français / européens.

3 Atelier « Développer la formation en cybersécurité et susciter des vocations »

Sur cette thématique riche ont été identifiés 5 défis majeurs et bien distincts.

Comment faire de la formation différenciée et déclinée de façon adéquate ?

Le secteur de la cybersécurité comporte beaucoup de branches différentes, la formation doit donc être adaptée à chaque spécialité cyber (formation différenciée). Les formations existantes des différents acteurs de la cybersécurité doivent être valorisées.

Idées proposées :

- Développer des centres et des moyens d'entraînement pratique mutualisés, dans un lieu neutre.
- Mais aussi prioriser l'apprentissage et la formation continue.
- Sensibiliser les RH aux possibilités de mobilité en interne pour intégrer ces nouvelles formations.

Comment remplir les formations (attractivité) ?

Il existe déjà beaucoup de formations dédiées à la cybersécurité. L'enjeu est donc surtout de remplir ces formations, de les rendre plus attractives car les métiers sont souvent méconnus. Les échanges ont mis en avant le manque de représentation des femmes dans ce secteur.

Idées proposées :

- Sensibiliser à la cyber sécurité dès le collège / lycée.
- Coordonner les dispositifs destinés aux femmes pour des métiers vus comme masculins.

Le défi du partage et de la co-construction des contenus et pratiques

Il faut capitaliser sur les contenus de formation et les contenus pratiques des acteurs de la cybersécurité. (use-cases à partir des contenus de formation par exemple)

Idées proposées :

- Créer un espace commun de partage du contenu de formation, qui puisse être évalué par la communauté.

Comment modifier l'image et la culture Cyber ?

La culture cyber est méconnue du grand public ce qui explique le manque de vocations créées autour de ces métiers.

Idées proposées :

- S'insérer dans les produits culturels grand public.
- Mais aussi former les agents de l'État.
- Faire des évènements de communication.
- Modifier la communication sur les incidents cybersécurité.

Comment former les formateurs / encourager l'orientation et la réorientation vers les métiers de la cybersécurité ?

Idées proposées :

- Créer un parcours dédié aux formations Cyber (former les formateurs).
- Créer des outils de description des métiers aux différents publics.

4 Atelier « contribuer au développement des communs de la cybersécurité »

L'atelier a commencé par deux interventions pour définir un premier cadre de compréhension autour de la notion de communs numériques : d'abord sur des enjeux de protection des libertés par Valérie PEUGEOT de la CNIL, ensuite sur un exemple lié à la mobilité avec Fabien GAINIER de la Fabrique des Mobilités, pour montrer comment des collectifs aux intérêts partagés se rejoignent pour mutualiser des ressources rares (infrastructure, données, compétences) dans un cadre de confiance et proposer des offres de service communes.

Du fait de ces présentations, 3 défis majeurs sont ressortis des 2 sous-groupes :

Développer l'interopérabilité et valoriser la complémentarité des offres du campus

L'enjeu principal pour les communs de la cybersécurité est lié au développement de ressources communes à forte valeur ajoutée, permettant de mettre en commun la robustesse des grands acteurs avec la souplesse et la capacité d'innovation de petites structures.

Les sous-groupes ont proposé la création d'une infrastructure interopérable, qui permette ainsi à des organisations de toute taille de pouvoir tester la robustesse de leur solution, en réalisant par exemple des simulations et des essais.

Les équipes ont mis en lumière la nécessité de dé-siloter en interne du campus et de le faire savoir à l'externe. Un lieu physique partagé et hautement sécurisé permettrait une telle visibilité, afin de pouvoir tester des solutions de manière extrêmement agile (logique plug & play).

Idées proposées :

- Créer un lieu physique avec une programmation thématique (exercices, conférences…)
- Créer un showroom des offres cyber à l'état de l'art, avec des démonstrations scénarisées et des visites guidées accessibles des industriels, des entreprises
- Mutualiser une plateforme de tests afin de pouvoir tester la robustesse de différents dispositifs
- Mutualiser une infrastructure de confiance
- Fournir des briques facilement accessibles aux participants du campus

Comment partager la donnée en toute confiance

Idées proposées :

- Mettre à disposition, sur une plateforme opérée par un tiers de confiance, de multiples données (clients, menaces, contextes, tests…) pour pouvoir par exemple permettre aux acteurs de valider leurs solutions, d'identifier les menaces, d'entraîner leurs systèmes avec des données sensibles, des menaces récentes ou encore de simuler des attaques…
- Créer un Cyber Data Hub : L'un des deux sous-groupes a évoqué l'exemple du Health Data Hub créé par la délégation ministérielle du numérique en Santé et qui permet aux acteurs du secteur d'échanger des données anonymisées pour la recherche ou encore pour développer des services innovants.
- Organiser un premier cadrage commun permettant d'initier une dynamique de coopération dans le référencement et la qualification des menaces : IOC, attaques, état des menaces…
- Publier des API et proposer une logique d'animation et de prototypage de projets au sein du campus.

Aligner les acteurs autour d'engagement et de principes communs.

Idées proposées :

- Élaborer des principes partagés par l'ensemble des acteurs, au sein d'une charte liée au Campus.
- Proposer une première gouvernance partagée, multipartite puis organiser un forum thématique.

AUTRES IDÉES PROPOSÉES :

Pour inciter à mettre en commun ressources, compétences et connaissances :

- Le campus devra créer un environnement juridique agile. Les sous-groupes ont beaucoup échangé sur la nécessité de faire du campus un lieu d'expérimentation concrète, à la manière d'un bac à sable règlementaire et par exemple en suivant des cycles thématiques sectoriels. Un lien privilégié avec des dispositifs tels que France Expérimentation permettrait de créer cet environnement favorable.
- Créer des objets liens qui fédèrent en rendant tangible cette idée de communs.

Pour concilier partage et concurrence : charte de partage aux communs à intégrer dans les contrats (cf expérience de la Fabrique des Mobilités).

Penser les communs de la cybersécurité par filière, et impliquer les organisations professionnelles sur le campus.

Remerciements

Je tiens à remercier l'ensemble des personnes qui ont accepté de partager leur vision, leurs attentes et leurs intuitions à l'égard du projet Campus Cyber, lors de l'une des 60 auditions organisées entre septembre et novembre ou à l'occasion des ateliers thématiques de la matinée spéciale du 28 novembre 2019 qui aura réuni plus de 150 personnes.

Je remercie également l'ensemble des services de l'État ayant apporté leur expertise à la mission : l'ANSSI, la Direction générale des entreprises et la Direction des affaires juridiques du Ministère de l'Economie, des Finances, de l'Action et des Comptes publics, tout comme les services économiques des Ambassades de France ayant participé à l'étude comparative internationale.

Je remercie les industriels – Atos, Capgemini, Orange, Thales – qui ont, comme moi, adhéré immédiatement à la vision du Président de la République pour le Campus Cyber mais également les autres industriels, ETI et start-up, les organismes de recherche et de formation qui ont permis d'enrichir cette proposition.

Je remercie tout particulièrement celles et ceux ayant déjà déclaré leur soutien et leur souhait de prendre part à cette formidable aventure que sera le Campus Cyber.

Mes remerciements s'adressent, pour finir, à l'ensemble des personnes qui m'ont appuyé pendant cette mission : Nicolas Arpagian, Charly Berthet, Yann Bonnet, Christian Daviot, Jean-Baptiste Demaison, Magali Marques, Barbara Milia, Marc Renaudin et Faustine Saunier.