GOUVERNEMENT

Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

FRANCE 2030 : Bruno Le Maire, ministre de l'Economie, des Finances et de la Relance, inaugure le Campus cyber à la Défense et est revenu sur les premières réalisations de la stratégie nationale cyber

Paris-La Défense, le 15 février 2022

Un an après l'annonce de la Stratégie Nationale Cyber, le Campus Cyber a été inauguré par Bruno Le Maire, ministre de l'Economie, des Finances et de la Relance, Frédérique Vidal, ministre de l'Enseignement supérieur et de la recherche et de l'innovation, et Cédric O, secrétaire d'Etat à la Transition numérique et aux Communications. Ce campus sera le fer de lance de la France en matière de politique cyber.

Annoncé par le président de la République à l'été 2019, le Campus Cyber est l'incarnation de la politique française en matière de cybersécurité menée par la France. **Rassemblant plus de 160 acteurs nationaux et internationaux de la sécurité numérique - soit 1 800 experts - le Campus dirigé par Michel Van Den Berghe permettra de favoriser la réalisation de projets de recherche et de développement ainsi que l'éclosion des licornes cyber de demain.**

Ce campus accueillera et favorisera la collaboration entre les entreprises (grands groupes, PME et startups), les services de l'État (ANSSI, Ministère de l'Intérieur, Ministère des Armées…), les acteurs de la recherche (INRIA, CEA, CNRS…) les organismes de formation et les associations. Le regroupement de l'ensemble de ces acteurs, métiers et compétences est la clé du succès pour innover et pour renverser le rapport de force avec les cyber-attaquants ou cybercriminels. Lieu d'expérimentation et de partage, le Campus est fortement soutenu par la stratégie d'accélération cyber, avec près de 100 millions d'euros directs et indirects.

La stratégie cyber française a plus largement pour ambition de tripler le chiffre d'affaires du secteur cyber et de créer 37 000 emplois d'ici 2025. Le déploiement de ce plan doté de plus

d'un milliard d'euros est dynamique. De nombreuses actions ont été lancées depuis un an parmi lesquelles :

Soutenir l'innovation et la recherche

Le soutien au développement de technologies cyber innovantes et critiques, au centre de la stratégie, est lancé. **Financés à hauteur de 150 M€ par France 2030 sur la durée du plan, trois appels à projets ont déjà été ouverts (dont 2 en cours).** Plus de cinq startups, PME et grandes entreprises sont déjà soutenues parmi les premiers lauréats (voir la liste en annexe).

De nombreuses actions de soutien à l'entreprenariat ont aussi été mises en place, comme le start-up studio Cyber Booster, co-localisé entre Rennes et le Campus cyber et financé par le PIA4. Ce dispositif unique en Europe accompagne la création, et l'amorçage dans le domaine de la cybersécurité. Trois startups sont déjà incubées et près de 50 dossiers sont en cours d'instruction.

La prochaine étape sera la mise en place d'un accélérateur de start-ups.

La stratégie ambitionne également de soutenir la recherche sur le sujet. A cet effet, un **Programme et Equipement Prioritaires de Recherche (PEPR), doté de 65M€ et piloté par le CEA, CNRS, INRIA est en cours.** Il permettra d'exploiter le fort potentiel de recherche et de croissance de la filière française afin de garantir les conditions de sécurité nécessaires au développement des usages**.**

Pour accompagner et favoriser le transfert de compétences et de technologies issues de la recherche publique, un **Programme de transfert sur le Campus opéré par l'Inria** permettra de se concentrer sur le sourcing et la mise en œuvre de projets de R&D à forte valeur ajoutée, en partenariat avec le CEA, le CNRS, l'IMT et les grandes universités de recherche actives en cybersécurité, l'ANSSI et des entreprises.

Renforcer la résilience

Pour ce qui est de notre protection collective, le volet cybersécurité de France Relance, mobilisant 136 M€ sous pilotage de l'ANSSI, a pour vocation d'élever significativement le niveau de sécurité numérique de l'État et des services publics. Ce dispositif est orienté en priorité vers les collectivités territoriales et les entités impliquées dans la vie quotidienne des citoyens. Au 1er décembre 2021, 590 bénéficiaires ont déjà été retenus pour 45 M€ d'accompagnement, dont 438 collectivités territoriales, 109 établissements de santé et 43 établissements publics sur toute la France.

Par ailleurs, les Computer Security Incident Response Team (CSIRT) de Bourgogne Franche-Comté, du Centre Val de Loire, de Corse, du Grand Est, de Normandie, de Nouvelle Aquitaine et du Sud -Provence Alpes Côte d'Azur participeront au programme d'incubation de 4 mois mis en place par l'ANSSI dès février 2022. Cette incubation permettra aux CSIRT régionaux d'être rapidement opérationnels pour répondre de manière pertinente et efficace aux besoins identifiés, tout en s'intégrant pleinement à l'écosystème territorial et national. Un nouveau programme d'incubation sera proposé au second semestre 2022 pour les régions volontaires.

Former les talents cyber de demain

Pour répondre aux besoins en formation, la stratégie est dotée de 140 M€ via l'appel à manifestation « Compétences et métiers d'avenir » (CMA) de France 2030, dont deux vagues de relèves sont prévues les 24 février et 5 juillet 2022.

L'objectif de créer 37 000 emplois dans la filière ne sera atteignable que si des moyens de formation importants sont déployés. Environ 9250 personnes seront formées afin de devenir des spécialistes du domaine à tous les niveaux de bac+2 à bac+8. La recherche sera également soutenue via le financement de 100 thèses.

La formation massive des non spécialistes, 3 050 000 étudiants sur 5 ans, permettra enfin de donner un socle indispensable sur la cybersécurité à de nombreux jeunes Françaises et Français afin d'augmenter considérablement le niveau de conscience cyber de la population.

Sur ces sujets, la stratégie s'appuiera de manière importante sur les synergies apportées par le Campus cyber qui regroupe déjà plusieurs organismes de recherche, des acteurs de la formation et des employeurs à la recherche de profils cyber qualifiés.

Le Ministre de l'Economie, des Finances et de la Relance Bruno Le Maire a déclaré «*Le numérique est porteur d'avenir et d'espoir, mais il est aussi porteur de menaces. Face à ces menaces, l'Etat lève les boucliers, pour protéger ses citoyens, ses entreprises et ses services publics. En ce sens, l'inauguration de ce campus cyber est une étape majeure dans la mise en œuvre de la stratégie nationale de cybersécurité décidée par le président de la République. C'est un enjeu vital pour notre souveraineté et une opportunité économique majeure pour nos entrepreneurs et nos start-ups. Il faut donc continuer à déployer cette stratégie et investir aux côtés des acteurs privés de l'écosystème cyber français dans les compétences, la formation et les entreprises du secteur*».

Cédric O, secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques déclare *« Après un an de mise en œuvre au pas de charge, la stratégie nationale cyber accélère et prend une nouvelle dimension avec l'inauguration du campus cyber. Nous sommes fiers de ce lieu emblématique public-privé, qui est une première en Europe.*

La stratégie nationale cyber allie une grande ambition technologique et une action résolue pour élever notre niveau de résilience face aux cyber-menaces.

La protection de nos concitoyens, de nos entreprises et des collectivités publiques passe par la mobilisation des talents, des énergies, des moyens et des intelligences de chacun : start-ups, grands groupes, filières industrielles, collectivités territoriales, organismes de recherche, forces et agences de sécurité. Les acteurs sont pleinement au rendez-vous. ».

Contacts presse

Cabinet du secrétaire d'Etat chargé de la Transformation numérique et des Communications électroniques
presse@numerique.gouv.fr

Secrétariat général pour l'investissement 01 42 75 64 58 presse.sgpi@pm.gouv.fr	**Direction générale des entreprises** 01 44 97 04 49 presse.dge@finances.gouv.fr

A propos de France 2030

Le plan d'investissement France 2030 :

- ✓ **Traduit une double ambition** : transformer durablement des secteurs clefs de notre économie (énergie, automobile, aéronautique ou encore espace) par l'innovation technologique, et positionner la France non pas seulement en acteur, mais bien en leader du monde de demain. De la recherche fondamentale, à l'émergence d'une idée jusqu'à la production d'un produit ou service nouveau, France 2030 soutient tout le cycle de vie de l'innovation jusqu'à son industrialisation.
- ✓ **Est inédit par son ampleur** : 54 Md€ seront investis pour que nos entreprises, nos universités, nos organismes de recherche, réussissent pleinement leurs transitions dans ces filières stratégiques. L'enjeu : leur permettre de répondre de manière compétitive aux défis écologiques et d'attractivité du monde qui vient, et faire émerger les futurs champions de nos filières d'excellence.
- ✓ **Sera mis en œuvre collectivement :** pensé en concertation avec les acteurs économiques, académiques, locaux et européens pour en déterminer les orientations stratégiques. Les porteurs de projets sont invités à déposer leur dossier via une procédure ouverte, exigeante et sélective pour bénéficier de l'accompagnement de l'Etat, dans la continuité des Programmes d'investissements d'avenir et du plan France Relance.
- ✓ **Est piloté par le Secrétariat général pour l'investissement** pour le compte du Premier ministre.

Plus d'informations sur : https://www.gouvernement.fr/secretariat-general-pour-l-investissement-sgpi
@SGPI_avenir

ANNEXE

Les premiers lauréats retenus sont les suivants :

OLVID – WORKSPACE / OLVID

L'objectif du projet est de développer une solution de visioconférence, chat et partage de fichiers sécurisée qui offre une garantie sur la confidentialité et l'intégrité des données, l'assurance de l'identité des interlocuteurs, un anonymat complet vis-à-vis des tiers, tout cela sans avoir à faire confiance au moindre serveur, avec une simplicité d'usage, ouverte sur l'extérieur et sans aucune limite sur le nombre d'utilisateurs.

PARSEC EVENT HORIZON / SCILLE

Le projet consiste à réaliser, par hybridation avec des produits existants, une suite bureautique complète « Zero Trust » et « Zero Knowledge » (édition collaborative, messagerie instantanée, stockage de fichier, moteur d'indexation, couplage annuaire d'entreprise …), permettant aux utilisateurs de collaborer et d'échanger sans latence des données sensibles chiffrées de bout-en-bout et signées en utilisant le Cloud Public comme pivot d'échange.

CYBERSAFE OS / PROVE & RUN

L'objectif du projet CyberSafeOS est de fournir aux architectes des systèmes cyber physique, une brique technologique essentielle sous la forme d'un système d'exploitation (OS) destiné à être utilisé et intégré comme un composant off-the-shelf (COTS) lors de la conception de ces systèmes pour répondre aux doubles exigences cybersécurité et sureté de fonctionnement.

CASES / CLEARSY

Le projet CASES vise à construire un calculateur générique sûr et sécuritaire souverain, permettant de contrôler et commander des infrastructures critiques au plus haut niveau d'intégrité. Il combine l'état de l'art en matière de calculateur et de logiciel, en ayant recourt de manière raisonnée aux méthodes formelles.

OVERSEC / STORMSHIELD

Le projet Oversec vise à concevoir une brique logicielle multiplateforme intégrable dans les différents actifs des infrastructures critiques, permettant de filtrer et chiffrer leurs communications. Durcie, elle sera conçue de façon à être très résiliente aux cyberattaques et aux pannes matérielles ou logicielles qui pourraient impacter la sûreté de fonctionnement et les processus pour la maintenir en conditions opérationnelles et de sécurité, dont les mises à jour, devront être transparents pour la production protégée. En outre, le déploiement et la configuration des différentes instances du logiciel se feront de façon globale, avec une approche accessible pour les métiers non experts en cybersécurité.