GOUVERNEMENT

Liberté
Égalité
Fraternité

COMMUNIQUE DE PRESSE

Paris, le 27/10/2022
N° 260

Nouveaux lauréats France 2030 : Le Gouvernement dévoile 17 projets d'envergure pour hisser la France au rang des champions mondiaux de la cybersécurité

Jean-Noël Barrot, ministre délégué chargé de la Transition numérique et des Télécommunications, a annoncé lors de sa visite du Campus Cyber le soutien de 17 projets dans le cadre de la stratégie nationale d'accélération pour la cybersécurité de France 2030.

Essentielle à la souveraineté des états et vecteur de confiance dans l'économie et les outils numériques, la cybersécurité est un enjeu majeur du notre époque. Les craintes relatives à la sécurité des données représentent un frein à la numérisation, notamment des TPE et PME : près d'un chef d'entreprise sur deux déclare avoir peur de perdre ou se faire pirater des données[1]. Les acteurs publics et privés, au travers de synergies, ont un rôle essentiel à jouer pour parvenir à une parfaite maîtrise des technologies, développer les savoirs et renforcer les compétences nécessaires.

Annoncée le 18 février 2021, la stratégie nationale d'accélération pour la cybersécurité a prévu d'allouer plus d'un milliard d'euros (dont 720 M€ de financements publics) afin de faire de la France une nation de rang mondial en cybersécurité.

Cette stratégie s'articule autour de cinq axes :

- **Développer des solutions souveraines** de cybersécurité ;
- Renforcer **les liens et les synergies entre les acteurs** de la filière ;
- Soutenir l'adoption de solutions cyber par les individus, les entreprises, les collectivités et l'Etat, notamment via **des actions de sensibilisation** tout en faisant la promotion des offres nationales ;

[1] Source : Baromètre annuel France Num sur la transformation numérique des TPE et PME – Direction générale des Entreprises Septembre 2022

- **Former plus de jeunes et professionnels aux métiers** de la cybersécurité, fortement en déséquilibre ;
- **Soutenir en fonds propres** le développement des entreprises.

C'est dans cette optique que Jean-Noël Barrot a annoncé un soutien à hauteur de 39 M€ de financements publics de 17 projets d'envergure sélectionnés via 5 dispositifs lancés par le Gouvernement dans le cadre de France 2030. Ces projets visent à contribuer au développement de solutions innovantes en cybersécurité, à renforcer les dynamiques collaboratives entre les acteurs de l'écosystème et à accroitre l'offre de formation en cybersécurité. Cette annonce suit d'autres mesures déjà mises en œuvre, telles que l'aide à la mise en place du Campus cyber ou l'organisation d'une journée autonomie et souveraineté numérique destinée à faciliter les rencontres entre les offreurs de solutions souveraines de cybersécurité et grands donneurs d'ordres du secteur.

Cette visite a été également l'occasion pour le ministre de féliciter Florent Kirchner, nommé coordinateur national de la stratégie d'accélération Cybersécurité à compter du 1er décembre. Fort d'une expérience solide dans la recherche et auprès d'industriels dans les secteurs de la sûreté et cybersécurité, membres actif de divers groupes de travail sur les logiciels de haute confiance en France et en Europe, cet expert alliera compétences et connaissances des acteurs pour mener à bien la mission de France 2030 sur le volet cyber. Florent Kirchner partagera son temps entre le secrétariat général pour l'investissement, qui pilote France 2030, et le campus Cyber pour être en contact permanent avec l'écosystème.

Contacts presse :

Cabinet de Jean-Noël Barrot
presse@numerique.gouv.fr

Direction générale des Entreprises
presse.dge@finances.gouv.fr

Secrétariat général pour l'investissement
01 42 75 64 58
presse.sgpi@pm.gouv.fr

À PROPOS DE FRANCE 2030

- ✓ **Traduit une double ambition** : transformer durablement des secteurs clefs de notre économie (santé, 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 leaders de nos filières d'excellence. France 2030 est défini par deux objectifs transversaux consistant à consacrer 50 % de ses dépenses à la décarbonation de l'économie, et 50% à des acteurs émergents, porteurs d'innovation sans dépenses défavorables à l'environnement (au sens du principe *Do No Significant Harm*).
- ✓ **Sera mis en œuvre collectivement :** pensé et déployé en concertation avec les acteurs économiques, académiques, locaux et européens pour en déterminer les orientations stratégiques et les actions phares. Les porteurs de projets sont invités à déposer leur dossier via des procédures ouvertes, exigeantes et sélectives pour bénéficier de l'accompagnement de l'Etat.
- ✓ **Est piloté par le Secrétariat général pour l'investissement** pour le compte du Premier ministre et mis en œuvre par l'Agence de la transition écologique (ADEME), l'Agence nationale de la recherche (ANR), Bpifrance et la Banque des Territoires.

Plus d'informations sur : https://www.gouvernement.fr/france-2030 | @SGPI_avenir

ANNEXE : Détails des projets

APPEL A PROJETS : « SOUTIEN AU DEVELOPPEMENT DE TECHNOLOGIES INNOVANTES ET CRITIQUES EN CYBERSECURITE »

Cybelangel – Asset Discovery and Monitoring (ADM)
Développement d'une solution permettant de suivre l'exposition aux menaces cyber des différents éléments d'un système d'information. Cet outil permettra aux utilisateurs de focaliser leurs efforts de sécurisation de leur surface d'attaque vers leurs vulnérabilités les plus critiques.

Snowpack & Alternativ Brighnet
Ce projet vise à développer une surcouche de sécurisation et d'anonymisation des échanges sur Internet et une première application dédiée à la sécurité des PME et collectivités publiques. Exploitant plusieurs brevets du Commissariat à l'énergie atomique (CEA), les partenaires développeront la surcouche et l'intégreront dans une solution DNS « sans tiers de confiance » facilement déployable.

NANO Corp – EYE-OT
Solutions logicielles permettant de cartographier automatiquement tout réseau et détecter attaques comme anomalies. Sans dépendance matérielle, ces outils viseront particulièrement les réseaux industriels (IT/OT) et les TPE/PME, très exposés aux menaces cyber.

SYSTEREL, Schneider Electric & ARCYS – KICS2
Développement d'une brique générique personnalisable et des outils d'aide à l'administration conciliant les contraintes de mise à jour de cybersécurité avec le maintien de la sûreté des systèmes critiques. Elle proposera un compromis optimisé en termes de coût, d'employabilité et de performances (disponibilité, résilience…) entre approche générique et particularisation du produit.

Quarkslab – Quarks Remote Attestation (QRA)
Cet outil permet d'assurer qu'un équipement connecté à un réseau est bien celui fourni par le constructeur et qu'il n'a été ni altéré ni copié. Il sera particulièrement utile dans les domaines critiques utilisant de nombreux objets connectés : domaine médical, bancaire et réseaux industriels.

Synacktiv – Taranix
Ce projet vise à développer une gamme de produits et de services avancés à destination des services de police européens pour l'investigation cyber. La gamme sera composée d'un produit transportable permettant l'acquisition et la visualisation des données, ainsi que d'un ensemble de serveurs permettant la mise en commun de ressources entre différents services.

Apizee – VisoConfiance
Plateforme de collaboration en temps réel, sécurisée et souveraine, bénéficiant des dernières innovations en matière de chiffrement de données.

APPEL A PROJETS : « PROJETS INNOVANTS AU SEIN DU CAMPUS CYBER »

Hub France IA, ALEIA & QWAM – CYLVIA
Création d'une plateforme qui met en lien IA & Cybersécurité et permet de développer les compétences nécessaires à la formation d'un écosystème IA & Cyber. Il s'insère dans la dynamique du Campus Cyber et a été porté par son groupe de travail dédié à l'intelligence artificielle et la cybersécurité.

APPEL A PROJETS : « MUTUALISATION ET VALORISATION DES DONNEES D'INTERET CYBER »

Chapvision, Beware Cyberlabs, Olfeo, Exatrack & Quarkslab – SMART-CTI
Ce système d'alerte et d'anticipation cyber et des outils de renseignement avancés permettront de

qualifier et de contextualiser une menace avec réactivité et précision. Ce système collecte des données provenant de capteurs multiples répartis, les formate pour les agréger sur une plateforme de données de grande capacité. Ces données seront corrélées, analysées et présentées de manière à fournir un renseignement pratique aux responsables de la cybersécurité dans les centres de réponse aux incidents.

Thales, Sekoia, Harfanglab, Glimps, Geotrend, Snowpack, Filigran, Kor Labs, Telecom Sud Paris & Grenoble INP – SCRED

Ce projet vise à apporter un ensemble de services de renseignement sur la menace cyber au travers de la fourniture d'une source unique de renseignement structurée, agnostique et souveraine. Les acteurs de la détection et de la cybersécurité y sont associés afin de mutualiser et relier leurs bases de connaissance et leurs compétences.

APPEL A MANIFESTATION D'INTERET : « COMPETENCE ET METIER D'AVENIR » - VOLET DIAGNOSTIC

Pôle d'excellence cyber – DiagCyber

Elaboration d'un diagnostic partant de la perspective d'emplois en cybersécurité (37 000 selon France 2030) pour analyser les métiers à pourvoir (en nature, volumes et qualifications) puis faire le lien avec les formations et compétences existantes et à créer.

Université de Montpellier – Chaîne de production 4.0

Ce projet permet d'estimer les besoins de formation en cybersécurité afin de répondre aux besoins de la filière « industrie 4.0 ».

CCIR Paris Ile de France & CCI Hauts de Seine – Diagnostic CS&IA -92

Ce projet consiste à faciliter la structuration d'un écosystème territorial ouvert dans lequel l'offre de formation en cybersécurité et IA permet d'accroître la compétitivité des entreprises des Hauts-de-Seine. Cette offre proposera des parcours de professionnalisation robustes à des jeunes et des personnes en reconversion professionnelle, en adéquation avec les besoins en compétence des entreprises.

APPEL A MANIFESTATION D'INTERET : « COMPETENCE ET METIER D'AVENIR » - VOLET DISPOSITIF

Groupement d'intérêt public formation continue et insertion professionnelle – Cyber-Indus

Ce projet a pour objectif final de donner les ressources humaines et techniques nécessaires aux industriels français pour continuer le virage numérique amorcé dans un environnement sécurisé et ainsi rester en lice sur le marché européen et international.

INSA Centre Val de Loire – Cyberinsa

Ce projet construit en lien avec la feuille de route cyber du Conseil régional de la région Centre Val de Loire, vise à acculturer les organisations aux enjeux de la cybersécurité en les dotant de mécanismes de compréhension, d'anticipation et d'approches actives par la formation et l'expérimentation, *via* des mises en situation sur des réseaux et la mobilisation des résultats de la recherche.

Institut Mines-Télécom – Train-Cyber-Expert

Le but est de construire des ressources pédagogiques, sous forme de contenus numériques et de plateformes technologiques, organisés par blocs de compétences, dans une optique de modularité, de réutilisabilité et de pédagogie centrée sur les compétences conduisant à des certifications.

Université Grenoble Alpes – CyberSkills

Renforcement de l'offre de formation en cybersécurité en développant des outils pédagogiques innovants destinés à un public spécialisé et en renforçant la connaissance des enjeux cyber du public non-spécialiste avec des formations sur l'hygiène numérique et les réglementations liées au respect du RGPD et des actions de promotion de la filière, notamment auprès du public féminin.