**COMMUNIQUE DE PRESSE NATIONAL – PARIS – 6 AVRIL 2023**

# Stratégie nationale « Cybersécurité » de France 2030 : deux nouveaux projets lancés dans le cadre du Programme de recherche (PEPR)

**Lancé en 21 juin 2022 dans le cadre de la stratégie nationale pour la cybersécurité de France 2030, le programme de recherche (PEPR) Cybersécurité vise à apporter des réponses à 10 défis de recherche fondamentale au service de la filière industrielle et des acteurs étatiques. Il est piloté par le CEA, le CNRS et Inria et opéré par l'Agence nationale de la recherche (ANR). En marge du Forum International de la Cybersécurité, qui se tient du 5 au 7 avril 2023 à Lille), deux nouveaux projets de recherche du programme sont lancés.**

Dans un contexte d'une menace cyber en constant développement et d'une grande compétition mondiale visant le développement de solutions pour protéger les citoyens, les entreprises et les institutions, la France s'est dotée d'une stratégie nationale pour la Cybersécurité, dans le cadre de France 2030. Le but : tripler le chiffre d'affaires de la filière d'ici 2025, former plus de professionnels et développer des solutions souveraines alors que l'enjeu de cybersécurité est toujours plus visible.

Financé à hauteur de 65 millions d'euros par le plan France 2030, le programme de recherche Cybersécurité soutient des activités de recherche au meilleur niveau mondial et ses résultats nourrissent les actions plus aval de cette stratégie nationale comme le Programme de Transfert au Campus Cyber opéré par Inria, l'incubateur CyberBooster, le Grand Défi Automatisation de la Cybersécurité, les appels à projets Développement de Technologies Innovantes Critiques, entre autres.

Impliquant environ 200 chercheurs et enseignants-chercheurs permanents issus du CEA, du CNRS, d'Inria, ainsi que de 23 universités[1] et grandes écoles[2], il fait appel à plusieurs disciplines : informatique, mathématiques, électronique et traitement du signal pour aider à sécuriser les trois couches du cyberespace (matériel, logiciel, données).

Le PEPR Cybersécurité soutient des actions spécifiques avec notamment la mise en place de projets ciblés et des appels à projets. Des actions d'animation et de transferts de connaissance entre académiques et industriels sont également mis en place. **Sept premiers projets ont été lancés en 2022[3] lors d'un évènement organisé au Campus Cyber (La défense) :**

Le projet **iPOP** (Projet interdisciplinaire sur la protection des données personnelles) vise à étudier les menaces vis-à-vis de la vie privée introduites par ces nouveaux services et de concevoir des solutions théoriques et techniques de protection de la vie privée, compatibles avec la réglementation française et européenne, qui préservent la qualité d'expérience des utilisateurs. Ces solutions seront déployées et évaluées, à la fois sur leurs aspects technologiques, mais également juridiques et d'acceptabilité sociétale.

Le projet **SECURE COMPUTE** (Sécurité des calculs) vise à étudier les mécanismes cryptographiques permettant d'assurer la sécurité des données, au cours de leur transfert ainsi que pendant toute la période de stockage, mais également lors de traitements, malgré des environnements non-maîtrisés tels qu'Internet pour les échanges et le Cloud pour l'hébergement et le traitement.

Le projet **SVP** (Vérification de protocoles de sécurité) vise à permettre l'analyse de protocoles déployés ou en cours de déploiement, aussi bien au niveau des spécifications de ces protocoles, que de leurs implémentations. Il développera des techniques et des outils permettant la mise en place de solutions dont la sécurité ne sera plus remise en question de manière cyclique.

Le projet **DEFMAL** (Défense contre les programmes Malveillants) vise l'étude des logiciels/programmes malveillants (malware, ransomware, botnet, etc). Il développera de nouvelles approches pour analyser les programmes malveillants et aidera à la compréhension globale de l'écosystème du malware dans une approche interdisciplinaire impliquant l'ensemble des acteurs concernés.

Le projet **SUPERVIZ** (Supervision et orchestration de la sécurité) cible la détection, la réponse et la remédiation aux attaques informatiques, sujets regroupés sous l'appellation de « supervision de sécurité », qui cherche à renforcer les mécanismes de protection préventifs et à pallier leurs insuffisances.

Le projet **SECUREVAL** vise à concevoir de nouveaux outils bénéficiant des nouvelles technologies numériques pour vérifier l'absence de vulnérabilités matérielles comme logicielles, et réaliser les preuves de conformité requises.

Le projet **ARSENE** vise à accélérer de manière coordonnée et structurée la recherche et le développement de solutions de sécurité souveraines et industrialisables. La mise en œuvre de démonstrateurs ASIC et FPGA intégrant les briques étudiées et développées permettra dans une dernière étape de tester et valoriser ces travaux de recherche.

**REV et CRYPTANALYSE, lauréats du premier appel à projets du programme Cybersécurité**

Le premier appel à projets du PEPR Cybersécurité, lancé en juin 2022 et opéré par l'ANR, a permis de sélectionner deux nouveaux projets qui seront financés sur 5 ans :

Le projet **REV** (Recherche et exploitation de vulnérabilités), dont la coordination a été confiée à Aurélien Francillon (Eurecom) étudiera les attaques sur les systèmes numériques (comme les smartphones et les objets connectés). Ces cibles sont désormais des systèmes complexes et le projet s'intéressera à toutes leurs couches, matériel, logiciel et interfaces de communications (Web et IoT), avec des applications possibles des résultats du projet dans la forensique, la criminalistique ou encore la correction des vulnérabilités.

Le projet **CRYPTANALYSE,** dont la coordination a été confiée à Gaétan Leurent et Emmanuel Thomé (Inria), étudiera la résistance des systèmes cryptographiques. La cryptographie est en effet devenue un outil indispensable pour sécuriser les communications et la confiance repose sur la supposée difficulté de l'attaquer. Le projet visera à éprouver la solidité de ces primitives, et utilisera tout l'arsenal mathématique et algorithmique disponible pour déployer des attaques efficaces afin de faire progresser l'état de l'art en cryptanalyse et augmenter à terme la sécurité des primitives cryptographiques utilisées aujourd'hui et demain.

**Citations :**

Pour **Florent Kirchner**, SGPI, Coordinateur de la stratégie nationale pour la cybersécurité
« Face aux enjeux de la transition numérique pour les citoyens, les entreprises et les institutions, et aux évolutions rapides des cyberattaquants, il est plus que jamais essentiel d'étudier la résistance des systèmes cryptographiques et la détection des vulnérabilités des outils numériques de la vie quotidienne. Les deux projets sélectionnés à l'issue de cet appel à projets opéré par l'ANR, financés par France 2030 à hauteur de 10 M€, vont compléter les 7 autres projets déjà lancés en 2022 dans le cadre du Programme de recherche de la stratégie nationale. Pour contribuer, *in fine*, à la maîtrise de technologies numériques souveraines et sures. »

**Clara Bertolissi**, Responsable d'action Cybersécurité, Direction des grands programmes d'investissements de l'Etat, Agence nationale de la recherche
« Avec l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu sociétal tant pour les institutions, les entreprises que les citoyens. Le monde de la Recherche contribue significativement à proposer des solutions nouvelles, adaptées et compétitives. C'est l'ambition du programme de recherche Cybersécurité pour lequel l'Agence nationale de la recherche assure l'évaluation, le financement et le suivi des projets pour le coordinateur de la Stratégie nationale Cybersécurité, avec es pilotes du PEPR.. La qualité des projets soumis et sélectionnés dans le cadre de ce premier appel à projets démontre une fois de plus la vitalité et les compétences d'une communauté académique française internationalement reconnue dans ce domaine. Ils vont contribuer à structurer des communautés de recherche interdisciplinaires et au meilleur niveau mondial pour développer les technologies et outils indispensables à la filière. »

L'Etat consacre 3 milliards d'euros pour la recherche à travers des programmes de recherche ambitieux (les PEPR), portés par les institutions de recherche pour consolider le leadership français dans des domaines clés ; liés ou susceptibles d'être liés à une transformation technologique, économique, sociétale, sanitaire ou environnementale et qui sont considérés comme prioritaires au niveau national ou européen.

## Notes

1. Sorbonne Université ; Université Bretagne Occidentale ; Université Bretagne Sud ; Université de Lille ; Université de Lorraine ; Université de Montpellier ; Université de Rennes ; Université de Versailles Saint-Quentin-en-Yvelines ; Université Grenoble Alpes ; Université Jean Monnet St Etienne ; Université Paris-Saclay ; Université de Picardie Jules Verne.

2. ENS Rennes ; ENSTA Bretagne ; ENS PSL ; EURECOM ; Grenoble INP ; INSA CVL ; INSA Lyon ; INSA Rennes ; Institut Mines Télécom ; CentraleSupélec ; EDHEC.

***A propos de France 2030***

Présenté le 12 octobre 2021 par le Président de la République **France 2030 :**

- ✓ **Traduit une double ambition** : **transformer durablement des secteurs clefs** de notre économie (énergie, automobile, santé, aéronautique ou encore espace) par l'innovation technologique et industrielle, 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 enjeux écologiques et d'attractivité** du monde qui vient, et faire émerger les futurs champions de nos filières d'excellence pour ainsi **renforcer la souveraineté et l'indépendance française** dans des secteurs clés. 50 % des dépenses seront en ce sens consacrées à la décarbonation de l'économie, et 50% fléchées au profit d'acteurs émergents, porteurs d'innovation sans impact défavorable sur l'environnement (au sens du principe *Do No Significant Harm*).

- ✓ **Sera mis en œuvre collectivement :** le plan est pensé et déployé **en concertation avec les acteurs économiques, académiques, locaux et européens** qui ont contribué à en déterminer les orientations stratégiques comme 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'État.

- ✓ **Est piloté par le Secrétariat général pour l'investissement** pour le compte de la Première ministre et mis en œuvre par l'Agence de la transition écologique (**ADEME**), l'Agence nationale de la recherche (**ANR**), la Banque publique d'investissement (**Bpifrance)** et la **Banque des territoires**.

Plus d'informations sur : france2030.gouv.fr | @SGPI_avenir

## Notes

1. Sorbonne Université ; Université Bretagne Occidentale ; Université Bretagne Sud ; Université de Lille ; Université de Lorraine ; Université de Montpellier ; Université de Rennes ; Université de Versailles Saint-Quentin-en-Yvelines ; Université Grenoble Alpes ; Université Jean Monnet St Etienne ; Université Paris-Saclay ; Université de Picardie Jules Verne.

2. ENS Rennes ; ENSTA Bretagne ; ENS PSL ; EURECOM ; Grenoble INP ; INSA CVL ; INSA Lyon ; INSA Rennes ; Institut Mines Télécom ; CentraleSupélec ; EDHEC.

**Contacts**

**Presse CNRS** l Priscilla Dacher l **T +33 1 44 96 46 06** l priscilla.dacher@cnrs.fr
**Presse CEA** l Tuline Laeser l **T +33 06 12 04 40 22** l tuline.laeser@cea.fr
**Presse Inria** l l Laurence Goussu l **T +33 1 39 63 57 29** l laurence.goussu@inria.fr

**Presse ANR |** Katel Le Floc'h |**T +33 1 78 09 80 70** | Katel.lefloch@agencerecherche.fr