CAMPUS CYBER

STRATÉGIE NATIONALE CYBERSÉCURITÉ

PROGRAMME transfert campus cyber

FRANCE 2030

Programme de Transfert au Campus Cyber

opéré par

Inria

Appel à Projets de Recherche partenariale

Ouverture des candidatures *: 1er Janvier 2023 à 12h00 (heure de Paris)*

Format de dépôt : *Fil de l'eau avec une levée le dernier mardi de chaque mois*

Adresse de dépôt *: ptcc.rd@inria.fr*

Point de contact *: michel.mauny@inria.fr*

Durée du programme : 60 mois (5 ans)

Versions :

- 2024-05 : mise à jour points de contact
- 2023-11 : mention frais de fonctionnement
- 2023-04 : version initiale

Résumé

La stratégie nationale d'accélération pour la cybersécurité, qui s'inscrit dans le plan d'investissement France 2030, s'articule autour de cinq axes :

- Renforcer les liens et synergies entre les acteurs de la filière ;
- Développer des solutions souveraines et innovantes de cybersécurité ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- Soutenir le développement des entreprises de la filière via un abondement en fonds propres ;
- Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales.

Dans le cadre du **Campus Cyber** et de son réseau en régions, Inria a été mandaté pour assurer la mise en œuvre d'un programme de transfert de compétences et de technologies issues de la recherche publique vers l'ensemble des écosystèmes territoriaux de la cybersécurité, le **Programme de Transfert au Campus Cyber (PTCC).**

Ce **programme de 5 ans** opéré pour le compte de l'ensemble de la communauté académique a pour objectifs :

- De renforcer les efforts de recherche en cybersécurité, en particulier en favorisant les projets conjoints entre acteurs académiques, industriels et gouvernementaux ;
- De favoriser le transfert de compétences et de technologies issues de la recherche publique vers l'ensemble des acteurs de l'écosystème, avec un rôle affirmé de tiers de confiance neutre garant d'un cadre souverain ;
- D'accélérer la mise sur le marché de produits de cybersécurité avec une vraie barrière technologique et de renforcer les logiques partenariales ;
- D'accélérer la dynamique de formation initiale et de formation continue à la cybersécurité, répondant au besoin des entreprises, en lien avec les établissements de formation concernés, en premier lieu les grandes universités de recherche ;
- De s'articuler avec les dispositifs de soutien à l'entreprenariat technologique afin de soutenir la création et le développement d'entreprises innovantes.

Cet appel à projets s'inscrit dans le cadre du renforcement des efforts de recherche en cybersécurité, il a pour objectifs :

- De soutenir l'accélération de l'obtention de savoirs, technologies et outils sur des problématiques stratégiques/des cas d'usage identifiés par les acteurs de l'écosystème ;
- De financer des projets de recherche appliquée partenariale développés par des acteurs académiques (établissements d'enseignement supérieur, organismes de recherche) sur le modèle développé dans les PEPR, et étatiques, actifs en cybersécurité, en relation avec les industriels.

Il est doté d'un budget de 7,6 M€ pour financer au moins 5 projets sur la durée du programme.

Le projet de recherche prend la forme d'une équipe sous la direction d'un responsable de projet, chercheur ou enseignant-chercheur, dans le cadre d'un consortium regroupant plusieurs partenaires académiques et permettant de produire des résultats de recherche exploitables en contexte industriel à court ou moyen terme afin de développer des solutions technologiques répondant à un ou des cas d'usage.

Mots clefs

Sécurité de l'information
Sécurité des systèmes

1. Contexte et objectifs de l'appel à projet

Contexte général

Dans le cadre du Plan « France 2030 » et du Programme d'investissements d'avenir, le Gouvernement a défini une stratégie d'accélération « Cybersécurité ».

Construite en pleine collaboration entre les administrations compétentes sur les sujets cyber et les acteurs de l'écosystème (industriels, organismes de recherche, collectivités…), cette stratégie se décline selon cinq axes :

- Renforcer les liens et synergies entre les acteurs de la filière ;
- Développer des solutions souveraines et innovantes de cybersécurité ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- Soutenir le développement des entreprises de la filière via un abondement en fonds propres ;
- Soutenir la demande (individus, entreprises, collectivités et État), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales.

Le Campus Cyber

L'une des mesures portées par la stratégie d'accélération vise au lancement du Campus Cyber. Ce lieu totem de la cybersécurité en France, est structuré autour de 4 piliers :

- Les opérations : partage des données pour renforcer la capacité de chacun à maîtriser le risque numérique.
- La formation : aide à la formation initiale et continue des différents publics (agents de l'État, salarié(e)s, étudiante(s), personnels en reconversion…) pour une montée en compétence globale de l'écosystème.
- L'innovation : développement des synergies entre les acteurs publics et privés pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique.
- L'animation : un lieu vivant et ouvert dédié à la programmation d'événements innovants propice aux échanges et à la découverte des évolutions de la société numérique de confiance.

Le Campus Cyber implanté dans un bâtiment de 26 000 m² dans le quartier de La Défense est au cœur d'un réseau de « Campus Cyber territoriaux » en cours de création dans plusieurs régions.

Le Programme de Transfert au Campus Cyber

Dans le cadre du Campus Cyber et de son réseau en régions, Inria a été mandaté pour assurer la mise en œuvre d'un programme de transfert de compétences et de technologies

issues de la recherche publique vers l'ensemble des écosystèmes territoriaux de la cybersécurité, le Programme de Transfert au Campus Cyber (PTCC) par Inria.

En cohérence avec la feuille de route du Campus Cyber les objectifs du programme sont, dans ce cadre :

- De renforcer les efforts de recherche en cybersécurité, en particulier en favorisant les projets conjoints entre acteurs académiques, industriels et gouvernementaux ;
- De favoriser le transfert de compétences et de technologies issues de la recherche publique vers l'ensemble des acteurs de l'écosystème, avec un rôle affirmé de tiers de confiance neutre garant d'un cadre souverain ;
- D'accélérer la mise sur le marché de produits de cybersécurité avec une vraie barrière technologique et de renforcer les logiques partenariales ;
- D'accélérer la dynamique de formation initiale et de formation continue à la cybersécurité, répondant au besoin des entreprises, en lien avec les établissements de formation concernés, en premier lieu les grandes universités de recherche franciliennes ;
- De s'articuler avec les dispositifs de soutien à l'entreprenariat technologique afin de soutenir la création et le développement d'entreprises innovantes.

Objectifs de l'appel à projet

Cet appel à projets s'inscrit dans le cadre du renforcement des efforts de recherche en cybersécurité, il a pour objectifs :

- De soutenir l'accélération de l'obtention de savoirs, technologies et outils sur des problématiques stratégiques/des cas d'usage identifiés par les acteurs de l'écosystème ;
- De financer des projets de recherche partenariale associant des acteurs académiques (établissements d'enseignement supérieur, organismes de recherche). Des acteurs étatiques actifs en cybersécurité et des acteurs industriels peuvent être associés, sans être financés.

Il est doté d'un budget de 7,6 M€ pour financer au moins 5 projets sur la durée du programme.

2. Source, nature et résultats des projets attendus

L'Appel à Projet permanent : « AAP de recherche partenariale » est piloté par la direction de programme du PTCC.
Il est diffusé au niveau national par la direction de programme, en étroite association avec les établissements d'enseignement supérieur et de recherche, les écoles et les organismes de recherche.
La détection et la structuration des projets sont assurées par la direction de programme, avec le soutien de ses partenaires.

Résultats attendus

Le projet doit permettre de produire des résultats de recherche (savoirs, technologies, outils) exploitables par la filière à court ou moyen terme afin de développer des solutions technologiques répondant à un ou des cas d'usage. Ainsi, les deux principaux livrables d'un projet sont :

- la production d'une preuve analytique ou expérimentale des principales fonctions et/ou caractéristiques du concept proposé au regard du ou des cas d'usage proposés ;
- un démonstrateur de laboratoire (TRL 3).

Les sujets de recherche attendus doivent être complémentaires à ceux traités dans les projets du PEPR Cybersécurité, que les porteurs de projets sont invités à consulter avant de soumettre leurs propositions.

La proposition de projet doit identifier les cas d'usage rendus possibles par les résultats attendus. Cette proposition doit également argumenter la capacité de valorisation ultérieure des travaux.

Organisation des projets

Le projet est porté par une équipe sous la responsabilité d'un responsable de projet, chercheur ou enseignant-chercheur, dans le cadre d'un consortium regroupant plusieurs partenaires académiques. La constitution d'équipes de recherche conjointes confirme l'implication des partenaires.
Les membres constituant l'équipe sont typiquement :

- du personnel permanent des partenaires académiques à hauteur totale d'1 ETP, parmi lequel sera identifié un responsable de projet contribuant pour un minimum de 20% de son temps au projet ;
- 1 post-doctorant ;
- 1 doctorant ;
- 2 ingénieurs de développement.

Les membres du projet devront contribuer aux actions d'animation du PTCC en y organisant au moins leurs ateliers de travail et réunions significatives (lancement, points d'avancement, présentations de résultats importants, etc.). En regard des objectifs du programme, certains de ces évènements seront publics.

Les projets sélectionnés disposent d'un accueil dans l'espace Recherche du Campus Cyber et de l'accès aux équipements et services mis à disposition dans le cadre du Fab Lab et des plateformes numériques du Campus Cyber, notamment pour la réalisation de leurs démonstrateurs.

Les projets sélectionnés feront l'objet d'un accord de consortium qui aura pour objet de définir le cadre dans lequel les partenaires souhaitent coopérer et qui précisera notamment les objectifs du projet, les apports des parties prenantes au contrat et les conditions d'accès à la PI.

3. Structuration et durée des projets

La proposition décrivant un projet doit contenir un diagramme de Gantt, reprenant les différents lots, indiquant leurs livrables et identifiant leurs dépendances.

Les projets sélectionnés ont une durée de 36 mois à 48 mois.

4. Examen des projets proposés

Procédure de qualification et de sélection

Les projets font l'objet dans leur phase de définition, d'un accompagnement assuré par la **direction du Programme** Transfert du Campus Cyber.

Le dossier de soumission doit être déposé complet. La direction de programme validera sa recevabilité (voir ci-dessous). Un message de confirmation sera alors envoyé aux porteurs pour organiser une présentation du projet initial au **Comité Technique**. Elle permettra notamment d'apporter un regard critique destiné à consolider la proposition au regard de ses qualités scientifiques et techniques, ainsi que de sa pertinence au regard des objectifs du programme.

La sélection du projet et la caractérisation de son financement sont assurées par le **Comité des Opérations** du PTCC composé d'un représentant de chacune des organisations suivantes : ANR, SGPI, ANSSI, DGA, Inria, complété en tant que de besoin de personnalités choisies dans un pool d'experts.

Les étapes d'instruction et de sélection des projets incluent les mesures nécessaires à la prévention et à la gestion des risques conflits d'intérêt.

Critères de recevabilité et de sélection

Les conditions de recevabilité sont la complétude du dossier, l'éligibilité des partenaires et la conformité du consortium aux contraintes données ci-dessus.

Les principaux critères de sélection sont :

- la stratégie et la pertinence du projet vis-à-vis des objectifs affichés dans l'appel à projets, et notamment :
  - la clarté de la définition des objectifs et leur adéquation à l'APP et aux objectifs du PTCC,
  - l'identification des besoins auxquels répondent les objectifs du projet
  - la pertinence applicative du projet et l'horizon auquel se situent les perspectives de transfert,
  - son positionnement par rapport à l'existant ou aux projets concurrents,
  - l'impact potentiel qu'auront les résultats du projet ;
- l'organisation et la gestion prévues du projet :
  - l'organisation des tâches, l'identification des livrables et l'organisation générale du projet ;
- et l'évaluation de la faisabilité du projet, et en particulier de :
  - la bonne répartition des tâches,
  - la pertinence des analyses des risques techniques qui pourraient menacer la bonne exécution des tâches,
  - la qualité de la couverture par les équipes des différents champs de compétences nécessaires au bon déroulement du projet,
  - l'expérience antérieure et le niveau de compétences des équipes,
  - l'adéquation des ressources aux tâches et objectifs du projet.

5. Modalités de financement

Le projet bénéficie d'un financement complémentaire aux apports des partenaires.

Le financement d'un projet par le programme est au maximum de 1,3 M€, frais généraux non inclus.

Les moyens sont alloués en regard des objectifs du projet par le Comité des Opérations. Le dimensionnement sera défini au regard du potentiel de développement du projet.

Les financements apportés aux partenaires « établissements d'enseignement supérieur et de recherche, les écoles et les organismes de recherche »[1] sont destinés à couvrir les coûts directs du projet c'est-à-dire les salaires et charges du personnel encadrant (responsable de projet avec des statuts de permanents ou statutaires dans certaines limites) et les opérationnels du projet (ingénieurs de recherche, doctorants et post-doctorants). Des frais de fonctionnement (déplacements, petit matériel) peuvent être inclus dans la demande de financement des partenaires, dans la limite de 3 000€ par personne x année d'aide demandée[2].

Les frais généraux viennent en sus de ce financement.

Il n'y a pas de prise en charge de coût d'environnement ni d'achats informatiques.

Le soutien financier sera apporté dans le cadre d'un conventionnement entre Inria et chacun des partenaires.

6. Dossier de candidature

Le dossier de soumission sous forme électronique doit être soumis complet aux formats demandés. Il devra comporter l'ensemble des éléments nécessaires à l'évaluation scientifique et technique du projet ainsi que son budget. Chaque dossier de candidature contiendra obligatoirement :

- Un descriptif scientifique du projet : annexe technique ;
- Une demande de financement du projet : annexe financière ;
- Une présentation simplifiée du projet : trame de présentation.

Les trames sont fournies en annexe du présent document.

7. Accord de consortium

Un projet sélectionné devra faire l'objet d'un accord de consortium précisant les droits et obligations de chaque établissement partenaire du projet. Cet accord prendra la forme d'un avenant à un accord générique, disponible sur demande à la direction du programme. Cet avenant précisera notamment :

- La répartition de la dotation financière, des tâches et des livrables entre les différents partenaires, ainsi que les moyens humains et financiers mobilisés en propre par ces derniers ;

[1] Financés sur la base du coût marginal, au sens de l'ANR.

[2] À titre d'exemple, un partenaire demandant le financement de 18 mois d'ingénieur et 36 mois de doctorant pourra bénéficier au maximum de 3000 € x (18 + 36)/12 = 13500 € de frais de fonctionnement.

- Les modalités scientifiques, techniques et financières d'accès aux ressources partagées entre les partenaires ;
- Les modalités de valorisation des résultats obtenus à l'issue des recherches et de partage de leur propriété intellectuelle et industrielle.

8. Ordonnancement

Le processus de qualification et de sélection des projets est le suivant :

- Réception des projets ;
- Validation de la recevabilité par la direction de programme ;
- Réception et envoi aux membres du Comité Technique de la V0 des annexes technique et financière (AT et AF) ;
- Organisation par la direction de programme de la revue du projet initial par le Comité Technique ;
- Retour par la direction de programme au porteur des premières préconisations pour finalisation de la V0 des AT et AF ;
- Présentation des projets au Comité Technique par les porteurs de projet ;
- Rédaction et envoi aux porteurs par la direction de programme des préconisations du Comité Technique ;
- Rédaction par le porteur d'une V1 des AT et AF ;
- Réception et envoi aux membres du Comité des Opérations de la V1 des AT et AF, accompagnée d'un recueil des recommandations corédigées avec le Comité Technique ;
- Présentation des projets au Comité des Opérations par les porteurs de projet ;
- Sélection et validation de la demande de financement par le Comité des Opérations.

9. Données

Le partage de données entre les acteurs d'une filière est un élément essentiel à sa structuration, axe fort de la Stratégie Nationale cyber. Dans le plein respect du droit de propriété des producteurs des données, cet appel à projets introduit certaines exigences qui doivent faciliter leur partage. Ces exigences seront valables pour tous les projets recevant des financements étatiques dans le cadre de la Stratégie Nationale Cyber.

Protection et respect de la réglementation

Il est essentiel que les données produites ou manipulées dans le cadre des projets financés par la Stratégie Nationale, que ce soit lors de la phase de développement, d'expérimentation ou ultérieurement en production, soient protégées au bon niveau en fonction de leur sensibilité. Les objectifs sont à la fois de veiller à la protection de la propriété intellectuelle, d'éviter l'appauvrissement informationnel (typiquement contractuel) et de prévenir au mieux les fuites massives de données.

Dans cette optique un travail d'analyse préalable est demandé au(x) porteur(s) pour déterminer le niveau de sensibilité des différentes catégories de données du projet. Les mesures de sécurité qui en découleront (et qui devront être implémentées dans le cadre du projet) pourront faire intervenir la protection des communications de bout en bout (i.e. cryptographie) lors du transfert des données, un stockage sécurisé (i.e. chiffré et sauvegardé), un contrôle d'accès adéquat ainsi que des mesures juridiques ou

contractuelles appropriées. Le cas échéant, le respect de la réglementation applicable (RGPD par exemple) sera bien sûr le point de départ de cette analyse et de ces travaux.

Production, stockage et valorisation de données d'intérêt cyber

Dans le cadre des projets candidats, il est également demandé au(x) porteur(s) de capitaliser sur les opportunités de production de données d'intérêt cyber (de toutes natures). Cela implique de mettre en place les mécanismes ad-hoc de captation, de prétraitement (typiquement de labélisation ou de normalisation) et de stockage de ces données même s'il s'agit de données annexes non essentielles au projet.
Les réflexions sur un modèle économique autour de ces données sont fortement encouragées.

Dans le cas d'une abondance trop importante de données ou de contraintes spécifiques, une priorisation sur les données à stocker pourra être effectuée en discussion avec le comité de suivi du projet. De même, la durée de stockage est à déterminer en fonction de la typologie des données concernées.

Le non-respect de cet aspect impactera négativement le dossier lors du processus de sélection et pourra in fine aboutir à une réduction du taux d'aide.

Accès aux données d'expérimentation

Les données générées dans le cadre du paragraphe précédent restent la propriété de leur producteur. Néanmoins, il est demandé au(x) porteur(s) bénéficiant d'aide d'Etat dans le cadre de la Stratégie Nationale de cybersécurité de s'engager à mettre à disposition ces données gracieusement de manière ponctuelle dans le cadre d'expérimentations techniques non commerciales sous réserve de la compatibilité avec la réglementation et avec la non-concurrence des acteurs. Dans les deux cas d'exception, les données pourront éventuellement être mise à disposition si des traitements permettent de s'affranchir de ces contraintes (par exemple par de la cryptographie homomorphe, de l'anonymisation, de l'échantillonnage, etc.).

Annexes – Documents dossier de candidature

PTCC – Trame d'annexe technique du projet
PTCC – Annexe financière du projet
PTCC – Trame de présentation succincte du projet

— o —