

## Stratégie Nationale Cyber

### « Développement de technologies innovantes critiques »

#### Cahier des charges de l'appel à projets n°1

Le numérique est aujourd'hui présent dans tous les pans de la vie des Français. Support de nombreuses innovations qui bénéficient à chacun, il induit aussi des risques en matière de sécurité et de souveraineté. En outre, le développement du télétravail durant la crise sanitaire a contribué à rendre plus ténue la frontière entre les outils informatiques professionnels et personnels, augmentant d'autant la vulnérabilité des systèmes. Dans ce cadre, le gouvernement a souhaité, via la Stratégie Nationale Cyber, accompagner le développement de la filière française de la cybersécurité. À ce titre, cette stratégie visera à faire émerger des champions français de la cybersécurité, tant pour accompagner le développement d'une filière au potentiel économique important, que pour garantir à notre pays la maîtrise des technologies essentielles à la garantie de sa souveraineté.

À l'horizon 2025, l'objectif assigné à cette stratégie est l'atteinte d'un chiffre d'affaires de 25 Md€ pour la filière (soit un triplement du chiffre d'affaires actuel), le doublement des emplois dans le secteur en passant de 37 000 à 75 000 emplois et l'émergence de trois licornes françaises en cybersécurité. Pour cela, elle s'articule autour de 5 axes :

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

Cet appel à projets s'inscrit dans l'axe 1 de la stratégie et vise à soutenir le développement de briques technologies innovantes et critiques en cybersécurité. Il participera toutefois aussi à l'atteinte des objectifs de l'axe 2 de la stratégie, puisqu'il peut permettre de financer des projets collaboratifs entre les acteurs de la filière.

### Calendrier

- **Le dépôt des dossiers se clôture le 15 octobre 2021 à 12h00 (heure de Paris).**
- Les sélections pour audition seront finalisées le 29 octobre 2021.
- Les auditions se tiendront la semaine du 1<sup>er</sup> novembre 2021.

- Pour les projets aux enveloppes totales supérieures à 7,5M€, le dossier final complet sera à déposer avant le 5 décembre 2021.

## **1. Contexte et objectifs de l'appel à projet**

### **1.1. Action globale « Développement de technologies innovantes critiques »**

L'offre française en cybersécurité comporte des lacunes en ce qui concerne la maîtrise de certaines technologies clés, comme en font état plusieurs initiatives (action « technologies clés » de la revue stratégique de cyberdéfense, feuille de route de l'ANSSI<sup>1</sup>, feuille de route du projet « cybersécurité et sécurité de l'IoT » du Comité Stratégique de Filière « Industries de sécurité » par exemple).

Les technologies ainsi identifiées sont critiques du fait de leur sensibilité en termes de sécurité et appellent autant que possible des solutions souveraines. En outre, elles représentent un marché potentiel de taille pour les acteurs français.

Le développement de solutions innovantes de confiance et souveraines sur ces briques doit donc être une priorité de la stratégie d'accélération. C'est ce que vise à permettre cet appel à projets (AAP) en cofinçant des projets de recherche et développement portant sur des briques technologiques innovantes et critiques en cybersécurité. Pour ce faire, une liste de thématiques de travail a été constituée (voir annexe 1). Au terme du présent AAP, la liste des thématiques sera amendée et une nouvelle phase de soumission de projets sera lancée.

Les thématiques proposées s'articuleront autour de 4 axes :

1. la protection des infrastructures critiques à l'heure des nouveaux usages (OIV/OSE notamment) ;
2. la protection des collectivités locales, startups/PME et télétravailleurs ;
3. la sécurité de l'IoT ;
4. les briques technologiques critiques spécifiques à certains secteurs clés.

### **1.2. Nature des projets attendus**

Les projets visant au développement de technologies innovantes critiques sont des projets de R&D en cybersécurité adressant les thématiques détaillées dans l'annexe 1.

Les projets peuvent être conduits par (au choix) :

- Une entreprise, porteur unique ;
- un consortium qui rassemble des partenaires industriels ;
- un consortium qui rassemble des partenaires industriels et des partenaires de recherche<sup>2</sup>.

Ils correspondent à des assiettes de travaux d'un montant supérieur à **1 million d'euros**. Cette limite inférieure **pourra être abaissée à 500 000 € dans le cas d'un projet porté par une jeune pousse** au sens de la définition adoptée pour le régime exempté relatif aux aides en faveur des PME (SA.59106).

<sup>1</sup> liée notamment à la qualification de produits et services.

<sup>2</sup>Dont les IRT, ITE. Des projets financés dans le cadre de ces structures pourront ainsi être cofinancés.

Sont notamment éligibles les dépenses de personnels affectés au projet, identifiés et appartenant aux catégories suivantes : chercheurs, ingénieurs et techniciens, les amortissements d'équipements et de matériels de recherche et les travaux sous-traités à des laboratoires publics ou privés<sup>3</sup>.

Les travaux de R&D représentant moins de 5 % de l'assiette de dépenses du projet ou, dans le cas d'un consortium, ayant une contribution faible à son caractère collaboratif ont vocation à être pris en charge soit directement par les entreprises, soit en sous-traitance.

Les établissements de recherche ne peuvent être pilotes des projets.

## **2. Critères d'éligibilité**

Pour être éligible, le projet déposé à cet AAP doit satisfaire simultanément aux critères suivants :

### **Dossier**

1. être soumis, dans les délais, sur [l'extranet des Projets Innovants Collaboratifs](#) de Bpifrance ;
2. compléter un dossier de candidature complet, au format imposé ;

### **Projet**

3. respecter l'objet de l'AAP et s'inscrire dans l'un des domaines d'application identifiés dans l'annexe 1 ;
4. présenter un total de dépenses éligibles situé entre 1M€ (500k€ pour les jeunes pousses) et 15M€ ;
5. présenter une durée minimale de 12 mois et maximale de 36 mois ;
6. porter sur des travaux fortement innovants de recherche et développement en cybersécurité réalisés en France et non commencés (*i.e.* seul les coûts postérieurs à la demande seront éligibles à une aide) avant le dépôt de la demande d'aide ;

<sup>3</sup> Liste non exhaustive.

## **Porteur**

7. être déposé par (au choix) :
  - a. une entreprise, porteuse unique ;
  - b. un consortium, dont le chef de file est un industriel, pouvant impliquer d'autres industriels et des acteurs de la recherche (dans le respect d'au moins 20% des travaux réalisés par des PME et qu'aucun membre du consortium ne soit destinataire de moins de 5% du coût total du projet) ;
8. être porté par une société immatriculée en France au registre du commerce et des sociétés (RCS) à la date de dépôt du dossier ;
9. être porté par une entreprise à jour de ses obligations fiscales et sociales. Si l'entreprise est « entreprise en difficulté » selon le droit européen, son projet ne sera considéré comme éligible et donc instruit que si elle présente lors du dépôt de son dossier des éléments probants et jugés satisfaisants par Bpifrance justifiant sa sortie du statut d'« entreprise en difficulté » avant la décision sur le financement potentiel.

Les projets ne respectant pas l'un des critères d'éligibilité sont écartés du processus de sélection, sans recours possible.

## **3. Organisation et financement des projets**

### **3.1. Organisation du consortium (le cas échéant)**

Un accord de consortium portant sur tous les aspects liés à la réalisation du projet et notamment les règles applicables en matière de propriété intellectuelle, devra être préparé le plus tôt possible. La présentation d'un accord de consortium signé est indispensable au premier versement de l'aide.

Est appelé « partenaire du projet » toute entité signataire de l'accord de consortium. Il est rappelé qu'un partenaire du projet n'est pas forcément bénéficiaire direct d'aide : soit parce qu'il est financé en tant que sous-traitant, soit parce que ses dépenses ne sont pas éligibles ou retenues, soit parce qu'il n'a pas demandé de financement. Dans ces cas, il s'agit d'un partenaire non-bénéficiaire.

Chaque bénéficiaire d'une aide sera signataire d'une convention bilatérale avec Bpifrance. Les partenaires non-bénéficiaires n'auront pas de convention, mais en tant que membres du consortium, ils pourront être associés aux actions de communication du projet.

Le consortium doit être constitué de manière à ce que les conditions suivantes soient respectées (toute demande de dérogation devra être dûment justifiée) :

- Au moins 20% des coûts éligibles correspondent à des travaux réalisés par des PME ;
- Aucun bénéficiaire ne doit être concerné par moins de 5% du coût total du projet.

## 3.2. Financement octroyé

### 3.2.1. Coûts éligibles à cet AAP

Les dépenses liées au projet sont à présenter hors taxe et selon la ventilation requise dans l'annexe financière du projet en annexe 2 du dossier de candidature

Les coûts éligibles correspondent entre autres aux :

- **Salaires de personnel interne ;**
- **Frais connexes forfaitaires<sup>4</sup> ;**
- **Coûts communs :**
  - Études de faisabilité ou d'intégration des traitements sur les données hétérogènes,
  - Études permettant d'élaborer les méthodes d'évaluation et de recueil des données et sur les enjeux de sécurité,
  - Études permettant d'élaborer un modèle économique sur les données,
  - Collecte, validation, stockage, partage, exploitation des données recueillies,
  - Synthèse des résultats et leur communication,
  - Animation et coordination du projet,
  - Transfert des résultats aux autorités publiques.
- **Infrastructures :**
  - Équipements rendus nécessaires sur l'infrastructure,
  - Surcoûts d'exploitation rendus nécessaires par l'intégration du service ou de la captation des données.
- **Coûts de sous-traitance (max 30%)**
- **Contribution aux amortissements, frais de mission directement liés au projet, autres coûts (achats, consommables, etc.)**

Les dépenses seront éligibles à l'AAP uniquement si elles ne sont pas déjà financées par un ou des acteurs publics (Métropoles, Régions, EPCI, Europe notamment).

Les dépenses ne peuvent être prises en compte qu'à compter de la date de relève du dossier (cf. processus de sélection), étant entendu que les dépenses engagées avant la notification des conventions d'aide par Bpifrance le sont au risque des bénéficiaires.

L'ensemble des coûts relatifs au projet doit être détaillé dans le dossier de demande d'aide. L'instruction permet notamment de déterminer les coûts éligibles et retenus pour le financement par le Programme d'Investissements d'Avenir (PIA).

Par ailleurs, le quatrième programme d'investissements d'avenir participe au plan « France relance » de 100 Md€ pour la période 2021-2022, ayant vocation à être financé à hauteur de 40 % par l'Union

<sup>4</sup> Les frais connexes sont les dépenses qui concourent à la réalisation du projet sans toutefois pouvoir être directement attribués à celui-ci et s'appliquent uniquement sur les dépenses de RDI. Le montant forfaitaire de ces dépenses est égal à 20 % des salaires de personnel internes.

européenne. Le présent AAP s'inscrit pleinement dans le cadre des mesures éligibles à cette part européenne, qui sont présentées dans le plan national de relance et de résilience (PNRR) de la France<sup>5</sup> et qui seront financées in fine via son outil, la « Facilité pour la reprise et la résilience » (FRR)<sup>6</sup>. Le soutien apporté au titre de cette facilité interviendra sous forme de remboursement à l'Etat des financements octroyés et non d'un financement direct auprès des bénéficiaires. En vertu de l'article 9 du règlement précité, ce soutien est toutefois conditionné par l'interdiction de bénéficier d'un autre soutien au titre d'autres programmes et instruments de l'Union couvrant les mêmes coûts. Dans ce contexte, le candidat pourra être amené à fournir des informations sur les autres sources de financement d'origine européenne mobilisées ou demandées pour son projet dans son dossier de candidature.

### **3.2.2. Taux d'aide pour les bénéficiaires soumis au secteur concurrentiel**

Dans le cas général, le régime d'aide retenu est le régime cadre exempté de notification N° SA.58995 relatif aux aides à la recherche, au développement et à l'innovation (RDI) dans le cadre du PIA.

La somme des financements publics doit respecter le taux d'aide maximal fixé par ce régime d'aide.

Sur la base de la classification des dépenses éligibles, Bpifrance détermine une aide pouvant aller jusqu'au maximum du taux permis par le régime d'aide.

Une fois le taux d'aide déterminé, l'aide elle-même sera composée de subventions et d'avances remboursables selon la répartition suivante<sup>7</sup> :

- Pour le développement expérimental : 60% de subvention / 40% d'avances remboursables
- Pour la recherche industrielle : 75% de subvention / 25% d'avances remboursables
- Pour la recherche fondamentale : 100% de subventions

**Les avances remboursables pourront être converties en subvention** lorsque les projets conduisent à des perspectives technologiques, d'industrialisation ou de structuration de l'écosystème et contribuant à terme aux **objectifs de la Stratégie cyber**.

### **3.2.3. Taux d'aide pour les autres bénéficiaires**

Pour les établissements publics et assimilés et les organismes de recherche et assimilés, **l'aide se fait sous forme de subvention.**

- Pour les établissements de recherche, quel que soit leur statut, et remplissant une mission d'intérêt général en consacrant une part prépondérante de leur activité à la R&D, les aides sont accordées sous forme de subvention dans la limite de 100% des coûts marginaux. Tout organisme de ce type peut néanmoins, s'il en fait la demande, être pris en charge à 50% des coûts complets. Le responsable légal de l'organisme doit préalablement attester sur l'honneur qu'il possède une comptabilité analytique lui permettant de justifier des coûts présentés dans l'assiette de dépenses. Cette demande est définitive pour l'ensemble des appels à projets de soutien public à la RDI. De ce fait, tout établissement de recherche ayant déjà bénéficié, pour un projet antérieur de la prise en charge de coûts complets au taux de 50% se verra obligatoirement appliquer cette modalité pour l'AAP.

<sup>5</sup> Sous réserve de sa validation par la Commission européenne et son adoption prévue à l'été 2021.

<sup>6</sup> Règlement (UE) 2021/241 du Parlement européen et du Conseil du 12 février 2021 établissant la facilité pour la reprise et la résilience.

<sup>7</sup> Ces ratios portent sur la composition de l'aide accordée et non sur le taux d'aide qui est déterminé en cohérence avec le régime RDI.

### 3.2.4. Date d'acceptation des coûts et début des projets

La date de début des projets et d'acceptabilité des coûts correspond à la date de relève du dossier (cf. processus de sélection) sous réserve de la sélection définitive. Aucun coût antérieur ne pourra être accepté.

### 3.2.5. Mise en œuvre, suivi des projets et allocation des fonds

Chaque bénéficiaire signe une convention avec Bpifrance. Cette convention précise notamment l'utilisation des crédits, le contenu du projet, le calendrier de réalisation, les modalités de pilotage du projet, le montant des tranches et les critères de déclenchement des tranches successives, les prévisions de cofinancement des projets, les conditions de retour financier pour l'état, les modalités de restitution des données nécessaires au suivi et à l'évaluation des investissements, et les modalités de communication.

La convention d'aide est signée dans le cas général dans un délai de 3 mois à compter de la date de signature de la décision du Premier ministre, sous peine de perte du bénéfice de la décision d'aide.

Le bénéficiaire met en place un tableau de bord comportant des indicateurs de suivi de l'avancement des projets et des résultats obtenus. Il le transmet régulièrement à Bpifrance selon les modalités prévues par la convention. Pour chaque projet soutenu, une réunion d'avancement est prévue, au moins annuellement. Organisée par Bpifrance le cas échéant, elle associe le Secrétariat général pour l'investissement (SGPI) et l'ensemble des ministères concernés. Cette réunion a pour objet de suivre la mise en œuvre du projet et notamment le niveau d'exécution budgétaire, l'avancement des opérations financées et le respect du planning.

Une fois le projet sélectionné, chaque bénéficiaire soutenu par le PIA est tenu de mentionner ce soutien dans ses actions de communication, ou la publication des résultats du projet, avec la mention unique : « Ce projet a été soutenu par le Programme d'Investissements d'Avenir et le Plan de Relance. », accompagnée des logos du Programme d'Investissements d'Avenir<sup>8</sup> et de France Relance<sup>9</sup>. L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires. Toute autre communication est soumise à l'accord préalable du bénéficiaire.

Le bénéficiaire est tenu de communiquer régulièrement à Bpifrance et à l'État les éléments d'informations nécessaires à l'évaluation de l'avancement du projet (performance commerciale, emplois créés, brevets déposés, effets environnementaux et énergétiques), ainsi qu'à l'évaluation *ex post* donc après réalisation du projet. Ces éléments, et leurs évolutions, sont précisés dans conditions générales de la convention d'aide entre Bpifrance et le bénéficiaire.



## 4. Critères de sélection et fixation du niveau de financement

Les dossiers retenus pour instruction seront **évalués selon les critères ci-dessous**.

### 4.1. Pertinence du projet

- Pertinence de la taille du projet et du dimensionnement des étapes conduisant à une exploitation commerciale future. Le projet mené présente une envergure appropriée pour obtenir des résultats en quantité suffisante pour être représentatifs et exploitables ;
- Pertinence des choix technologiques ;
- Caractère généralisable, à un coût global raisonnable, de la solution innovante développée dans le cadre du projet soumis et existence d'un marché pour ce type de solution rendant possible un fort impact économique ;
- Adéquation du projet avec les objectifs de la stratégie d'accélération cyber, notamment la capacité du projet à accroître l'autonomie nationale ou européenne en particulier au regard des enjeux de sécurité et de souveraineté dans le cyber espace.

### 4.2. Impact économique et social du projet

- Pertinence des objectifs commerciaux en exploitation, notamment sur l'adéquation du niveau d'équipement des infrastructures avec un déploiement massif futur ;
- Argumentation du modèle économique au regard d'un déploiement futur, qu'il s'agisse du modèle économique de l'entreprise commercialisant la solution ou de la viabilité économique pour les partenaires supportant une expérimentation ;
- Capacité de valorisation des travaux du projet notamment en termes de propriété intellectuelle (notamment brevets et licences) ;
- Capacité à faire progresser les connaissances sur les usages, les domaines de pertinence et l'acceptabilité des systèmes et des services ; Le projet doit présenter à cet égard des expérimentations menées avec de vrais usagers/clients.

### 4.3. Eco-conditionnalité du projet et responsabilité environnementale de l'entreprise

Les projets démontrent une réelle prise en compte de la transition écologique et solidaire et du développement durable. Les effets positifs attendus et démontrés du projet, du point de vue écologique et énergétique, sont utilisés pour sélectionner les meilleurs projets parmi ceux présentés, ou pour moduler le niveau d'intervention publique accordé au projet.

À cet effet, chaque **projet doit systématiquement expliciter sa contribution** à l'environnement, en présentant les effets quantifiés, autant que faire se peut, directs et indirects, positifs et négatifs, estimés pour les axes ci-dessous :

- utilisation, avec ou sans production, d'énergies renouvelables ;
- efficacité énergétique ;
- climat via la réduction des gaz à effet de serre (GES) ;
- pollution de l'air ;
- qualité de l'eau ;
- consommation des ressources ;
- réduction des déchets ;
- impact sur la biodiversité ;
- impact sociétal.



Les estimations des effets des projets s'appuient notamment sur des analyses du cycle de vie menées au niveau des produits, procédés ou équipements.

#### **4.4. Qualité de l'organisation du projet**

- Pertinence et complémentarité du partenariat (adéquation du nombre de partenaires aux enjeux du projet, synergie et valeur ajoutée de tous les partenaires) ;
- Gouvernance, gestion et maîtrise des risques inhérents au projet, par exemple, avancement du projet d'accord de consortium ;
- Adéquation du programme de travail et du budget avec les objectifs du projet (définition des jalons, des résultats intermédiaires et des livrables) ;
- Solidité du plan de financement du projet et robustesse financière des partenaires, notamment capacité financière à mener le projet ;
- Qualité des informations transmises : celles-ci apportent suffisamment de précision dans les références et les arguments pour permettre d'évaluer sérieusement les aspects techniques et scientifiques, la justification des coûts du plan de travail ainsi que les perspectives industrielles et commerciales.

#### **4.5. Impact de l'intervention publique**

- Caractère incitatif de l'intervention ;
- Effet de levier de l'intervention publique.

### **5. Composition des dossiers**

Le dossier de candidature complet est constitué des pièces suivantes :

- **ANNEXE 1 : Annexe technique (document au format Word)**
  - Une présentation du projet détaillant les objectifs, la description générale, le plan de travail, le budget prévisionnel, le partenariat, les retombées économiques et industrielles et les impacts du projet (30 pages environ) ;
  - Une description détaillée des tâches du projet sous forme de fiches de lot (1 page par lot) ;
  - Les présentations des partenaires détaillant l'actionnariat, l'activité actuelle et les financements de l'entreprise ; chaque projet devra préciser, pour chaque partenaire, son rôle au sein du projet, les compétences, méthodes et données qu'il apporte et qu'il met en commun entre acteurs du consortium et avec les autorités publiques, et ce que le projet peut lui apporter ;
- **ANNEXE 2 : Annexe financière (tableur Excel à remplir par chacun des partenaires)**
  - Comprenant un ensemble de données économiques et financières concernant le projet et l'entreprise et une déclaration de demande d'aide datée et signée par les représentants habilités du coordonnateur et des différents partenaires (version scannée).
- **ANNEXE 3 : Une présentation du projet sous forme de diapositives (format libre, 20 diapositives maximum)**

- **ANNEXE 4 : Fiche communication du projet en 1 page (document Word).**
- **ANNEXE 5 : Questionnaire relatif aux activités en lien avec des pays sanctionnés**
- **Un projet d'accord de consortium (le cas échéant) ;**
- **Un ensemble de documents administratifs détaillés dans le dossier de candidature.**

Les modèles de dossier de candidature et de base de données des coûts du projet, présentant notamment la liste exhaustive des documents à fournir, sont disponibles en téléchargement sur le site internet Bpifrance de l'appel à projets. Les projets incomplets ou ne respectant pas les formats de soumission ne sont pas recevables.

## **6. Processus de sélection**

Afin de retenir les meilleurs projets respectant l'ambition du PIA, **la procédure de sélection est menée par le Comité de Pilotage (Copil) de la Stratégie Nationale cyber** selon le déroulé suivant :

- Présélection des dossiers pour audition ;
- Audition des dossiers présélectionnés ;
- [Pour les dossiers dont l'enveloppe totale dépasse 7,5M€] Dépôt du dossier finalisé (suite aux demandes de précisions lors des auditions) ;
- Sélection des dossiers par le Copil de la Stratégie.

**L'instruction est conduite par Bpifrance, qui s'appuie sur les experts des ministères.** À l'issue de cette phase d'instruction, le Copil statue sur le financement des projets et les modalités de ce financement sur la base de l'instruction effectuée par Bpifrance. **La décision d'octroi de l'aide est prise par le Premier Ministre, sur proposition du Copil et avis du Secrétariat Général Pour l'Investissement.**

## **7. 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.

### **7.1. 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.

## **7.2. 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 importantes 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.

## **7.3. 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.).

## **8. Confidentialité**

Bpifrance s'assure que les documents transmis dans le cadre de l'AAP sont soumis à la plus stricte confidentialité et ne sont communiqués que dans le cadre de l'expertise et de la gouvernance du PIA, de la Stratégie Nationale de cybersécurité et du Grand Défi cybersécurité. L'ensemble des personnes ayant accès aux dossiers de candidatures est tenu à la plus stricte confidentialité.

Une fois le dossier sélectionné, les bénéficiaires sont tenus de mentionner le soutien apporté par le Programme d'investissements d'avenir dans leurs actions de communication et la publication de leurs résultats avec la mention unique « ce projet a été financé par le Gouvernement dans le cadre du plan de relance et du programme d'investissement d'avenir » et les logos de France Relance, du PIA et de Bpifrance.

Toute opération de communication doit être concertée entre le porteur et Bpifrance, afin de vérifier notamment le caractère diffusable des informations et la conformité des références au plan de relance, au PIA et à Bpifrance.

L'État se réserve le droit de communiquer sur les objectifs généraux de l'action, ses enjeux et ses résultats, le cas échéant à base d'exemples anonymisés et dans le respect du secret des affaires.

Enfin, les bénéficiaires sont tenus à une obligation de transparence et de *reporting* vis-à-vis de l'État et de Bpifrance, nécessaire à l'évaluation *ex post* des projets ou du plan de relance.

## **9. Soumission des projets**

Les projets peuvent être soumis pendant toute la période d'ouverture et dans la limite du budget alloué sur la plateforme de Bpifrance : <https://extranet.bpifrance.fr/projets-innovants-collaboratifs/>

Pour toutes questions relatives au dépôt du dossier sur la plateforme, Bpifrance peut être contacté directement : [grandsdefis@bpifrance.fr](mailto:grandsdefis@bpifrance.fr)

Pour toutes questions relatives à l'appel à projets, le Directeur de programme peut être contacté directement : [aap-technos-cyber.dge@finances.gouv.fr](mailto:aap-technos-cyber.dge@finances.gouv.fr)

Pour toutes questions relative à la Stratégie Nationale cyber ou dépassant le cadre de cette appel à projets, le coordinateur de la Stratégie peut être contacté directement : [strategie.cyber@pm.gouv.fr](mailto:strategie.cyber@pm.gouv.fr)

## Annexe 1 : Thématiques des projets attendus

### 1. Développement de briques de sécurisation des outils de communication à distance et collaboratifs

La crise sanitaire liée à l'épidémie de la Covid-19 et le confinement qui s'en est suivi ont mis en exergue l'importance des technologies de travail à distance et la dépendance de la France à l'égard des grands acteurs américains. Si des acteurs français existent, force est de constater que ces derniers n'occupent pas une place centrale sur le marché français.

Cette dépendance apparaît problématique dès lors que ces technologies sont essentielles au maintien de la vie économique du pays et à l'enseignement à distance. En outre, les données pouvant transiter sur ce type de plateformes peuvent s'apparenter à des données sensibles, notamment s'agissant de plateformes de télémédecine ou lorsqu'elles sont utilisées dans un cadre professionnel.

Dans le cadre des travaux de la revue stratégique de cyberdéfense, la maîtrise des technologies relatives à la sécurisation des échanges *via* les messageries instantanées, les systèmes de visioconférence et les plateformes de travail collaboratif a été estimée insuffisante au niveau national. Alors que cette problématique apparaît de plus en plus prégnante du fait de la multiplication des usages, il est apparu pertinent de conduire des travaux sur ce thème au travers de la stratégie d'accélération cyber.

Cette thématique s'inscrit dans le second axe de travail de cet AAP : *la protection des collectivités territoriales, startups/PME et télétravailleurs*.

Les projets soutenus devront avoir un niveau initial de TRL (*Technology Readiness Level*<sup>10</sup>) égal au moins à 4 et viseront un niveau de TRL en fin de projet au moins égal à 7.

### 2. Développement de technologies de chiffrement innovantes

Face à l'inflation de la quantité de données échangées, la nécessité de développer de nouvelles technologies de chiffrement est un besoin crucial pour garantir la souveraineté de notre pays.

Il s'agit notamment de soutenir le développement de solutions permettant des traitements sur les données chiffrées ou de maîtriser le chiffrement côté client pour tout type de données (structurées et non structurées). Ces solutions pourront par exemple s'appuyer sur des mécanismes de type ABE (*attribute-based encryption*) permettant la mise en place de contrôle d'accès et de politique de « besoin d'en connaître » sur la base d'attributs comme l'entité d'appartenance ou le rôle.

Il s'agit aussi de soutenir le développement de briques de chiffrement robustes et à bas coût dédiées à l'IoT (besoin identifié dans le cadre de la revue stratégique de cyberdéfense). La

<sup>10</sup> Qualifie le niveau de maturité d'une technologie.

problématique de la sécurisation de l'IoT est en effet patente : ils sont pleinement intégrés au sein de systèmes critiques et ne peuvent, de par leur faible prix de vente et leurs capacités de traitement limitées, intégrer des systèmes complexes de sécurisation.

Ces deux sujets s'intègrent respectivement dans le premier axe de cet appel à projets : *la protection des infrastructures critiques à l'heure des nouveaux usages (OIV/OSE notamment)*, ainsi que dans le troisième : *la sécurité de l'IoT*.

Les projets soutenus devront avoir un niveau initial de TRL égal au moins à 4 et viseront un niveau de TRL en fin de projet au moins égal à 7.

### **3. Développement de solutions associant cybersécurité et sûreté de fonctionnement à l'interface entre systèmes cyber et physiques**

La première exigence des systèmes industriels est la sûreté de fonctionnement, c'est-à-dire la disponibilité et la fiabilité des opérations, la maîtrise des pannes dangereuses, etc. L'utilisation croissante des TIC (Technologie de l'Information et de la Communication) dans ces systèmes a nécessité l'élaboration de processus de développement et d'assurance particuliers, formalisés dans des référentiels aujourd'hui reconnus.

La cybersécurité constitue pour ces systèmes un nouvel enjeu : une vulnérabilité cyber peut induire un défaut du système et impacter leur sûreté de fonctionnement. Il apparaît donc nécessaire de développer des dispositifs qui associent ces deux enjeux au profit des systèmes les plus critiques (transports, énergie, moyens de production, etc.).

Au travers de cet appel à projets, le développement de solutions associant sûreté de fonctionnement et cybersécurité en incluant l'enjeu du maintien de qualification dans le temps (gestion des mises à jours, déploiement de certificats, système de journalisation, etc.) et adaptées à certains secteurs spécifiques est donc soutenu.

Cette thématique s'intègre dans les axes *protection des infrastructures critiques à l'heure des nouveaux usages (OIV/OSE notamment)* et *briques technologiques critiques spécifiques à certains secteurs clés*.

Les projets soutenus devront avoir un niveau initial de TRL égal au moins à 4 et viseront un niveau de TRL en fin de projet au moins égal à 7.

### **4. Développement de solutions de cybersécurité pour la sécurité des grands événements**

La sécurisation des grands événements, et en particulier la sécurisation des Jeux Olympiques et Paralympiques de Paris 2024 (JOP 2024) a fait l'objet d'un projet structurant du contrat de filière du CSF « Industries de sécurité ».

Si une large partie de ces travaux ont vocation à être portés par des budgets propres au ministère de l'intérieur et au Comité d'organisation des jeux olympiques et paralympiques

d'été de 2024, certains projets relatifs au développement de solutions innovantes de cybersécurisation pourront être soutenus par la stratégie d'accélération cyber.

Pour prendre en compte les enjeux calendaires liés à l'imminence des JOP 2024, les projets soutenus dans le cadre de cette thématique devront viser un niveau de TRL en fin de projet élevé de l'ordre de 8 et le niveau initial devra être supérieur à 4. Une attention particulière sera portée à la cohérence de la planification du projet avec le calendrier des JOP 2024 ainsi que la capitalisation sur les travaux déjà effectués dans le domaine.