GOUVERNEMENT
Liberté
Égalité
Fraternité

Stratégie Nationale de Cybersécurité

Grand Défi cybersécurité

Appel à projets
« Mutualisation et valorisation des données d'intérêt cyber »
Cas d'usage n°1 : Cyber Threat Intelligence
(AAP MVDC-CTI)

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, renforçant 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. A 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 maitrise des technologies essentielles à la garantie de sa souveraineté.

A 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 Etat), 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 les axes 1 et 2 de la stratégie et vise à soutenir l'émergence d'un « socle commun » pour la mutualisation et la valorisation des données d'intérêt cyber basé sur des cas d'usage spécifiques, ici la *Cyber Threat Intelligence*.

Calendrier

- **Le dépôt des dossiers se clôture le 16 novembre 2021 à 12h00 (midi heure de Paris).**
- La phase de pré-sélection s'achèvera le 8er décembre 2021.
- A l'issu, les porteurs des dossiers pré-sélectionnés seront mis en relation et invités à déposer les éléments finaux de leurs dossiers avant le 18 février 2022 à 12h (midi heure de Paris).
- Les auditions pour les projets pré-sélectionnés seront la semaine du 28 février 2022.
- La sélection définitive est prévue pour avril 2022.

Les projets doivent être adressées exclusivement sous forme électronique sur l'extranet de Bpifrance à l'adresse https://extranet.bpifrance.fr/projets-innovants-collaboratifs/ et peuvent être soumis pendant toute la période d'ouverture. Ils seront évalués après la date de clôture.

Pour toutes questions relatives à l'appel à projets, le Directeur de programme peut être contacté directement : gd.cyber@pm.gouv.fr

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

1 - CONTEXTE ET OBJECTIFS DE L'APPEL A PROJETS

A. ACTION GLOBALE « MUTUALISATION ET VALORISATION DES DONNEES D'INTERET CYBER »

La mesure 7 de la Stratégie Nationale de Cybersécurité, sur la base de l'axe transverse de la feuille de route du Grand Défi cybersécurité sur les données, et s'appuyant également sur les différentes réflexions dans le cadre du Contrat Stratégique de Filière « Industrie de Sécurité » (CSF) et du Campus Cyber, a vocation à faire émerger un « socle commun » de mutualisation et de valorisation des données d'intérêt cyber ayant une ambition européenne à terme.

Cette démarche est alimentée par le constat de l'importance et de la valeur croissante des données à l'heure du « big data » et du « machine learning ». En cybersécurité en particulier, l'enjeu est triple. D'une part, les données représente une richesse qu'il convient de protéger et de valoriser. Ensuite, les données sont un élément à présent essentiel pour favoriser l'innovation, par exemple pour l'expérimentation. Enfin, les données et leur qualité représentent déjà un différentiant technologique et bientôt les meilleures solutions se baseront sur les modèles les mieux entrainés.

La série d'appels à projets (AAP) « Mutualisation et valorisation des données d'intérêt cyber » (MVDC), chacun centré sur un cas d'usage différent, vise à soutenir des projets de R&D adressant simultanément deux aspects : la mutualisation de différentes sources de données et la valorisation de ces données (par exemple par application de « machine learning »). **L'objectif de l'ensemble des AAP MVDC est de capitaliser de manière incrémentale et concertée sur les développements spécifiques des cas d'usage successifs pour faire émerger un socle commun**. Celui-ci pourra inclure des aspects matériels, logiciels, commerciaux, de normes et standards, etc. [Cf. Annexe 1].

Ce « socle commun » sera défini conjointement et progressivement avec les porteurs des projets retenus. Chaque projet devra apporter sa brique à l'édifice sous diverses formes possibles [cf. Annexe1].

B. CONTEXTE DU CAS D'USAGE « CYBER THREAT INTELLIGENCE »

Le premier cas d'usage choisi pour la série des AAP MVDC est la *Cyber Threat Intelligence* au sens large. Il s'agit à la fois d'un sujet fortement centré sur les données et d'un enjeu critique identifié dans la feuille de route du Grand Défi cyber.
En effet, ce sujet est essentiel à la fois pour la modélisation des risques et pour la contextualisation des alertes, mais aussi pour la détection des attaques. La consolidation de ce secteur de la cybersécurité sur lequel plusieurs acteurs se positionnent est crucial pour pouvoir disposer d'une chaine complète partant de données brut et allant jusqu'à un flux à forte valeur ajoutée.

C. OBJET DE L'AAP MVDC-CTI

Le choix des pouvoir publics est de sélectionner un **nombre limité de projets**, de taille critique suffisante, disposant de la **meilleure gouvernance entre les partenaires du projet, mais aussi avec les autres projets et les pouvoirs publics**, afin d'exploiter au maximum les synergies entre les cas d'usages et la mutualisation des compétences nécessaires à la R&D. Ainsi, **l'assiette totale éligible de chaque projet proposé devra se situer entre 2 millions et 9 millions d'euros.**

i. Domaine d'application

L'objectif de l'AAP MVDC-CTI est de pouvoir retenir un ou plusieurs projets couvrant le domaine de la « Cyber Threat Intelligence » (CTI) et **permettant d'amorcer la création d'un « socle commun » (un standard, une base logicielle, éventuellement une base matérielle, un modèle économique, etc.) entre ces derniers et sur lequel pourront capitaliser les futurs AAP MVDC**.

L'AAP vise les projets de R&D qui peuvent contribuer simultanément à :

- La mutualisation et la fusion de données hétérogènes applicables à la CTI ;
- La production de données de CTI valorisées et éventuellement leur application ;
- La construction d'un « socle commun » pour la mutualisation et la valorisation des données d'intérêt cyber.

Le TRL[1] global attendu en fin de projet doit être situé entre 7 et 9. Néanmoins, il est fortement encouragé d'aborder des sujets de recherche plus amonts qui impact le projet et sont susceptibles de contribuer au « socle commun ». A titre d'exemple, les sujets suivants peuvent être de bon candidats :

- Protection de la vie privée ;
- Fusion de données ;
- Modélisation et représentation abstraite des données ;
- Apprentissage sur données anonymisées, voire chiffrées ;
- Traitement automatique du langage naturel pour exploiter les données textuelles ;
- Génération de données afin de compléter des jeux de données imparfaits ;
- Architecture innovante (ex : distribuée) pour les données.

Les projets proposés devront présenter une durée d'un minimum de 12 mois et au maximum de 36 mois.

ii. Partage et accessibilité du « socle commun » et des connaissances acquises

D'une part, les projets permettent de développer et diffuser un « socle commun » pour les acteurs, fondé sur un partage des résultats du projet, et notamment des retours d'expérience, afin d'aboutir à une **vision partagée** des enjeux, des méthodes de conception (amont) et d'évaluation (aval) sur la mutualisation et la valorisation des données d'intérêt cyber.

[1] TRL : *Technology readiness level*, qualifie le niveau de maturité d'une technologie.

Ces éléments constituent pour l'essentiel un « socle commun » à l'ensemble des acteurs de la filière cybersécurité.

D'autre part, il est demandé que les projets proposent des modalités (périmètre des connaissances partagées / acteurs ayant accès à ces connaissances / conditions d'accès) :

- De mise en commun, **au sein du consortium** :
    - des données le permettant (en cas de limitation, préciser les données concernées par le partage),
    - des méthodes,
    - des résultats,
    - du « socle commun » développé ;
- De partage et mise en commun des méthodes, **entre les projets** retenus pour financement :
    - des données le permettant (en cas de limitation, préciser les données concernées par le partage),
    - des résultats,
    - du « socle commun ».
- De partage **avec les autorités publiques** pour l'élaboration des réglementations et plus largement des politiques publiques :
    - des données le permettant (en cas de limitation, préciser les données concernées par le partage),
    - des méthodes,
    - des résultats,
    - du « socle commun ».

iii. Eléments imposés

Il sera essentiel de capitaliser sur les standards et outils (notamment OpenSource) déjà existants et largement utilisés par la communauté cyber. Il sera ainsi nécessaire d'**expliquer l'articulation avec les différents standards actuels**, notamment les formats suivants :

- STIX : format de structuration des observables ;
- MAEC : format de structuration des codes ;
- OpenIOC : format de capitalisation ;
- Formats « de fait » pour les signatures complexes :
    - SURICATA, SNORT et Bro/Zeek pour le format des signatures réseau ;
    - YARA essentiellement pour les signatures systèmes ;
    - Sigma pour le format des évènements ;
- TAXII : format d'échange de la donnée ;
- Le framework Mitre ATT&CK.

Les interactions avec les plateformes suivantes seront également à expliciter :

- MISP ;
- OpenCTI.

Sur les aspects « Big Data », il sera également indispensable de s'appuyer sur les briques logicielles couramment utilisées (Hadoop, Spark, Kafka, etc.).

2 - CRITERES D'ELIGIBILITE

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 identifiées dans la section 1.C.i ;
4. présenter un total de dépenses situé entre 2M€ et 9M€ ;
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 ;

Porteur

7. être déposé par un consortium, dont le chef de file est un industriel, pouvant impliquer d'autres industriels, des acteurs de la recherche et des acteurs territoriaux (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

A. ORGANISATION DU CONSORTIUM

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 dument 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 coûts total du projet.

B. FINANCEMENT OCTROYE

i. Coûts éligibles à cet AAP

Les dépenses liées au projet sont à présenter hors-taxe et selon la ventilation requise dans les onglets « Annexe financière - coûts RI » (Recherche industrielle) et « Annexe financière - coûts DE (Développement expérimental) de l'« Annexe 2 - Dossier de financement » du dossier de candidature.

Les coûts éligibles correspondent entre autres aux :

- **Salaires de personnels internes ;**
- **Frais connexes forfaitaires[2] ;**
- **Coûts communs**
  - Études préalables pour la définition du « socle commun » (dont études juridiques),
  - 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.

[2] 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

- **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 pré-sélection du dossier, à la réception du dossier complet (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 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[3] et qui seront financées in fine via son outil, la « Facilité pour la reprise et la résilience » (FRR)[4]. 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.

ii. 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.

Pour les travaux concernant le « socle commun », l'aide sera composé exclusivement de subventions.

Pour le reste des travaux, une fois le taux d'aide déterminé, l'aide elle-même sera composée de subventions et d'avances remboursables selon la répartition suivante[5] :

- 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.

[3] Sous réserve de sa validation par la Commission européenne et son adoption prévue à l'été 2021.
[4] Règlement (UE) 2021/241 du Parlement européen et du Conseil du 12 février 2021 établissant la facilité pour la reprise et la résilience.
[5] 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.

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.**

iii. Taux d'aide pour les autres bénéficiaires

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

- Les collectivités territoriales peuvent être financées dans le cas où des travaux de R&D spécifiques pour le projet leur incombent avec application d'un taux d'aide pouvant aller au maximum à 50% des dépenses éligibles et retenues du projet.

- 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 se verra obligatoirement appliquer cette modalité pour l'AAP MVDC-CTI.

iv. DATE D'ACCEPTATION DES COUTS ET DE DEBUT DES PROJETS

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

v. 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 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[6] et de France Relance[7]. 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'Etat 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 - CRITERES DE SELECTION ET DE FIXATION DU NIVEAU DE FINANCEMENT

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

A- 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 (en termes de durée, quantité de données traitées, etc.) pour obtenir des résultats en quantité suffisante pour être représentatifs et exploitables.
- Pertinence de la typologie des données traitées.
- Pertinence des choix technologiques.
- Présence de ressources et de méthodologies dans le projet d'analyses des impacts juridiques sur la captation et l'exploitation des données.
- Caractère généralisable, à un coût global raisonnable, de la solution innovante développée dans le cadre du projet soumis à la présence d'un marché rendant possible un fort impact économique.
- Adéquation du projet avec les objectifs de la stratégie d'accélération cyber, notamment la capacité du projet à accroitre l'autonomie nationale ou européenne en particulier au regard des enjeux de sécurité et de souveraineté dans le cyber espace.

B- 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. Les projets doivent permettre d'évaluer les impacts de la mutualisation et de la valorisation des données d'intérêt cyber.
- Le projet doit présenter à cet égard des expérimentations menées avec de vrais usagers/clients.
- Proposant un échantillon suffisamment représentatif du ou des usages et des enjeux de validation de la sécurité.

---

6 

7 

C- 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.

A 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.

D- 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, etc.
- 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.

E- Participation au « socle commun »

- Permettant d'alimenter le « socle commun » de mutualisation et valorisation des données d'intérêt cyber. Ceci se fera au travers des types de livrables mentionné en Annexe 1.
- Permettant d'alimenter une base de connaissances communes sur les usages et l'acceptabilité de ces systèmes et services.
- Permettant d'assurer une interaction forte avec les services de l'Etat. Les porteurs de projets devront notamment assurer la communication des méthodes et des résultats des expérimentations auprès des administrations spécialisées en cybersécurité.

F- Impact de l'intervention publique

- Caractère incitatif de l'intervention (cf. annexe 3.b).

- 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 : Dossier de financement (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 coordinateur et des différents partenaires (version scannée).

- **ANNEXE 3 : Une présentation du projet sous forme de diapositives (PowerPoint, 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 (version scannée et signée).**

- **ANNEXE 6 : Autorisation de mise en relation (version scannée et signée).**
- **Un projet d'accord de consortium.**
- **Un ensemble de documents administratifs, éléments détaillés dans le dossier de candidature.**

Le modèle du dossier de candidature présentant notamment la liste exhaustive des documents à fournir, est disponible 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 SELECTION

Afin de retenir les meilleurs projets respectant l'ambition du PIA, **la procédure de sélection est menée par le Comité Technique (Cotech) du Grand Défi cyber**.

1ère Phase (présélection)

Une fois les propositions de dossier déposées sur l'extranet de Bpifrance, une évaluation préliminaire des dossiers est effectuée par Bpifrance. Les projets retenus seront présentés par les porteurs et discutés lors d'auditions d'une heure face à un jury. Sur la base des avis du jury et de l'évaluation préliminaire, le Cotech présélectionne les dossiers les plus prometteurs et les mets en relation entre eux pour leur permettre de travailler sur la seconde phase.

2nde Phase (Sélection finale)

Sur la base des échanges lors des auditions, des recommandations du Cotech et des discussions qu'ils auront eues avec les autres porteurs présélectionnés, les porteurs de projets déposent leur dossier final sur l'extranet de Bpifrance en apportant *a minima* les nouveaux éléments suivants :

- Toutes précisions demandées par le jury ou le Cotech ;
- Les adaptations décidées par le(s) porteur(s) suites aux différents échanges ;
- Les contributions de chacun des dossiers retenus pour la seconde phase au « socle commun » et l'organisation inter-projets proposée (incluant le rôle de chacun, les questions de propriété intellectuelle, les conditions de mise à disposition, etc.) ;
- Eventuellement la fusion de différents projets retenus pour la seconde phase.

Sur la base de l'évaluation lors de la première phase et des nouveaux éléments apportés les projets sont choisis par le Cotech pour entrer en instruction approfondie. **Cette instruction est conduite par Bpifrance, qui s'appuie sur les experts des ministères.** À l'issue de cette phase d'instruction, le Cotech 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 Cotech et avis du Secrétariat Général Pour l'Investissement.**

7 - CONDITIONS SUR LES DONNEES

A l'heure du « big data » et du « machine learning » l'enjeu de disposer, de manière sécurisée, de données de qualité prend toute son importance. A ce titre, les éléments suivants seront **exigés de tous les projets recevant des financements étatiques dans le cadre de la Stratégie Nationale de cybersécurité.**

A. PROTECTION ET RESPECT DE LA REGLEMENTATION

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.

B. PRODUCTION, STOCKAGE ET VALORISATION DE DONNEES D'INTERET 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.

C. ACCES AUX DONNEES A DES FINS D'EXPERIMENTATION

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 - CONFIDENTIALITE

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'Etat 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'Etat 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 à l'appel à projets, le Directeur de programme peut être contacté directement : gd.cyber@pm.gouv.fr

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

Annexe 1 : Notion de « Socle commun »

La notion de « socle commun » au sens des AAP MVDC est relativement large. Elle peut inclure, sans que la liste soit exhaustive ou qu'un de ces éléments soit individuellement requis :

- Les définitions des termes et vocabulaire standards communs ;
- Des aspects matériels (plateformes ou architectures) mutualisables, généralisables ou extensibles
- Des aspects logiciel (briques, plateformes ou architectures) mutualisables, généralisables ou extensibles
- Des aspects normatif (développement de standards, de normes ou autres éléments permettant de donner un cadre à l'interopérabilité des solutions dans le domaine)
- Une modélisation permettant une abstraction généralisable
- Des données partagées
- Un modèle économique permettant le partage
- Une organisation ou une gouvernance commune
- Une démarche partenarial extensible
- Un cadre juridique pertinent permettant le partage et les échanges

Dans tous les cas, le « socle commun » doit participer à mettre en avant la valeur des données et à faciliter leur utilisation en cybersécurité.