Conseil de site
Séance du 19 décembre 2023

Délibération n°3
Portant approbation de l'accord de consortium « TAL-CYB » entre le Campus Cyber et CY Cergy Paris Université dans le cadre du projet AMI CMA « TAL-CYB »

Vu le code de l'éducation ;
Vu l'ordonnance n° 2018-1131 du 12 décembre 2018 relative à l'expérimentation de nouvelles formes de rapprochement, de regroupement ou de fusion des établissements d'enseignement supérieur et de recherche ;
Vu le décret n°2019-1095 du 28 octobre 2019 portant création de CY Cergy Paris Université et approbation de ses statuts ;
Vu la convention attributive d'aide n° ANR-23-CMAS-0020, conclue en date du 27 juin 2023 entre l'Agence nationale de la recherche et le Campus Cyber ;
Vu la délibération n°9 du conseil d'établissement du 28 novembre 2023 portant avis sur la signature de l'accord de consortium TAL-CYB ;

Considérant qu'un appel à manifestation d'intérêt « Cybersécurité » a été lancé en 2022 et que le jury a refusé les projets déposés séparément par le Campus Cyber et par CY Cergy Paris Université,

Considérant qu'un nouveau projet a été soumis conjointement par le Campus Cyber et un consortium composé de douze (12) partenaires, dont CY Cergy Paris Université, dans un périmètre et une enveloppe budgétaire plus restreints,

Considérant que le projet a été sélectionné par l'Agence nationale de la recherche (ANR) ; qu'il prévoit de mettre en place de nouvelles formations en cybersécurité et de produire des contenus audiovisuels pour sensibiliser le plus grand nombre sur la question de la cybersécurité,

Considérant qu'il convient de mettre en œuvre le financement ; qu'à cet effet les partenaires ont l'obligation de signer un accord de consortium afin de définir, notamment, les modalités de fonctionnement de tous les partenaires,

Après en avoir délibéré :

Vote

Nombre de membres en exercice : 32	Pour : 21
Nombre de membres présents : 19	Contre : 0
Nombre de membres représentés : 2	Abstention : 0
Membres absents et non représentés : 11	Non-participation : 0

Article 1er :

Le conseil de site approuve la signature, par le président de CY Cergy Paris Université, de l'accord de consortium TAL-CYB tel qu'annexé à la présente délibération.

Article 2 :

La présente délibération sera transmise au recteur de la région académique d'Ile-de-France, chancelier des universités, et entrera en vigueur à compter de sa publication.

Article dernier :

La directrice générale des services et l'agent comptable de l'université sont chargés, pour ce qui les concerne, de l'exécution de la présente délibération.

Le président de CY Cergy Paris Université,

Laurent GATINEAU

Transmise au rectorat le : 22 décembre 2023
Publiée le : 22 décembre 2023

En application de l'article R. 421-1 du code de justice administrative, la présente délibération peut faire l'objet d'un recours devant le tribunal administratif de Cergy-Pontoise dans un délai de deux mois à compter de sa publication et de sa transmission au recteur, en cas de délibération à caractère réglementaire.

ENTRE LES SOUSSIGNEES

La Société CAMPUS CYBER, SAS au capital de 8 910 000 euros, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le numéro B 892 343 633, dont le siège social est situé au 5-7 rue Bellini 92800 Puteaux, représentée par Michel Van den Berghe, Président.

CI-DESSOUS DENOMMEE : « CAMPUS CYBER »

D'UNE PART

ET

La Société Root me PRO, SAS au capital de 4 000 euros, immatriculée au Registre du Commerce et des Sociétés de Lyon sous le numéro 878 403 906, dont le siège social est situé au 29 B Chemin de Grave 69450 Saint Cyr au Mont d'or, représentée par Sébastien Dartilalongue, Directeur Général

CI-DESSOUS DENOMMEE : « ROOT ME PRO »

L'association Women4Cyber France, déclarée depuis le 13 juillet 2021 sous le numéro W423014177, dont le siège social est situé au 9 rue du Moulin 42290 Sorbiers, représentée par Valéria Muntia, Présidente.

CI-DESSOUS DENOMMEE : « WOMEN4CYBER »

La fondation CGénial, reconnue comme établissement d'utilité publique au JO du 21 août 2006,
SIRET 49305066000023, dont le siège est situé : 20 avenue Rapp, 75007 Paris
et représentée par Hélène Chahine en qualité de : Déléguée générale

CI-DESSOUS DENOMMEE : « CGENIAL»

La Société Radio France, SA à conseil d'administration au capital de 92 795 391 euros, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro

326 094 471, dont le siège social est situé au 116 avenue du Président Kennedy 75220 Paris cedex 16, représentée par Sibyle Veil, Présidente.

CI-DESSOUS DENOMMEE : « RADIO FRANCE »

L'établissement public national à caractère administratif CNED (centre national d'enseignement à distance), au capital de XXX euros, immatriculée au Registre du Commerce et des Sociétés XXX sous le numéro XXX, dont le siège social est situé au 2 boulevard Nicéphore Niepce 86360 Chasseneuil du Poitou, représenté par Jean-Noël Tronc, Directeur général.

CI-DESSOUS DENOMME : « CNED »

Le groupement d'intérêt public PIX au capital de XXX euros, immatriculée au Registre du Commerce et des Sociétés XXX sous le numéro XXX, dont le siège social est situé au XXX, représenté par Benjamin Marteau, Directeur.

CI-DESSOUS DENOMME : « PIX »

L'ONISEP (office national d'information sur les enseignements et les professions), établissement public national à caractère administratif, dont le siège social est situé au 12 mail Barthélémy Thimonnier 77437 Marne-la-Vallée cedex 2, représenté par Frédérique Alexandre-Bailly, Directrice générale.

CI-DESSOUS DENOMME : « ONISEP »

Class'Code, association déclarée depuis le 11 mars 2020 sous le numéro W691101990, dont le siège social est situé au 43 boulevard du Onze Novembre 1918 69100 Villeurbanne, représentée par Bastien Masse, Délégué général.

CI-DESSOUS DENOMMEE : « CLASS CODE »

L'académie de Versailles, chargée du déploiement de la politique éducative du gouvernement dans les départements de l'Essonne, du Val-d'Oise, des Hauts de Seine et des Yvelines, représenté par Etienne Champion, recteur de l'académie.

CI-DESSOUS DENOMMEE : « ACADEMIE DE VERSAILLES »

CY Cergy Paris Université, établissement public national à caractère scientifique culturel et professionnel, dont le siège social est situé au 33 boulevard du Port 95011 Cergy Pontoise, représentée par Laurent Gatineau, président.

CI-DESSOUS DENOMMEE : «CY CERGY PARIS UNIVERSITE »

L'université Paris 1 Panthéon-Sorbonne, établissement public national à caractère scientifique culturel et professionnel, dont le siège social est situé au 12 place du Panthéon 75231 Paris Cedex 05, représentée par Christine Néau-Leduc, Présidente.

CI-DESSOUS DENOMMEE : « UNIVERSITE PANTHEON-SORBONNE »

L'université Sorbonne Paris Nord (Paris XIII), établissement public national à caractère scientifique culturel et professionnel, dont le siège social est situé au 99 Av. Jean Baptiste Clément, 93430 Villetaneuse, représentée par Christophe Fouquéré, Président.

CI-DESSOUS DENOMMEE : « UNIVERSITE PARIS NORD »

D'AUTRE PART

Ci-dessous dénommées collectivement les Parties ou les Partenaires ou individuellement la Partie ou le Partenaire.

Table des matières

***

Article 1. PRÉAMBULE

1. Les Partenaires ont mis en place un projet collaboratif dénommé « TAL-CYB » afin d'exécuter ensemble des travaux pour répondre aux enjeux d'attractivité, d'orientation et de formation pour la filière cybersécurité.

Il est ici précisé que les Partenaires reçoivent un soutien pour la réalisation du Projet, via des fonds publics.

2. Les objectifs que se sont assignés les Partenaires au titre du Projet sont détaillés en annexe « Description du Projet » (reprise du document de soumission auprès de l'ANR).

1. CAMPUS CYBER est un acteur de référence et le lieu totem de la cybersécurité en France. Il apporte dans le Projet sa connaissance de l'écosystème cybersécurité. Il coordonne les travaux du consortium, contribue à leur mise en visibilité et réalise des contenus d'attractivité et de formation, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

2. ROOT ME PRO est une plateforme de service spécialisée dans le hacking éthique. Elle apporte dans le Projet son savoir-faire en création et animation de séquence de mode de jeu du type "Capture The Flag" et d'autres exercices disponibles sur sa plateforme, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

3. RADIO FRANCE est l'entité qui gère les stations de radio publiques françaises. Elle apporte dans le Projet son savoir-faire dans la création de programme, de contenus de types podcast, de stratégie de diffusion et le matériel nécessaire, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

4. CGENIAL est une fondation qui œuvre au rapprochement du monde des sciences, des technologies et des métiers associés et des élèves. Elle apporte dans le Projet sa connaissance préalable du terrain et son savoir-faire dans la création et l'animation d'ateliers dans les écoles et établissements, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

5. WOMEN4CYBER est une association qui vise à promouvoir la place des femmes dans la filière cybersécurité. Elle apporte dans le Projet sa capacité à développer des formats destinés à sensibiliser sur la féminisation des métiers, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

6. PIX est un groupement d'intérêt public qui opère une plateforme d'évaluation des compétences numériques des élèves et étudiants. Elle apporte au Projet sa capacité à densifier son référentiel de compétences cybersécurité et à produire des parcours d'évaluation qui y sont adossés, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

7. ONISEP est l'opérateur de référence qui produit et diffuse des informations sur l'orientation (métiers et formation) à destination des élèves, enseignants et parents à l'échelle nationale. Il apporte dans le Projet son savoir-faire et ses outils pour créer de nouveaux contenus d'orientation

focalisés sur la cybersécurité, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

8. CLASS CODE produit et anime des ressources de formation des formateurs autour de la pensée informatique sur le territoire. Elle apporte dans le Projet sa méthodologie et son savoir-faire en termes de production de ressources, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

9. Le CNED est un opérateur public de la formation en ligne. Il apporte dans le Projet ses outils et sa capacité à développer des modules pédagogiques en ligne sur la cybersécurité, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

10. L'ACADEMIE DE VERSAILLES décline la politique éducative définie par le gouvernement dans les départements des Yvelines, de l'Essonne, du Val d'Oise et des Hauts-de-Seine. Elle apporte dans le Projet sa connaissance du territoire et sa capacité à mobiliser les personnels enseignants, de la formation et de l'orientation au service des élèves, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

11. CY CERGY PARIS UNIVERSITE est localisée à Cergy. Elle apporte dans le Projet ses infrastructures et son savoir-faire en termes de développement de programmes pédagogiques sur la cybersécurité, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

12. L'UNIVERSITE PANTHEON-SORBONNE est localisée à Paris. Elle apporte dans le Projet ses infrastructures et son savoir-faire en termes de développement de programmes pédagogiques sur la cybersécurité, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

13. L'UNIVERSITE PARIS NORD est localisée à Villetaneuse. Elle apporte dans le Projet ses infrastructure et son savoir-faire en termes de développement de programmes pédagogiques sur la cybersécurité, comme indiqué à l'annexe « Description du Projet » du présent Contrat.

3. Dans ce contexte, les Partenaires entendant organiser leur collaboration dans l'exécution du Projet, en conformité avec la réglementation applicable, ont convenu de ce qui suit :

Article 2. Définition

4. Au sens du présent contrat, les expressions ci-dessous auront la définition suivante :

- « Connaissances Propres » : toutes les informations et connaissances techniques et/ou scientifiques et/ou tout autre type d'informations, sous quelque forme qu'elles soient, protégeables ou non et/ou protégées ou non par un droit de Propriété Intellectuelle y compris, sans que cette liste ne soit limitative, les savoir-faire, les secrets de fabrique, les secrets commerciaux, les données, les bases de données, les Logiciels (et notamment les Logiciels de Base), les dossiers, les plans, schémas, dessins, formules ou tout autre type d'information, sous quelque forme qu'elle soit, ainsi que tous les droits y afférant, utiles ou potentiellement utiles dans le cadre de la réalisation du Projet que chaque Partenaire pourrait détenir avant la Date d'Effet, et/ou développer ou acquérir, individuellement ou avec des tiers sans la Contribution des autres Parties, pendant le Projet mais indépendamment de celui-ci, la preuve pouvant en être rapportée, et que chaque Partenaire accepte de mettre à la disposition des autres Partenaires pour les besoins du Contrat. Les Connaissances Propres sont listées à l'annexe « Connaissances Propres » du Contrat. Cette liste devra être mise à jour régulièrement sur décision du Comité de pilotage ;

- Coordinateur : désigne CAMPUS CYBER en sa qualité de responsable de la coordination du Projet dont les missions sont listées au présent Contrat ;

- « Consortium » : groupement momentané composé de tous les Partenaires participant au Projet ;

- « Contrat » : le présent contrat, ses annexes et ses éventuels avenants ;

- « Contribution » : toute contribution au Projet de quelque nature que ce soit, notamment d'ordre intellectuel, humain, matériel ou financier. ;

- Date d'Effet : désigne la date de démarrage du Projet et de prise en compte des dépenses, fixée au 1er juillet 2023, conformément au contrat attributif d'aide joint en annexe ;

- « Entreprise » : entité, quel que soit son statut juridique (organisme de droit public ou privé) et son mode de fonctionnement (but lucratif ou non lucratif), qui exerce une activité économique (entendue comme offre de produits ou de services sur un marché donné) ;

- « Financeur(s) » : désigne l'Agence Nationale de la Recherche (ci-après désignée « ANR ») ;

- « Informations Confidentielles » : informations et données de toute nature, notamment technique, scientifique, économique, financière, commerciale, comptable, tout plan, étude, prototype, matériel, audit, données expérimentales et de tests, dessins, représentations graphiques, spécifications, savoir-faire, expérience, logiciels et programmes, quels qu'en soient la forme, le support ou le moyen, incluant, sans limitation, les communications orales, écrites ou fixées sur un support quelconque, échangées entre les Partenaires et :
  - (i) se rapportant directement ou indirectement au Projet et ;
  - (ii) désignées comme confidentielles par le Partenaire émetteur, par un tampon ou une légende si lesdites Informations sont écrites ou, par une mention spéciale lors de sa divulgation, confirmée par écrit dans un bref délai, ne pouvant excéder 15 jours, si lesdites Informations sont orales.

  Les Partenaires reconnaissent que les Résultats générant des droits de Propriété Intellectuelle et les Connaissances Propres des Partenaires constituent des Informations Confidentielles. En revanche, les Partenaires reconnaissent et acceptent que les Résultats ne générant pas de droits de Propriété Intellectuelle ni de savoir-faire secret, quel que soit le Partenaire qui les a créés, ne constituent pas des Informations Confidentielles.

  En outre, n'est pas une Information Confidentielle, toute information :

- qui était librement accessible au public avant sa divulgation ou qui l'est devenue après celle-ci, sans faute de la part du Partenaire récipiendaire, et sans qu'il y ait violation d'une obligation de secret,
- que le Partenaire récipiendaire a reçu licitement d'un tiers, sans qu'il y ait eu violation d'une obligation de secret,
- développée par ou pour le Partenaire récipiendaire, indépendamment de tout accès à l'Information Confidentielle,
- devant être communiquée en application de lois, réglementations, décisions de justice, à condition que le Partenaire récipiendaire en informe le Partenaire émetteur et que des mesures aient été prises pour assurer la confidentialité de l'information malgré sa communication.

- « Logiciel » : séquences d'instructions pour la réalisation d'un processus, exprimées sous une forme, ou transposables dans une forme, permettant leur exécution par un ordinateur, ainsi que le matériel de conception préparatoire et éventuellement la documentation associée.

- « Logiciel de Base » : Logiciel développé par un Partenaire avant la Date d'Effet et/ou développé sans la Contribution des autres Parties, pendant le Projet mais indépendamment de celui-ci ;

- « Logiciel Dérivé » : Logiciel développé par un Partenaire dans le cadre du présent Contrat à partir d'un Logiciel de Base. On distingue deux catégories de Logiciels Dérivés : les Adaptations et les Extensions.

- « Adaptation » : un Logiciel Dérivé utilisant les mêmes algorithmes que le Logiciel de Base dont il dérive et/ou réécrit dans un autre langage.

- « Extension » : un Logiciel Dérivé permettant d'accéder à des fonctions ou des performances nouvelles, absentes du Logiciel de Base dont il dérive.

- « Logiciel Nouveau » : Logiciel développé par un ou plusieurs Partenaires au titre du Projet, indépendamment de tout Logiciel de Base. Lorsque le Logiciel est développé grâce à la Contribution de deux ou plusieurs Partenaires, on parle de Logiciel Nouveau Commun.

- « Nécessaire » : (i) concernant la réalisation du Projet, une Connaissance Propre ou un Résultat est Nécessaire si l'exécution des travaux à la charge du Partenaire qui en demande l'accès s'en trouve, à défaut, impossible à exécuter, significativement retardée ou nécessiterait des efforts financiers ou humains supplémentaires significatifs ; (ii) concernant les activités hors Projet, une Connaissance Propre ou un Résultat est Nécessaire si à défaut d'y avoir accès, l'exploitation industrielle ou commerciale, à partir ou visant des Résultats serait techniquement ou légalement impossible.

- « Organisme de recherche » : entité, quel que soit son statut légal (de droit public ou de droit privé) ou son mode de financement, dont l'objectif premier est d'exercer, en toute indépendance, des activités de recherche fondamentale, de recherche industrielle ou de développement expérimental, ou de diffuser largement les résultats de ces activités au moyen d'un enseignement, de publications ou de transferts de connaissances. Les Entreprises qui peuvent exercer une influence déterminante sur une telle entité, par exemple en leur qualité d'actionnaire ou d'associé, ne peuvent pas bénéficier d'un accès privilégié aux résultats qu'elle produit ;

- « Partenaires » : ensemble des participants (personnes morales) au Consortium, signataires du Contrat, Organismes de Recherche ou Entreprises, réalisant le Projet ;

- « Partenaire émetteur » : Partenaire qui communique une Information Confidentielle à un ou plusieurs Partenaire(s) ;

- « Partenaire(s) Récipiendaire(s) » : Partenaire(s) qui reçoi(ven)t l'(les) Information(s) Confidentielle(s) du Partenaire émetteur ;

- « Part des Travaux » ou « Part de Travaux » ou « Tâches scientifiques » : l'ensemble des tâches incombant à un Partenaire dans la réalisation du Projet, la répartition des tâches étant détaillée à l'annexe « Description du Projet » du Contrat ;

- « Projet » : projet collaboratif de recherche ou recherche et développement, tel que décrit dans le document scientifique sur la base duquel le Projet a été sélectionné pour financement à l'ANR (et ses modifications éventuelles), repris en annexe « Description du Projet » du Contrat ;

- « Propriété Intellectuelle » : tous les droits de propriété littéraire et artistique et/ou de propriété industrielle, existants ou futurs, comprenant notamment sans être limitatifs, le droit d'auteur, brevet, marque, certificat d'utilité, dessin ou modèle, certificat d'obtention végétale, droits sur les logiciels, puces et semi-conducteurs, droits des producteurs de bases de données, y compris les droits attachés aux demandes de tous titres de Propriété Intellectuelle ;

- « Règle de proportionnalité » : les droits de Propriété Intellectuelle résultant du Projet, ainsi que les droits d'accès connexes sont attribués aux différents Partenaires d'une façon qui reflète leurs Contributions respectives ;

- « Règle du Prix du marché / Rémunération équivalente au prix du marché » : L'Organisme de recherche doit recevoir une Rémunération équivalente au prix du marché pour les droits de Propriété Intellectuelle résultant de ses activités, attribués à une ou plusieurs Entreprises participantes au Projet ou pour lesquels une ou plusieurs autres Entreprises participantes au Projet bénéficient d'un droit d'accès. Le montant absolu de la valeur de la Contribution des Entreprises participantes aux coûts des activités de l'Organisme de recherche qui ont généré les droits de la Propriété Intellectuelle concernés peut être déduit de cette rémunération.

  La rémunération est équivalente au prix du marché lorsqu'une des conditions suivantes est remplie :

    - le montant de la rémunération a été fixé au moyen d'une procédure de vente concurrentielle ouverte, transparente et non discriminatoire,
    - une évaluation d'un expert indépendant confirme que le montant de la rémunération est au moins égal au prix du marché,
    - l'Organisme de recherche, en tant que vendeur, peut démontrer qu'il a effectivement négocié la rémunération dans des Conditions de pleine concurrence afin d'obtenir un avantage économique maximal au moment de la conclusion du contrat, tout en tenant compte de ses objectifs statutaires,

lorsque l'accord de collaboration confère à l'Entreprise partenaire le droit de premier refus pour ce qui est des droits de Propriété Intellectuelle générés par les Organismes de recherche participant au projet de collaboration, si ces entités exercent un droit réciproque de solliciter des offres économiquement plus avantageuses auprès de tiers de sorte que l'Entreprise partenaire adapte son offre en conséquence.

- « Résultats » : toutes les informations et connaissances techniques et/ou scientifiques, protégées ou non, protégeables ou non par un droit de Propriété Intellectuelle, y compris les savoir-faire, les secrets de fabrique, les secrets commerciaux, les données, les bases de données, les Logiciels, les dossiers, les matériels, les plans, schémas, dessins, formules ou tout autre type d'information, sous quelque forme qu'elle soit, et tous les droits y afférents, développées par un ou plusieurs Partenaires dans le cadre du Projet. Les Résultats peuvent être Propres ou Conjoints. Les Logiciels Nouveaux et les Logiciels Nouveaux Communs constituent des Résultats au sens de la présente définition.

- « Résultat Propre » : le Résultat obtenu par un Partenaire seul, sans la Contribution des autres Partenaires.

- « Résultat Conjoint » : le Résultat développé grâce aux Contributions d'au moins deux Partenaires, au titre du Projet.

Article 3. OBJET

5. Le Contrat a pour objet d'organiser les relations entre les Partenaires dans le cadre du Projet, et notamment de :

- déterminer leurs droits et leurs obligations, conformément à l'annexe « Description du Projet » du Contrat,
- déterminer la gestion et le suivi des Résultats,
- déterminer les modalités de reversement de l'aide aux Partenaires,
- organiser la gouvernance du Projet,
- fixer les règles de propriété, d'utilisation et d'exploitation des Connaissances Propres et des Résultats,
- déterminer la dévolution des droits de Propriété Intellectuelle de chacun d'entre eux.

6. Aucune stipulation du Contrat ne pourra être interprétée comme constituant une entité juridique de quelque nature que ce soit, ni impliquant une quelconque solidarité entre les Parties.

Les Parties déclarent que le Contrat ne peut en aucun cas être interprété ou considéré comme constituant un acte de société, l'*affectio societatis* étant formellement exclu.

Article 4. DURÉE

7. Le Contrat entrera rétroactivement en vigueur à la Date d'Effet à compter de sa signature par tous les Partenaires.

Par exception à ce qui précède, le Contrat n'entre en vigueur, s'agissant des obligations de confidentialité contenues à l'article 2, qu'à la dernière date de signature du Contrat par les Partenaires.

8. Le Contrat est conclu pour toute la durée du Projet, et prendra fin lorsque tous les Partenaires auront réalisé l'ensemble de leurs Parts des Travaux, conformément à l'annexe « Description du Projet » du Contrat, soit au 30 juin 2028 (projet de 60 mois). Le cas échéant, en cas de prolongation du Projet par le ou les organisme(s) Financeur(s), les Parties formaliseront un avenant pour proroger la durée du présent Contrat.

9. Nonobstant la fin du Contrat, les Partenaires resteront tenus par les termes des clauses « Propriété intellectuelle des Connaissances Propres », « Propriété intellectuelle des Résultats », « Confidentialité » et « Publications et communications » pour leurs durées propres restantes.

Article 5. GOUVERNANCE DU CONSORTIUM

10. La gouvernance du Consortium est organisée autour :

- d'un Coordinateur,
- d'un Comité stratégique,
- d'un Comité de pilotage,
- de Comités opérationnels.

5.1 LE COORDINATEUR

11. CAMPUS CYBER est désigné Coordinateur. A la date de signature du présent Contrat, le représentant de CAMPUS CYBER désigné pour assurer ce rôle est M. Yann BONNET.

12. Le Coordinateur est chargé d'assurer la coordination du Projet sur le plan de la réalisation des actions et livrables du Projet, de la mise en place et de la formalisation de la coopération entre les Partenaires, de la production de certains des documents à fournir du Projet auprès du Financeur. Sans préjudice des éventuelles obligations envers l'ANR qui incomberaient par ailleurs aux autres Partenaires (également financés par l'ANR, via un acte attributif d'aide) il est l'interlocuteur privilégié de ANR et le porte-parole du Projet pour notamment sa diffusion grand public et sa promotion.

13. Par ailleurs, le Coordinateur est chargé de faire le lien entre les Partenaires, entre eux et entre les Partenaires et le Comité de pilotage. A ce titre, le Coordinateur :

- est responsable de la communication entre les Partenaires, et assure notamment les échanges d'informations relatives aux Connaissances Propres et aux Résultats ;

- coordonne l'action des Partenaires tout au long de la durée du projet ;

- coordonne et assure le suivi de l'avancement de la réalisation des livrables attendus par le Financeur ;

- convoque les membres du Comité de pilotage, rédige, diffuse, et tient les registres des comptes rendus, et, de manière générale, assure le secrétariat du Projet ;

- tient la liste des Connaissances Propres, la met à jour sur décision du Comité de pilotage et la diffuse auprès des Partenaires ;

14. Sous réserve de l'accord préalable du Financeur, le Coordinateur est également chargé de faire signer à tout nouveau Partenaire entrant dans le Consortium en cours d'exécution du Contrat un avenant au Contrat, par lequel il ratifie celui-ci, conformément aux dispositions de l'article « Entrée d'un nouveau Partenaire » du Contrat.

13. Le Coordinateur est chargé :

- d'informer le Financeur et les membres du Comité de pilotage en cas de retrait volontaire d'un Partenaire tel que prévu à l'article 10 – « Modification au sein du consortium » ;

- dans le cas où l'un des Partenaires manquerait aux obligations qui lui incombent au titre du Contrat, de mettre en demeure ce Partenaire de s'exécuter par lettre recommandée avec demande d'avis de réception, conformément à l'article 10 – « Modification au sein du consortium ».

14. Indépendamment de ses obligations à l'égard du Financeur, le Coordinateur n'est pas autorisé à agir au-delà du périmètre de sa mission, défini au Contrat. Il n'est pas non plus autorisé à prendre un engagement quelconque au nom et pour le compte de l'un des Partenaires ou de l'ensemble d'entre eux, sans l'autorisation préalable de ceux-ci.

5.2 Le Comité Stratégique

5.2.1 Composition du Comité Stratégique

15 . Le comité stratégique est composé d'un représentant du Coordinateur et de représentants des institutions et organismes qui :

- Sont prescripteurs des politiques publiques en matière de formation initiale et continue, de travail, d'emploi et d'insertion (Ministère de l'Éducation nationale et de la Jeunesse, Ministère de l'Enseignement supérieur et de la Recherche, Ministère du Travail, de l'Emploi et de l'Insertion) ;
- Ont un rôle de fédérateur de l'offre de formation initiale et continue dans l'enseignement supérieur, dans le secteur numérique notamment (ex : CGE, CDEFI, France Université) ;
- Constituent une autorité indiscutable dans le domaine des compétences cybersécurité (ANSSI).

16. Il pourra être complété de personnalités et d'experts des sphères académique (enseignants-chercheurs), économique (représentants d'entreprises) ou de la société civile. La composition du comité

stratégique est donc susceptible d'évoluer en fonction de l'avancement du Projet, des orientations stratégiques nationales dans le secteur de la cybersécurité et des sujets d'intérêts des partenaires.

5.2.2 Réunions du Comité Stratégique

17. Le Comité stratégique se réunit une (1) fois par an, sur invitation du Coordinateur

18. Le Coordinateur définit l'ordre du jour de la réunion du comité stratégique après consultation des partenaires et l'adresse à chacune des Parties au moins quinze (15) jours avant la réunion.

19. Les réunions du Comité stratégique font l'objet de comptes rendus rédigés par le Coordinateur et transmis à chacune des Parties dans les quinze (15) jours suivant la date de la réunion. Ces comptes rendus sont également transmis aux Partenaires.

5.2.3 Règle du Comité Stratégique

20. Le Comité stratégique n'ayant qu'un rôle consultatif, il est réputé valablement réuni si la moitié des participants invités sont présents. Si ce quorum n'est pas atteint, le Coordinateur organise un second comité dans les trois (3) semaines à compter de la date de la réunion initiale. A la suite de cette seconde réunion, le Comité stratégique est valablement réuni même si le quorum n'est pas atteint.

5.2.4 Rôle du Comité Stratégique

21. Le comité stratégique n'a pas vocation à prendre de décisions dans le cadre du projet TALCYB. Son rôle est de challenger les orientations du programme au regard de l'évolution des enjeux stratégiques et d'éléments de contexte plus larges : contexte politique, économique et réglementaire, articulation avec des politiques nationales, veille scientifique et technologique, innovation pédagogique, stratégies et pratiques à l'international, etc.

5.3 Le Comité de pilotage

5.3.1 Composition du Comité de pilotage

22. Le comité de pilotage est composé de représentants des institutions et organismes suivants :
- SGPI
- ANR
- Contributeurs en financement (OPCO Atlas, INRIA)
- Campus Cyber
    - Directeur de projet
    - Directeur Général Délégué
    - Autres membres de l'équipe de coordination du projet
    - Représentants des comités opérationnels
    - Représentants des collèges formation et recherche
    - Coordinateur du groupe de travail « formation » du studio des communs

23. Le Comité de pilotage est présidé par le Coordinateur.

24. Les Partenaires conviennent que pour certains aspects techniques du Projet, le Comité de pilotage pourra faire appel à des experts qui auront un rôle consultatif. La liste des experts et les motifs de leur présence au Comité de pilotage devra avoir fait l'objet d'une information préalable auprès des Partenaires. En tant que de besoin et/ou à la demande des Partenaires, la signature d'un accord de confidentialité pourra constituer un préalable à la participation des experts sollicités.

5.3.2 Réunions du Comité de pilotage

25. Le Comité de pilotage se réunit au moins une (1) fois par an, sur convocation du Coordinateur. Une réunion préparatoire restreinte aux partenaires est idéalement organisée à l'initiative du Coordinateur.

26. Des réunions extraordinaires du Comité de pilotage peuvent être organisées par le Coordinateur, en cas d'urgence notamment, sur demande écrite et motivée d'un ou plusieurs Partenaires.

27. Sauf urgence, le Coordinateur adresse l'ordre du jour aux membres du Comité de pilotage au moins quinze (15) jours avant la réunion.

28.Les réunions du Comité de Pilotage font l'objet de comptes rendus rédigés par le Coordinateur et transmis à chacune des Parties dans les quinze (15) jours suivant la date de la réunion.

29. Les comptes rendus font état de la mise à jour des Résultats et de la Contribution des Partenaires. Ils comportent un tableau comprenant l'identification des Résultats obtenus au jour de la réunion, leur évaluation (brevetabilité ou non), leur classification (Résultats Propres ou Résultats Conjoints) ainsi que la propriété des Partenaires.

30. Ces comptes -rendus sont considérés comme acceptés par les Partenaires si, dans les quinze (15) jours à compter de leur réception, aucune objection, ni revendication, n'a été formulée par écrit auprès du Coordinateur par ces mêmes Partenaires.

5.3.3 Règles de décision au sein du Comité de pilotage

31. Le Comité de pilotage est valablement réuni si les trois quarts (3/4) de ses membres sont présents ou représentés. Si lors d'une réunion le quorum n'est pas atteint, le Comité de pilotage est convoqué une seconde fois, dans un délai qui ne peut excéder 3 semaines à compter de la date de la réunion initiale. A la suite de cette seconde convocation, le Comité de pilotage est valablement réuni, même si le quorum n'est pas atteint.

32. Chaque membre du Comité de pilotage peut recevoir, pour une réunion donnée, un mandat de représentation d'un autre membre, dans la limite d'un mandat par réunion.

33. Les membres du Comité de pilotage disposant de droits de vote sont :

- Le représentant du SGPI (1 voix)
- Le représentant de l'OPCO Atlas (1 voix)
- Le représentant de l'INRIA (1 voix)
- Les représentants du Campus Cyber
    - Directeur de projet (1 voix)

- Directeur Général Délégué (1 voix)

- Les représentants des Partenaires hors Coordinateur au titre de l'attractivité, de l'orientation et de la formation à désigner annuellement entre les Partenaires (3 voix)

34. A l'exception des cas expressément prévus au Contrat où les décisions doivent être prises à l'unanimité, le Comité de pilotage prend ses décisions à la majorité simple des votes des membres présents ou représentés.

35. En cas d'égalité, le directeur de Projet représentant du Campus Cyber dispose d'une voix d'arbitrage.

5.3.4 Rôle du Comité de pilotage

36. Sans préjudice des règles de financement et décisions de l'ANR relatives au Projet le Comité de pilotage prend les décisions relatives à la direction globale du Projet, et notamment :

- statue sur l'orientation stratégique et scientifique du Projet après avis du Conseil stratégique le cas échéant ;
- décide éventuellement de toute modification substantielle relative à l'estimation financière et/ou au calendrier, sous réserve de l'approbation du Financeur ; toute augmentation du budget est soumise à une décision unanime du Comité de pilotage (une Partie ne pouvant se voir imposer une augmentation de ses dépenses sans y avoir consenti) .Le caractère substantiel d'une modification est à l'appréciation du Coordinateur ;
- statue sur les modifications substantielles à apporter aux Parts des Travaux, voire sur l'abandon de tout ou partie de certaines Parts des Travaux, si celles-ci n'apportent pas les avantages techniques et/ou économiques escomptés, tels que définis à l'annexe « Description du Projet ». Le caractère substantiel d'une modification est à l'appréciation du Coordinateur ;
- statue sur l'avancement de la réalisation des Parts des Travaux ;
- s'assure de la mobilisation des ressources par les Partenaires pour la bonne réalisation du Projet ;
- valide les livrables attendus par le Financeur (reporting annuel, PGD, etc.) ;
- statue sur l'entrée d'un nouveau Partenaire dans le Consortium, dans les conditions de l'article « Entrée d'un nouveau Partenaire » ;
- statue sur le retrait ou l'exclusion d'un Partenaire, dans les conditions de l'article « Retrait ou exclusion d'un Partenaire » ;
- contrôle le respect des règles de confidentialité telles que définies à l'article « Confidentialité» ;
- contrôle le respect des Connaissances Propres, Résultats et droits de Propriété Intellectuelle de chaque Partenaire, tels que définis aux articles « Propriété intellectuelle des Connaissances Propres » et « Propriété intellectuelle des Résultats » ;
- fait des propositions et arbitre les questions en matière de Propriété Intellectuelle conjointe à un ou plusieurs Partenaires, notamment sur la protection adéquate, les dépôts éventuels (brevet, enveloppe Soleau, APP, etc.), le territoire géographique de protection des droits et les budgets corrélatifs ;
- arbitre en cas de manquement de l'un des Partenaires à ses obligations contractuelles, et statue notamment sur les conséquences de ce manquement.

5.4 Les Comités opérationnels

37. Des Comités opérationnels sont créés afin de permettre aux partenaires de travailler de façon transversale sur des problématiques communes. Il s'agit ainsi de groupes de travail thématiques dont l'objet est défini collectivement par les partenaires eux-mêmes.

5.4.1 Composition des Comités opérationnels

38. Les Comités opérationnels sont composés des représentants des partenaires sur la base du volontariat.

39. Chaque réunion de comité opérationnel est animée par un responsable de comité qui est le Coordinateur ou un représentant de l'un des Partenaires volontaire, sous réserve de l'acceptation de ce dernier par les autres membres du comité.

5.4.2 Réunions des Comités opérationnels

40. Chaque Comité opérationnel se réunit en tant que de besoin et au moins une (1) fois par mois.

41. Le responsable de comité est chargé de l'organisation des réunions du Comité, la rédaction et des comptes rendus et leur diffusion auprès de tous les partenaires par dépôt sur l'outil de travail collaboratif partagé.

5.4.3 Règles au sein des Comités opérationnels

42. Les Comités opérationnels peuvent être ouverts à des experts et contributeurs externes pertinents au regard de la thématique de travail traitée.

43. Les productions des Comités opérationnels sont partagées avec l'ensemble des Partenaires et des contributeurs.

5.4.4 Rôle des Comités opérationnels

44. Sans préjudice des éventuelles règles de financement et des décisions de l'ANR ou tout autre organisme financeur applicables (dans le contexte de financement en tout ou partie du Projet par des fonds publics), les Comités opérationnels ont vocation à :

- Permettre la mutualisation et la synchronisation entre les Travaux portés par les Partenaires s'agissant d'une problématique de travail commune ;

- Faire émerger les points de difficultés partagés par les partenaires et émettre des propositions de modification du Projet au Comité de pilotage ;

- Favoriser le travail en écosystème ouvert en permettant la contribution d'autres acteurs (de la cyber, de la formation, etc.) au Projet.

Article 6. Engagements des partenaires

6.1 Obligations des Partenaires à l'égard du Coordinateur

45. Chaque Partie s'engage –indépendamment de ses propres obligations éventuelles envers l'ANR- envers le Coordinateur à :

- fournir les éléments permettant au Coordinateur de répondre aux éventuelles demandes de l'ANR ;
- indiquer et justifier (notamment en cas de retard important) au Coordinateur l'état d'avancement des Travaux qu'elle exécute et les Résultats obtenus, selon une périodicité définie d'un commun accord entre le Coordinateur et le Partenaire au cas par cas;
- transmettre au Coordinateur les comptes rendus intermédiaires destinés à l'ANR ainsi que les éléments nécessaires à l'établissement du compte-rendu final unique en respectant un délai et une forme définis par le Coordinateur, en lien avec les éléments demandés par l'ANR ;
- prévenir sans délai le Coordinateur de toute difficulté pouvant compromettre l'exécution normale du Projet.

6.2 Engagements techniques

46. Les Partenaires s'engagent à réaliser leur Part des Travaux, telle que fixée à l'annexe « Description du Projet ». Leurs Parts des Travaux pourront être modifiées en cours de Projet par une décision du Coordinateur et une information du Financeur en cas de modification raisonnable, après décision du Comité de pilotage et accord du Financeur en cas de modification substantielle. Le caractère raisonnable ou substantiel d'une modification est à l'appréciation du Coordinateur.

47. Les Partenaires s'engagent en outre à mettre en place une traçabilité de leurs travaux et réalisations au titre du Projet, en conformité avec l'annexe « Description du Projet ».

48. De manière générale, les Partenaires s'engagent à mettre en œuvre tous les moyens nécessaires à la réalisation de leurs Parts des Travaux dans les délais impartis.

6.3 Autres engagements

49. Chaque Partenaire déclare disposer sur ses Connaissances Propres de tous les droits nécessaires pour pouvoir les communiquer et les donner –le cas échéant- en licence aux autres Partenaires sous réserve des droits des tiers.

50. Dans la réalisation de sa Part des Travaux, chaque Partenaire s'engage à respecter les droits des tiers, notamment les droits de Propriété Intellectuelle.

51. A cet égard, chaque Partenaire fait son affaire personnelle des droits que des salariés ou tiers pourraient revendiquer sur les Résultats dont il est propriétaire ou copropriétaire. Il s'engage à obtenir les autorisations ou cessions de droits nécessaires à l'exploitation des dits Résultats.

52. Chaque Partenaire s'engage en outre à respecter les dispositions d'ordre public du Code de la propriété intellectuelle relatives aux droits moraux et patrimoniaux des auteurs et inventeurs, et notamment celles relatives au droit au nom et au droit à rémunération.

53. Par ailleurs, dans l'hypothèse où un Partenaire connaitrait un changement de contrôle au sens de l'article L233-3 du code de commerce, ce dernier devra en informer –outre, le cas échéant, son organisme de financement- les autres Parties dans un délai de 30 jours à compter du caractère effectif de ce changement de contrôle.

54. Globalement, chaque Partenaire s'engage à respecter les réglementations applicables dans l'exercice de ses activités et de travaux de recherche (le cas échéant protocole de Nagoya, autorisations cohortes, données personnelles, droit du travail et de la sécurité sociale, sécurité des travailleurs et des installations, etc.) et bonnes pratiques applicables en matière scientifique.

Article 7. ENGAGEMENTS FINANCIERS

55. Indépendamment du soutien éventuel par des fonds publics, chaque Partenaire doit supporter ses propres coûts relatifs au Projet.

56. Chaque Partenaire s'engage à investir et engager dans le Projet les ressources financières fixées aux annexes « Description du Projet » et « Budget ».

57 . Le Coordinateur verse aux Partenaires les avances pour le Projet selon l'échéancier prévisionnel indiqué à l'annexe 6 du présent accord.

58. Le reversement de ces avances est subordonné au bon avancement du Projet et conditionné par la fourniture des documents de suivi au Coordinateur tels que définis dans les articles précédents.

59. Le Coordinateur se réserve le droit d'ajuster le montant des avances versées d'une année à la suivante au regard de l'analyse des documents ainsi fournis.

Article 8. RESPONSABILITÉ

60. Chaque Partenaire engage uniquement sa propre responsabilité pour la Part des Travaux qu'il réalise et en supporte toutes conséquences.

61. Cependant, d'un commun accord, les Partenaires conviennent que leur responsabilité pourrait le cas échéant être engagée à l'égard des autres Partenaires, pour les conséquences des dommages directs, l'indemnisation des dommages indirects étant exclue. Dans ce cadre, les Partenaires conviennent que sont des dommages indirects les pertes de bénéfices, de chiffre d'affaires, de marges, de revenus, pertes de commandes, de clients, d'exploitation, d'actions commerciales, ou encore l'atteinte à l'image de marque ou l'action de tiers.

62. Chaque Partie est responsable, dans les conditions de droit commun, des dommages directs de toute nature, causés par son personnel au personnel de toute autre Partie ainsi que des dommages directs qu'elle cause aux biens mobiliers ou immobiliers de toute autre Partie.

Article 9. Force majeure

64. Aucun Partenaire ne pourra être tenu responsable de la non-exécution totale ou partielle de ses obligations due à un cas de force majeure.

65. Dans un premier temps, les cas de force majeure suspendront l'exécution du présent Contrat.

66. Si le cas de force majeure a une durée d'existence supérieure à deux mois, le présent Contrat pourra être résilié par écrit par toute Partie non directement affectée, sans engager sa responsabilité.

67. De façon expresse, sont considérés comme cas de force majeure, ceux répondant à la définition de l'article 1218 du Code civil, et ceux habituellement retenus par la jurisprudence des cours et tribunaux français.

Article 10. Modifications au sein du Consortium

10.1 Entrée d'un nouveau partenaire

68. L'entrée d'un nouveau Partenaire dans le Consortium est subordonnée à l'accord du Coordinateur, et du Comité de pilotage. Elle deviendra effective le jour de la signature par le nouveau Partenaire, le Coordinateur et le Financeur d'un avenant au Contrat ratifiant celui-ci. Cet avenant sera annexé au Contrat.

69. A compter de cette date, le nouveau Partenaire est tenu par tous les termes du Contrat.

70. La Part des Travaux du nouveau Partenaire sera décrite dans une nouvelle annexe au Contrat.

71. Le nouveau Partenaire bénéficiera, comme les autres Partenaires, des droits définis au Contrat.

10.2 Retrait et exclusion d'un partenaire

10.2.1 Retrait d'un partenaire

72. Tout Partenaire peut décider de mettre fin à sa participation au Consortium, à condition de notifier préalablement sa décision au Coordinateur par l'envoi d'une lettre recommandée avec avis de réception, indiquant les motifs de son retrait.

73. Dans les deux (2) mois suivant la réception de cette lettre, le Comité de pilotage devra se réunir afin d'acter le retrait et statuer sur les conséquences sur la poursuite du Projet, en proposant une éventuelle réorganisation (exemple proposition de reprise de Parts des Travaux restantes).

73. Le retrait effectif du Partenaire qui entend se retirer ne pourra intervenir, sauf accord plus favorable du Comité de pilotage, qu'au terme d'un délai d'un (1) mois à compter de la réunion du Comité de pilotage actant du retrait.

74. En cas de retrait d'un Partenaire, l'exécution de sa Part des travaux pourra, sur décision des autres Partenaires prise au sein du Comité de pilotage, être assurée par les soins d'un ou plusieurs autre(s) des Partenaire(s) ou d'un nouveau Partenaire identifié par le Comité de pilotage. Le retrait du Partenaire et les modalités de réorganisation du Projet seront formalisés par la signature d'un avenant.

75. Le Partenaire se retirant s'engage à fournir gratuitement aux autres Partenaires ou au tiers substitué toutes les informations nécessaires à la poursuite de l'exécution des Travaux en ses lieu et place.

76. L'exercice de ce droit de résiliation ne dispense pas le Partenaire se retirant de respecter ses obligations contractuelles jusqu'à la date de résiliation effective fixée dans l'avenant susmentionné.

78. A l'initiative du Coordinateur ou des Partenaires, les évolutions sont présentées au Financeur, les modifications pouvant impliquer la mise en œuvre de démarches ou décisions de la part de ce dernier.

10.2.2 EXCLUSION D'UN PARTENAIRE

79. Sans préjudice des éventuelles règles applicables dans le contexte de financement en tout ou partie du Projet par le Financeur, en cas de défaillance suffisamment grave de l'un des Partenaires dans l'exécution de ses obligations contractuelles, et notamment dans la réalisation de sa Part des travaux, le Coordinateur lui adressera, par lettre recommandée avec avis de réception, une mise en demeure d'avoir à exécuter ses obligations. Faute pour le Partenaire de remédier à cette inexécution dans un délai de trente (30) jours à compter de la date de réception de la mise en demeure, le Partenaire sera considéré comme défaillant.

71. A compter de cette date, ses droits seront suspendus et plus aucune Information Confidentielle ne lui sera communiquée. Il pourra en outre, voir sa responsabilité engagée à raison du préjudice subi par les autres Partenaires, dans les limites de l'article « Responsabilité ».

72. Le Comité de pilotage devra se réunir dans un délai de trente (30) jours, afin de statuer sur les conséquences de la défaillance du Partenaire. Le Coordinateur pourra décider d'exclure le Partenaire défaillant. Cette exclusion sera formalisée par l'envoi par le Coordinateur d'une notification au Partenaire défaillant.

73. En cas de défaillance du Partenaire Coordinateur, les Partenaires non défaillants proposeront une réorganisation du Consortium, et -en accord avec le Financeur- désigneront le Partenaire qui prendra à son compte les missions du Partenaire Coordinateur jusqu'au terme du Projet, soit l'un des Partenaires non défaillants, soit un nouveau Partenaire.

74. Par ailleurs, dans l'hypothèse où un Partenaire connaitrait un changement de contrôle, au sens de l'article L. 233-3 du Code de commerce, le Coordinateur pourra se saisir ou être saisi à l'initiative d'un ou plusieurs Partenaire(s) pour statuer (indépendamment des éventuelles règles et obligations applicables à l'égard des organismes de financement) sur le maintien au sein du Consortium du Partenaire dont le contrôle a changé.

10.2.3 DROITS DU PARTENAIRE SORTANT

75. Le Partenaire sortant conservera ses droits de propriété sur les Résultats qu'il a développés. Lorsqu'il en sera l'unique propriétaire, il pourra continuer à les exploiter comme il l'entend. Lorsqu'il en sera copropriétaire avec d'autres Partenaires, il pourra continuer à les exploiter conformément aux accords de copropriété passés qui respecteront la Règle de proportionnalité et la Règle du Prix du marché.

76. Le Partenaire sortant conservera le droit de continuer à utiliser les Connaissances Propres et les Résultats des autres Partenaires qu'il a obtenu(e)s par licence contre une Rémunération équivalente au Prix du Marché pour ses besoins propres de recherche et dans le cadre de collaborations de recherche avec des tiers, à l'exclusion de toute utilisation, directe et/ou indirecte, à des fins industrielles et/ou commerciales.

10.2.4 OBLIGATIONS DU PARTENAIRE SORTANT

77. Les droits accordés, avant sa sortie du Consortium, par le Partenaire sortant aux autres Partenaires sur ses Connaissances Propres et/ou sur ses Résultats en exécution du Contrat resteront valables jusqu'au terme des licences initiales.

78. Le Partenaire sortant sera tenu de restituer ou détruire, selon la demande du Partenaire émetteur, toute Information Confidentielle qui lui aura été remise par un autre Partenaire.

79. Le Partenaire sortant restera tenu par ses engagements de confidentialité, tels que fixés à l'article « Confidentialité », sur les Informations Confidentielles, aussi longtemps que ces obligations demeureront en vigueur.

Article 11. PROPRIÉTÉ INTELLECTUELLE DES CONNAISSANCES PROPRES

11.1 PROPRIÉTÉ DES CONNAISSANCES PROPRES

80. Chaque Partenaire est et reste propriétaire de ses Connaissances Propres, listées à l'annexe « Connaissances Propres ».

81. Aucune communication des Connaissances Propres à d'autres Partenaires ne peut être interprétée comme un transfert de propriété.

11.2 PROTECTION DES CONNAISSANCES PROPRES

82. Chaque Partenaire assure librement la protection de ses Connaissances Propres. Notamment, il décide seul de protéger ou non ses Connaissances Propres et, le cas échéant, de la protection adéquate.

83. En tout état de cause, chaque Partenaire s'engage à conserver, par des dépôts ou démarches dont il choisit la forme, la preuve de ses Connaissances Propres, tant pour leur date que pour leur contenu.

11.3 UTILISATION ET EXPLOITATION DES CONNAISSANCES PROPRES

84. Chaque Partenaire exploite librement, directement ou indirectement, ses Connaissances Propres, sous réserve des droits suivants accordés aux autres Partenaires.

85. Chaque Partenaire accorde à chacun des autres Partenaires qui en fait la demande une licence d'utilisation de ses Connaissances Propres lorsque celles-ci sont Nécessaires au Partenaire qui en fait la demande pour la réalisation de sa Part de Travaux dans le cadre du Projet.

86. Cette licence peut être accordée contre une Rémunération équivalente au Prix du marché si la commercialisation de licence d'utilisation de ses Connaissances Propres constitue une source de revenus pour le Partenaire.

87. Cette licence est non cessible et non exclusive, et est concédée pour la durée du Contrat.

88. Lorsque les Connaissances Propres sont des logiciels, et à défaut de stipulations contraires prévues dans un contrat de licence conclu entre les Partenaires concernés, le Partenaire qui les reçoit ne peut les utiliser que sur ses propres matériels et n'est autorisé qu'à réaliser la reproduction strictement nécessitée par le chargement, l'affichage, l'exécution, la transmission et le stockage de ces logiciels aux seules fins de son utilisation pour la réalisation de sa Part des Travaux par ledit Partenaire, ainsi qu'une copie de sauvegarde.

89. Le Partenaire qui les reçoit s'interdit tout autre acte d'utilisation de ces logiciels et, notamment, tout prêt ou divulgation à des tiers (sauf dans l'hypothèse où ces actes sont nécessaires à l'exécution du Projet et après avoir obtenu l'autorisation préalable et écrite du Partenaire détenteur, par ex. mise à disposition à un sous-traitant) ainsi que toute exploitation. Le droit d'utilisation ainsi conféré n'entraîne pas l'accès aux codes sources des logiciels considérés sauf autorisation préalable et écrite du Partenaire titulaire des droits sur lesdits logiciels. En outre, le Partenaire qui les reçoit s'interdit tout acte de décompilation ou de rétroingénierie desdits logiciels.

90. La licence sera non cessible et non exclusive.

91. Elle donnera lieu à la signature entre les Partenaires concernés d'un accord écrit préalable, précisant les droits concédés, leur étendue, leur destination, le lieu et la durée de la licence, ainsi que les modalités financières de celle-ci. Il est entendu que la licence fera référence et application de la Règle du Prix du marché.

92. Il est d'ores et déjà convenu que lorsque la licence portera sur un logiciel, elle sera limitée au code objet de celui-ci.

93. Il est également d'ores et déjà convenu que le Partenaire licencié prendra à sa charge l'exécution des formalités qui pourraient être nécessaires pour rendre opposable aux tiers la licence qui lui est accordée.

94. Chaque Partenaire peut obtenir, sur sa demande et contre une Rémunération équivalente au Prix du marché, un droit d'utilisation des Connaissances Propres des autres Partenaires à des fins de recherche interne et dans le cadre de collaborations de recherche avec des tiers, à l'exclusion de toute utilisation, directe et/ou indirecte, à des fins industrielles et/ou commerciales. La demande doit être formulée pendant la durée du Contrat ou au plus tard dans les douze (12) mois qui suivent son terme. Cette licence d'utilisation donnera lieu à la signature entre les Partenaires concernés d'un accord écrit préalable, précisant les droits concédés, leur étendue, leur destination, le lieu et la durée de la licence, ainsi que les modalités financières de celle-ci. Il est entendu que la licence fera référence et application de la Règle du Prix du marché.

Article 12. Propriété intellectuelle des Résultats

12.1 Propriété des Résultats

12.1.1 Propriété des Résultats Propres

95. Les Résultats Propres sont la propriété du Partenaire qui les a générés seul.

12.1.2 Propriété des Résultats Conjoints (hors Logiciels)

96. Les Résultats Conjoints sont la copropriété des Partenaires les ayant développés, ci-après désignés « Parties Copropriétaires », à proportion de leurs Contributions, à moins que lesdits Partenaires ne conviennent conventionnellement d'une répartition différente.

97. En cas de répartition conventionnelle différente, il sera fait application de la Règle du prix du marché.

12.1.3 Propriété des Résultats Conjoints Brevetables

98. Sous réserve des dispositions ci-dessus, les Partenaires Copropriétaires des Résultats Conjoints brevetables décideront si ces derniers doivent faire l'objet de demandes de brevets déposées à leurs noms conjoints, et désigneront parmi eux, celui qui sera chargé d'effectuer les formalités de dépôt et de maintien en vigueur (ci-après désigné « Gestionnaire de la PI »).

99. Les frais de dépôt, d'obtention et de maintien en vigueur des brevets nouveaux en copropriété seront supportés par les Partenaires Copropriétaires selon leur quote-part de propriété définies ci-dessus.
Par exception à ce qui précède, les frais de dépôt, d'obtention et de maintien en vigueur des brevets nouveaux en copropriété seront supportés par les Entreprises lorsqu'elles en sont copropriétaires avec un Organisme de recherche.

100. Si l'un des Partenaires Copropriétaires renonce à déposer, à poursuivre une procédure de délivrance ou à maintenir en vigueur un ou plusieurs brevets nouveaux en France ou à l'étranger, il devra en informer les autres Partenaires Copropriétaires en temps opportun pour que ceux-ci déposent en leurs seuls noms, poursuivent la procédure de délivrance ou le maintien en vigueur desdits brevets nouveaux à leurs seuls frais et profits. Le Partenaire qui s'est désisté s'engage à signer ou à faire signer toutes les pièces nécessaires pour permettre aux autres Partenaires Copropriétaires de devenir seuls copropriétaires du ou des brevets nouveaux en cause pour le ou les pays concernés.

101. Un Partenaire Copropriétaire sera réputé avoir abandonné ses droits sur un brevet nouveau soixante (60) jours après la réception d'une lettre recommandée avec accusé de réception lui demandant de faire connaître sa décision sur ce point, adressée par le Partenaire Copropriétaire chargé d'effectuer les formalités de dépôt et de maintien en vigueur des brevets désignée conformément au premier paragraphe du présent article.

102. Chaque Partenaire Copropriétaire fait son affaire de la rémunération éventuelle de ses inventeurs.

103. En outre, les Partenaires s'engagent :

- à ce que les noms des inventeurs soient mentionnés dans les demandes de brevet, sauf refus écrit exprès de ceux-ci, conformément aux dispositions légales en vigueur ;
- et à ce que leur personnel respectif, cité en tant qu'inventeur, donne toute signature et accomplisse toutes formalités nécessaires pour le dépôt, le maintien et la défense des brevets déposés par les Partenaires.

104. En tout état de cause, le Partenaire cédant ou renonçant à ses droits percevra une compensation proportionnelle correspondant à une Rémunération équivalente au Prix du marché.

12.1.1 PROPRIÉTÉ DES LOGICIELS

105. Les Logiciels de Base sont la propriété du Partenaire qui les a développés.

106. Les Adaptations réalisées dans le cadre du présent Contrat sont, quel qu'en soit l'auteur, la propriété du Partenaire propriétaire du Logiciel de Base.

107. Dans l'hypothèse où les Adaptations généreraient des droits d'auteur au profit du Partenaire qui les a réalisées, il recevra au titre de la cession au Partenaire propriétaire du Logiciel de Base une Rémunération équivalente au Prix du marché.

108. Sans préjudice des dispositions précédentes, chaque Partenaire demeure propriétaire des Extensions qu'il a réalisées seul dans le cadre du présent Contrat. Les Extensions réalisées en commun par deux ou plusieurs Partenaires sont la propriété commune de ces Partenaires, à proportion de leurs Contributions, quel que soit le Partenaire propriétaire du Logiciel de Base dont ces Extensions dérivent.

109. Les Logiciels Nouveaux développés dans le cadre du présent Contrat sont la propriété de la Partie qui les a développés seule. Les Logiciels Nouveaux Communs sont la propriété commune des Partenaires ayant participé à leur obtention, à proportion de leurs Contributions.

Les Parties Copropriétaires prendront toutes dispositions contractuelles (ex : cession de quote-part de copropriété) nécessaires au respect de l'équilibre prévu par le présent article, en respectant la Règle de Proportionnalité.

110. Les Partenaires s'interdisent d'intégrer au Projet des Logiciels Libres/Open Source sans l'accord préalable, écrit et unanime des Partenaires.

111. En outre, les Partenaires s'interdisent d'utiliser des Logiciels Libres/Open Source, dans le cadre de la réalisation de leur Part des Travaux ou de toute autre manière que ce soit dans le cadre de l'exécution du présent Contrat, si cette utilisation devait porter atteinte aux droits des Partenaires sur les Résultats du Projet.

112. L'utilisation et/ou l'intégration de Logiciels Libres/Open Source dans le cadre du Projet devra faire l'objet d'une décision prise au cours d'une réunion du Comité de Pilotage.

113. Par principe, il est convenu entre les Parties que l'utilisation de logiciels Open Source bénéficiant d'une Licence Open source contaminante est interdite.

12.2 PROTECTION DES RÉSULTATS

114. Les Partenaires s'engagent à assurer une traçabilité de leurs Résultats Propres. Les Partenaires concernés, le Coordinateur veille à la bonne exécution de ces obligations de traçabilité.

115. Pour les Résultats Conjoints, les décisions relatives à leur traçabilité sont prises par le Comité de pilotage et exécutées par le Coordinateur.

116. Lorsqu'un Résultat appartient à un seul Partenaire, ce dernier assure seul la protection de celle-ci et décide seul des moyens de protection adéquats.

117. Lorsqu'un Résultat est détenu en copropriété par plusieurs Partenaires, les décisions relatives à sa protection sont, sous réserve des dispositions relatives aux Résultats Conjoints brevetables exposées ci-dessus, prises par les Partenaires Copropriétaires, conformément aux termes de l'accord de copropriété passé.

Dans le cas où au moins deux (2) Partenaires Copropriétaires d'un Résultat Conjoint seraient des personnes publiques investies d'une mission de recherche, et en accord avec les dispositions prévues par le décret n° 2020-24 du 13 janvier 2020 relatif à la gestion de la copropriété des résultats de recherche, au mode de désignation et aux missions du mandataire unique prévu à l'article L. 533-1 du Code de la recherche, ces Partenaires désigneront parmi eux, pour chaque Résultat Conjoint concerné, un mandataire unique (ci-après désigné « Mandataire Unique »). Le Mandataire Unique sera notamment l'interlocuteur du Gestionnaire de la PI dans le cas où ce dernier et le Mandataire Unique seraient deux Parties distinctes.

Les frais de dépôt, d'obtention et de maintien en vigueur des brevets nouveaux en copropriété uniquement entre des Partenaires personnes publiques investies d'une mission de recherche seront supportés par le Mandataire Unique, sous réserve des accords conclus entre eux.

12.3 UTILISATION ET EXPLOITATION DES RÉSULTATS

12.3.1 (CO)PROPRIÉTAIRE(S)

118. Le Partenaire propriétaire d'un Résultat Propre l'utilise et/ou l'exploite librement, directement ou indirectement, sous réserve des droits accordés par le Contrat aux autres Partenaires.

119. Les Partenaires Copropriétaires d'un Résultat Conjoint l'exploitent conformément aux termes du contrat de copropriété passé entre eux. Il est entendu que ce contrat de copropriété doit respecter et faire référence à la Règle de proportionnalité et à la Règle du Prix du marché.

120. Il est d'ores et déjà convenu entre les Parties que toute exploitation directe et/ou indirecte par un Partenaire Copropriétaire des Résultats Conjoints impliquera une Rémunération équivalente au Prix du marché au profit des autres Partenaires copropriétaires.

12.3.2 UTILISATION ET EXPLOITATION DES RÉSULTATS (PROPRES OU CONJOINTS) PAR LES PARTENAIRES NON PROPRIÉTAIRES

121. Chaque Partenaire peut obtenir, sur sa demande et contre une Rémunération équivalente au Prix du marché, un droit d'utilisation des Résultats Propres et/ou Conjoints des autres Partenaires pour ses besoins de recherche interne et dans le cadre de collaborations de recherche avec des tiers, à l'exclusion de toute utilisation, directe et/ou indirecte, à des fins industrielles et/ou commerciales. La demande doit être formulée pendant la durée du Contrat.

Cette licence d'utilisation donnera lieu à la signature entre les Partenaires concernés d'un accord écrit préalable, précisant les droits concédés, leur étendue, leur destination, le lieu et la durée de la licence, ainsi que les modalités financières de celle-ci. Il est entendu que la licence fera référence et application de la Règle du Prix du marché. A défaut de demande formulée pendant le délai mentionné ci-dessus, le(s) Partenaire(s) concédant le droit d'exploitation redevien(en)t libre d'exploiter ou faire exploiter ses(leurs) Résultats, y compris par le biais d'une licence exclusive.

12.3.3 UTILISATION ET EXPLOITATION DES LOGICIELS DÉRIVÉS

122. L'utilisation et l'exploitation des Logiciels constituant des Adaptations sont régies par les dispositions applicables aux Connaissances Propres des Partenaires.

123. Sans préjudice des dispositions de l'article 11 du présent Contrat, l'exploitation industrielle et/ou commerciale d'un logiciel constituant une Extension par la/les Partenaire(s) titulaire(s) des droits sur ladite Extension devra faire l'objet d'un accord préalable du Partenaire titulaire des droits sur le Logiciel de Base duquel est dérivée l'Extension.

12.4. LES PARTENAIRES CONCERNÉS PRÉCISERONT LES MODALITÉS DE CETTE EXPLOITATION DANS LE CADRE D'UN ACCORD DE VALORISATION NÉGOCIÉ AVANT TOUTE EXPLOITATION INDUSTRIELLE ET/OU COMMERCIALE. LES PARTENAIRES S'ENGAGENT À CE QUE L'ACCORD DE VALORISATION RESPECTE LA RÈGLE DE PROPORTIONNALITÉ ET LA RÈGLE DU PRIX DU MARCHÉ. DIFFUSION DES

Résultats (propres ou conjoints) par les Partenaires a des fins pédagogiques et de recherche

Compte tenu de l'objectif pédagogique et de recherche poursuivi par le Projet qui vise à créer des retombées futures pour la filière « Cyber », les Parties s'engagent à diffuser les Résultats en lien avec le Projet au public sous la licence Creative Commons CC-BY, ou sous une licence équivalente.

Sont exclus des dispositions du présent article, les Résultats listés en Annexe qui ont vocation à être commercialisés auprès du public par les Partenaires titulaires de ces Résultats.

Article 13. Confidentialité

125. Les Partenaires s'engagent à observer et faire observer la plus stricte confidentialité à l'égard des Informations Confidentielles, et à prendre toutes mesures nécessaires pour en préserver la confidentialité, à l'égard notamment de leur personnel permanent ou temporaire et de leur sous-traitant amenés à avoir connaissance des Informations Confidentielles.

126. A cet effet, les Partenaires s'engagent à :

- ce que les Informations Confidentielles soient protégées et gardées confidentielles ;
- ce que les Informations Confidentielles reçues soient traitées avec le même degré de précaution et de protection que celui accordé à leurs propres Informations Confidentielles ;
- ne pas utiliser les Informations Confidentielles dans un but autre que l'exécution du Projet, sauf à obtenir l'accord écrit, exprès et préalable du(ou des) Partenaire(s) titulaire(s) ;
- ne révéler les Informations Confidentielles qu'aux membres de leur personnel impliqués dans l'exécution du Projet ;
- ne révéler les Informations Confidentielles aux tiers impliqués dans l'exécution du Projet, et notamment aux sous-traitants, qu'après avoir sollicité l'accord écrit, exprès et préalable du Partenaire titulaire ;
- prendre toutes les dispositions nécessaires pour que tous les membres de leur personnel et tous les tiers impliqués dans l'exécution du Projet, qui auront communication d'Informations Confidentielles, s'engagent à traiter les Informations avec le même degré de confidentialité que celui résultant du présent Contrat ;
- signaler le caractère confidentiel des Informations Confidentielles aux membres de leur personnel et à tous les tiers impliqués dans l'exécution du Projet, dès la communication de ces Informations ;
- rappeler le caractère confidentiel des Informations Confidentielles avant toute réunion au cours de laquelle des Informations Confidentielles seront communiquées ;

- maintenir les formules de copyright, de confidentialité, d'interdiction de copie, ou toutes autres mentions de propriété ou de confidentialité, figurant sur les différents éléments communiqués, qu'il s'agisse des originaux ou des copies.

127. En outre, les Partenaires s'interdisent :

- toute divulgation quelle qu'elle soit, à quelque tiers que ce soit, des Informations Confidentielles, sauf accord écrit exprès et préalable du ou des Partenaire(s) titulaire(s) ;

- de déposer en leur seul nom une demande de brevet sur les Informations Confidentielles dont ils ne sont pas titulaires, et plus généralement un titre de propriété industrielle quel qu'il soit ;

- d'effectuer des copies, reproductions ou duplications de tout ou partie des Informations Confidentielles, sauf accord écrit exprès et préalable du ou des Partenaire(s) titulaire(s) ;

- de se prévaloir, du fait de la communication des Informations Confidentielles, d'une quelconque cession, concession de licence ou d'un quelconque droit de possession antérieur, tel que défini par le Code de la Propriété Intellectuelle, sur les Informations Confidentielles.

128. Les Partenaires reconnaissent et acceptent que les Résultats ne générant pas de droits de Propriété Intellectuelle ni un savoir-faire secret, quel que soit le Partenaire qui les a créés, auront vocation à être largement diffusés, ne constituant alors pas des Informations Confidentielles, dès lors que ces éléments auront été considérés comme tels par les Parties au sein des organes de gouvernance mis en place au titre du présent Contrat.

129. Les Partenaires se portent-fort du respect des présents engagements par toute personne, physique ou morale, à laquelle ils auraient communiqué les Informations Confidentielles.

130. Les Partenaires reconnaissent que toutes les Informations Confidentielles, sans aucune exception, ont un caractère secret au sens donné par l'article 226-13 du Code pénal qui punit d'un (1) an d'emprisonnement et de 15 000 euros d'amende la révélation d'une information à caractère secret.

131. Les présents engagements de confidentialité s'imposent aux Partenaires pour toute la durée du Contrat et aussi longtemps que ces obligations demeurent en vigueur.

132. Afin d'assurer une traçabilité des Informations confidentielles échangées, la liste des Informations confidentielles, annexée au Contrat, sera mise à jour par le Coordinateur à chaque fois qu'une Information confidentielle sera communiquée à un Partenaire.

133. Le Comité de pilotage et les Comités opérationnels veillent au respect des présents engagements de confidentialité. Tout manquement d'un Partenaire pourra donner lieu, à l'initiative d'un ou plusieurs Partenaire(s), au déclenchement d'une enquête, et pourra constituer une cause d'exclusion de ce Partenaire, conformément aux dispositions de l'article « Exclusion d'un Partenaire ». En tout état de cause, à titre de mesure conservatoire, le Partenaire défaillant ne recevra plus, à compter du constat de son manquement et jusqu'à ce qu'il soit statué sur celui-ci, aucune Information Confidentielle.

134. À tout moment, le Partenaire titulaire pourra exiger du Partenaire récipiendaire la restitution ou la destruction sans délai de tout ou partie des Informations Confidentielles communiquées.

135. Il en sera de même à la fin du Contrat, ainsi que dans l'hypothèse où un Partenaire renoncerait au Consortium ou en serait exclu.

136. Les présents engagements de confidentialité se substituent aux engagements de confidentialité que les Partenaires auraient pu prendre les uns à l'égard des autres avant la signature du Contrat et qui concernent le Projet.

Article 14. PUBLICATIONS ET COMMUNICATIONS

137. Les Partenaires conviennent que toute publication ou communication relative au Projet doit intervenir dans le respect des obligations de confidentialité et des droits de Propriété Intellectuelle des Partenaires.

138. Sous cette réserve, chaque Partenaire est libre de faire toute publication ou communication qu'il souhaite sur ses Connaissances Propres et sur ses Résultats.

139. Les Partenaires s'engagent à rendre disponible en libre accès toutes les publications scientifiques sous la licence Creative Commons CC-BY ou équivalente.

139. Tout projet de publication ou communication d'un Partenaire, concernant tout ou partie du Projet et/ou des Résultats dont le Partenaire intéressé n'est pas l'unique propriétaire, doit être soumis à l'autorisation préalable du Coordinateur et des Partenaires concernés.

140. A cette fin, le projet de publication ou communication, ou un résumé de celui-ci, doit être remis au Coordinateur et aux partenaires concernés par lettre recommandée avec avis de réception ou mail avec avis de réception. A compter de la réception du projet de publication ou communication, le Coordinateur et les partenaires concernés ont un délai de quinze (15) jours pour se prononcer ; à défaut de réponse dans ce délai, le projet de publication ou communication est considéré comme accepté.

141. Dans le délai imparti, le Coordinateur peut demander au Partenaire intéressé :

- d'apporter des modifications à son projet si certaines informations sont susceptibles de compromettre l'utilisation commerciale et industrielle des Résultats, à condition que les modifications n'altèrent pas la valeur scientifique du projet ;
- d'apporter des modifications à son projet s'il contient des Informations Confidentielles d'une des Parties ;
- de reporter la publication ou communication envisagée pour une durée à préciser, notamment si la publication ou communication porte sur des Résultats devant faire l'objet d'une protection par la Propriété Intellectuelle.

142. Toutefois, l'autorisation préalable du Coordinateur ne doit pas faire obstacle :

- aux règles habituelles de soutenance de thèse, à condition que les examinateurs soient soumis à des obligations de confidentialité ;
- à l'obligation que peut avoir un Partenaire de soumettre un rapport d'activité à l'Etat ou à l'administration à laquelle il appartient ou envers qui il a des obligations (organisme financeur par ex.), car il ne s'agit alors pas d'une divulgation publique.

143. Les présents engagements s'imposent aux Partenaires pour toute la durée du Contrat et pour une durée de six (6) mois la fin de celui-ci.

144. Les Partenaires acceptent et reconnaissent que les Résultats générant des droits de Propriété Intellectuelle, et/ou relevant d'un savoir-faire secret, doivent être diffusés dans le respect des obligations de confidentialité et des droits de Propriété Intellectuelle des Partenaires, selon la procédure supra faisant intervenir le Coordinateur et le cas échéant les Partenaires concernés.

145. A contrario, les Partenaires acceptent de ne pas entraver ou faire obstacle à une publication ou une communication relative aux Résultats ne générant pas de droits de Propriété Intellectuelle et/ou ne relevant pas d'un savoir-faire secret.

146. Tout projet de publication ou communication d'un Partenaire, concernant tout ou partie du Projet dont le Partenaire intéressé n'est pas l'unique propriétaire, doit être soumis à l'autorisation préalable du Coordinateur.

147. A cette fin, le projet de publication ou communication, ou un résumé de celui-ci, doit être remis au Coordinateur par lettre recommandée avec avis de réception ou par mail avec avis de réception. A compter de cette date, le Coordinateur a un délai de quinze (15) jours pour se prononcer ; à défaut de réponse dans ce délai, le projet de publication ou communication est considéré comme accepté.

148. Dans le délai imparti, le Coordinateur peut demander au Partenaire intéressé :

- d'apporter des modifications à son projet si certaines informations sont susceptibles de compromettre l'utilisation commerciale et industrielle des Résultats, à condition que les modifications n'altèrent pas la valeur scientifique du projet ;

- de reporter la publication ou communication envisagée pour une durée à préciser, notamment si la publication ou communication portent sur des Connaissances Propres ou Résultats devant faire l'objet d'une protection par la Propriété Intellectuelle.

149. Toutefois, l'autorisation préalable du Coordinateur ne doit pas faire obstacle :

- aux règles habituelles de soutenance de thèse, à condition que les examinateurs soient soumis à des obligations de confidentialité ;

- à l'obligation que peut avoir un Partenaire de soumettre un rapport d'activité à l'Etat ou à l'administration à laquelle il appartient, car il s'agit alors d'une communication interne et non d'une divulgation publique

150. Les présents engagements s'imposent aux Partenaires pour toute la durée du Contrat et pour une durée de six (6) mois après la fin de celui-ci.

Article 15. INTUITU PERSONAE

151. Le Contrat est conclu intuitu personae, en considération de la personne des Partenaires.

152. Aucun Partenaire ne pourra transférer ou céder, en tout ou en partie, ses droits et obligations en vertu du Contrat à un tiers, sans avoir obtenu au préalable une autorisation du Coordinateur.

153. Toutefois, dans l'hypothèse où le transfert ou la cession serait fait dans le cadre d'une transmission universelle de patrimoine, l'accord du Coordinateur ne pourra pas être refusé de manière déraisonnable. Dans ce cas, seul la concurrence que le nouveau Partenaire pourrait faire à un autre Partenaire sera de nature à justifier un refus de transfert ou cession ou encore pour une cause ne dépendant pas des Partenaires mais d'un autre organisme ou administration, telle qu'un organisme de financement ou une autorité de régulation.

154. A compter du transfert ou de la cession, le nouveau Partenaire sera subrogé dans les droits et obligations du Partenaire cédant.

155. De même il est ici également rappelé que le changement de contrôle est encadré par les dispositions du présent Contrat.

Article 16. SOUS-TRAITANCE

156. Chaque Partenaire peut faire appel à un ou plusieurs sous-traitant(s) pour la réalisation de parties techniques liées à ses Contributions au Projet.

157. Sans préjudice des règles applicables en matière de sous-traitance ou des éventuelles sujétions imposées par les organismes de financement, le sous-traitant retenu sera considéré comme valable, s'il est soumis à la signature préalable d'un accord de confidentialité entre le Partenaire intéressé et le sous-traitant, et s'il comporte une clause par laquelle le sous-traitant renonce à tous droits de Propriété Intellectuelle sur les prestations qu'il réalise dans le cadre du Projet étant précisé que cette cession ne saurait porter sur les droits de Propriété Intellectuelle acquis ou créés antérieurement par le sous-traitant indépendamment de la réalisation des prestations qu'il réalise dans le cadre du Projet.

Article 17. GARANTIE DE JOUISSANCE PAISIBLE

158. Chaque Partenaire garantit les autres Partenaires contre toute action en contrefaçon engagée à leur encontre du fait des Connaissances Propres ou Résultats dont il est propriétaire.

159. A ce titre, chaque Partenaire s'engage à intervenir dans toute action en contrefaçon de droit d'auteur, brevet, marques, dessins et modèles, ou autre, engagée à l'encontre d'un autre Partenaire du fait des Connaissances Propres ou Résultats dont il est propriétaire, à condition :

- que le Partenaire ait utilisé les Connaissances Propres ou les Résultats conformément au présent Contrat,
- que le Partenaire assigné en contrefaçon lui notifie, à bref délai par écrit, l'action en contrefaçon ou la déclaration précédant celle-ci,
- qu'il soit mis en mesure par le Partenaire assigné en contrefaçon d'assurer la défense de ses propres intérêts et de ceux du Partenaire assigné en contrefaçon et, pour ce faire, que le dit Partenaire collabore loyalement à la défense en fournissant tous les éléments, informations et assistances nécessaires pour mener à bien cette défense.

161. Chaque Partenaire s'engage à prendre à sa charge, dans la limite des stipulations du présent Contrat, les dommages et intérêts auxquels un autre Partenaire pourrait le cas échéant être condamné à payer, au titre de la contrefaçon du fait des Connaissances Propres ou Résultats dont il est propriétaire.

Article 18. RESPECT DES OBLIGATIONS SOCIALES

162. Les Partenaires certifient et attestent sur l'honneur embaucher du personnel pour lequel ils respectent l'ensemble des obligations légales et règlementaires mises à leur charge en qualité d'employeur, notamment en ce qui concerne les déclarations préalables à l'embauche, la durée du travail, le respect des dispositions légales en matière de prise de repos et des dispositions relatives aux conditions de travail, à l'hygiène et à la sécurité.

163. En conséquence, chaque Partenaire garantit les autres Partenaires contre toute action émanant d'un tiers et/ou d'une administration du fait du non-respect des obligations ci-dessus énoncées.

Article 19. RÉSILIATION

164. Sans préjudice des dispositions du présent Contrat en matière de retrait ou d'exclusion d'un Partenaire, le Contrat pourra être résilié dans son ensemble, pour quelle que cause que ce soit, sur décision du Comité de pilotage prise à l'unanimité.

Article 20. DISPOSITIONS GÉNÉRALES

20.1 INTÉGRALITÉ

165. Le Contrat exprime l'intégralité des obligations des Partenaires.

20.2 NULLITÉ

166. Si une ou plusieurs stipulations du Contrat venaient à être tenues pour non valides ou déclarées comme telles en application d'une loi, d'un règlement ou à la suite d'une décision passée en force de chose jugée d'une juridiction compétente, les autres stipulations garderont toute leur force et leur portée.

20.3 TITRES

167. En cas de difficultés d'interprétation entre l'un quelconque des titres figurant en tête des clauses, et l'une quelconque des clauses, les clauses prévaudront.

20.4 SINCÉRITÉ

168. Les Partenaires déclarent sincères les présents engagements.

169. À ce titre, ils déclarent ne disposer d'aucun élément à leur connaissance qui, s'il avait été communiqué, aurait modifié le consentement des autres Partenaires.

20.5 INDÉPENDANCE DES PARTENAIRES

170. Chaque Partenaire est indépendant et agit en son nom propre et sous sa seule responsabilité. Chaque Partenaire s'interdit donc de prendre un engagement au nom et pour le compte d'un autre et demeure en outre intégralement responsable de son personnel, ses prestations, ses produits et services.

20.6 NON-SOLLICITATION DU PERSONNEL

171. Les Partenaires s'engagent à ne pas débaucher ou embaucher le personnel d'un autre Partenaire pendant toute la durée du Contrat et pendant une durée de un (1) an à compter de la fin de celui-ci, sauf accord expresse du Partenaire concerné.

20.7 EXÉCUTION LOYALE

172. Les Partenaires s'engagent à exécuter leurs obligations avec une parfaite bonne foi.

20.8 TOLÉRANCE

173. Les Partenaires conviennent réciproquement que le fait pour l'un d'entre eux de tolérer une situation n'aurait pas pour effet d'accorder aux autres des droits acquis. Une telle tolérance ne pourrait être interprétée comme une renonciation à faire valoir les droits en cause.

20.9 LOI APPLICABLE

174. Le présent contrat est régi par la loi française. Il en est ainsi tant pour les règles de fond que pour les règles de forme.

20.10 Règlement des différends

175. Les Partenaires se comporteront de manière à résoudre à l'amiable tout différend qui pourrait s'élever à l'occasion de l'interprétation ou de l'exécution du Contrat, notamment par le biais du Coordinateur et du Comité de Pilotage.

176. En cas de désaccord persistant au-delà d'un délai d'un (1) mois à compter de sa survenance, le litige sera réglé en dernier ressort par les juridictions françaises compétentes.

20.11 Domiciliation

177. Les Partenaires élisent domicile au lieu de leur siège social.

20.12 Notification

178. Toutes les notifications pour être valides, devront être effectuées à l'adresse de domiciliation.

Article 21. Annexes

Annexe 1 : Description du Projet (documents tels que sélectionnés pour financement par l'ANR)
Annexe 2 : Annexes financières (document tels que sélectionné pour financement par l'ANR)
Annexe 3 : Connaissances Propres
Annexe 4 : Informations Confidentielles
Annexe 5 : Résultats non soumis à la licence Creative Commons CC-BY, ou sous une licence équivalente
Annexe 6 : Échéancier de versement de l'aide aux Partenaires

Article 22. Signatures

Pour	Pour
Nom ____________	Nom ____________
Qualité ____________	Qualité ____________
Date ____________	Date ____________
Signature	Signature
Pour	Pour
Nom ____________	Nom ____________
Qualité ____________	Qualité ____________
Date ____________	Date ____________
Signature	Signature
Pour	Pour
Nom ____________	Nom ____________
Qualité ____________	Qualité ____________
Date ____________	Date ____________
Signature	Signature
Pour	Pour
Nom ____________	Nom ____________
Qualité ____________	Qualité ____________
Date ____________	Date ____________

Signature	Signature
Pour	Pour
Nom ______________	Nom ______________
Qualité ______________	Qualité ______________
Date ______________	Date ______________
Signature	Signature
Pour	Pour
Nom ______________	Nom ______________
Qualité ______________	Qualité ______________
Date ______________	Date ______________
Signature	Signature
Pour	Pour
Nom ______________	Nom ______________
Qualité ______________	Qualité ______________
Date ______________	Date ______________
Signature	Signature

Annexe 1 : Description du Projet (documents tels que sélectionnés pour financement par l'ANR)

Annexe 2 : Annexes financières (documents tels que sélectionnés pour financement par l'ANR)

Annexe 3 : Connaissances Propres

Partenaire	Connaissances propres

Annexe 4 : Informations Confidentielles

Partenaire	Informations confidentielles

Annexe 5 : Résultats non soumis à la licence Creative Commons CC-BY, ou sous une licence équivalente

Partenaire	Résultats
Campus Cyber	Scénario, contenus audiovisuels, modèle économique et données d'exploitation relatifs aux livrables « Serious game » et « Escape game » décrit dans le document « Description du Projet » (documents tels que sélectionnés pour financement par l'ANR)

ANNEXE 6 : ÉCHÉANCIER DE VERSEMENT DE L'AIDE AUX PARTENAIRES

Partenaire	Janvier 2024	Janvier 2025	En 2026 (date à préciser)	Janvier 2027	Janvier 2028
Onisep	45 188,02 €	41 080,02 €	41 080,02 €	36 972,02 €	20 540,01 €
PIX	318 401,62 €	188 664,07 €	143 405,92 €	70 943,47 €	35 500,24 €
Class Code	106 197,73 €	86 889,05 €	86 889,05 €	67 580,38 €	38 617,36 €
Radio France	584 318,35 €	166 948,10 €	584 318,35 €	166 948,10 €	0,00 €
CGenial	29 206,80 €	29 206,80 €	29 206,80 €	29 206,80 €	29 206,80 €
Root me Pro	168 386,45 €	48 110,41 €	168 386,45 €	48 110,41 €	0,00 €
Women4Cyber	64 543,50 €	64 543,50 €	64 543,50 €	64 543,50 €	64 543,50 €
CNED	285 000,00 €	76 000,00 €	361 147,40 €		
Université Panthéon Sorbonne	112 328,20 €	188 667,56 €	189 909,85 €	11 500,00 €	
Université Sorbonne Paris Nord	8 497,22 €	123 024,94 €	184 722,13 €	184 722,13 €	244 849,18 €
CY Cergy Paris Université	1 260 878,40 €	1 260 878,40 €	1 260 878,40 €	1 260 878,40 €	1 260 878,40 €
Académie de Versailles	36 000,00 €	36 000,00 €	36 000,00 €	36 000,00 €	36 000,00 €

Conformément à l'article 5.2 du Contrat attributif d'aide N°ANR-23-CMAS-0020, le solde de l'aide (10% du montant de l'aide accordée) est versé après réception et validation du compte-rendu de fin de Projet. Le versement du solde est ajusté pour tenir compte de la dépense réelle dans la limite du montant de l'aide.

APPEL A MANIFESTATION D'INTERETS
COMPETENCES ET METIERS D'AVENIR - CMA
2022

CATEGORIE : DISPOSITIF DE FORMATION

DOCUMENT PROJECT OVERVIEW

Acronyme du projet
TAL-CYB

Les données à fournir dans cette page sont aussi demandées en ligne sur le site de soumission de l'action CMA et pourrons faire l'objet d'une communication par l'ANR et la CDC dès la sélection des projets.

<table>
<tr><td>Acronyme</td><td colspan="3">TAL-CYB</td></tr>
<tr><td>Titre du projet</td><td colspan="3">Talents Cybersécurité</td></tr>
<tr><td>Secteur(s) éligible(s) aux priorités France 2030
(Voir annexe 2 de l'AMI)</td><td colspan="3">Cybersécurité,
Education et numérique</td></tr>
<tr><td>Type(s) de formation envisagée(s)</td><td colspan="3">☒ Scolaire ☒ Supérieur
☒ Formation continue</td></tr>
<tr><td>Formation(s) visée(s)</td><td colspan="3">Licences, Masters, Doctorats, Secondaire, MOOC, évaluations et certifications des compétences</td></tr>
<tr><td>Branche professionnelle concernée (si pertinent)</td><td colspan="3">Numérique – cybersécurité</td></tr>
<tr><td>Suite d'un projet CMA « Diagnostic »</td><td colspan="3">☒ Non ☐ Oui, préciser :</td></tr>
<tr><td>Sur modèle(s) d'outil(s) PIA préexistant(s)</td><td colspan="3">☐ NON ☒ OUI, préciser :
☒ CMQe ☐ EUR ☐ IDEFI ☒ NCU
☐ IFPAI ☐ PFPE
☐ Autre :</td></tr>
<tr><td>Mots-clefs</td><td colspan="3">Cybersécurité, formation par projet, attractivité, orientation, souveraineté, mutualiser, talents, renforcer, apprentissage par le jeu, socle commun de ressources, creative commons</td></tr>
<tr><td>Chef de file</td><td colspan="3">Campus Cyber</td></tr>
<tr><td rowspan="4">Responsable du projet</td><td colspan="3">NOM, Prénom et fonction</td></tr>
<tr><td colspan="3">Yann Bonnet,
Directeur général délégué du Campus Cyber</td></tr>
<tr><td>Courriel</td><td colspan="2">Téléphone</td></tr>
<tr><td>yann@campuscyber.fr</td><td colspan="2">0660585796</td></tr>
<tr><td>Durée du projet
(maximum 5 ans)</td><td colspan="3">5 ans – 60 mois</td></tr>
<tr><td>Aide totale demandée</td><td>26 680 140 €</td><td>Coût complet (1)</td><td>53 702 108 €</td></tr>
</table>

(1) Préciser le statut du candidat au regard de la TVA ; assujetti ou non assujetti. Le coût complet correspond aux dépenses éligibles ; indiquer le montant HT si assujetti.

LISTE DES MEMBRES DU CONSORTIUM

Organismes de formation ou d'accompagnement (universités, écoles, lycées, CFA, organismes privés, Pôle emploi, etc.).	***Secteur(s) d'activité***
Université Sorbonne Paris Nord (Paris XIII)	***Enseignement supérieur et recherche***
Université Paris 1 Panthéon-Sorbonne	***Enseignement supérieur et recherche***
Université de Lorraine	***Enseignement supérieur et recherche***
CY Cergy Paris Université	***Enseignement supérieur et recherche***
Académie de Versailles	***Enseignement scolaire et supérieur***
GOBELINS, l'école de l'image	***Enseignement supérieur***
Association groupe ESSEC	***Enseignement supérieur***
CNED	***Formations certifiantes en ligne***
OPEN CLASSROOMS	***Formations certifiantes en ligne, cours en libre accès***
Fondation UNIT	***Enseignement supérieur et recherche***
Class Code	***Enseignement supérieur et recherche***
ONISEP	***Orientation et métiers***
PIX	***Evaluation, développement et certification de compétences numériques***
Entreprises	***Secteur(s) d'activité***
Campus Cyber	***Cluster de la cybersécurité***
TOD-The Oligarchs Digital (TOD)	***Production flux, divertissement et documentaire***
IX Campus	***Enseignement supérieur***
WebForce 3	***Enseignement supérieur***
Root me PRO	***Plateforme d'apprentissage par l'expérience***

Autres acteurs du monde socio-économique (groupements d'employeurs, organisations professionnelles, syndicats, fédérations professionnelles, OPCO, etc.)	***Secteur(s) d'activité***
Women4Cyber	***Association autour de la place des femmes en cybersécurité***
Fondation CGénial	***Fondation de culture scientifique, technique, numérique et découverte des métiers associés***
RADIO France	***Production, contenus audiovisuels***

Résumé du projet (Non confidentiel – 4000 caractères maximum, espaces inclus)

*Le projet Talents Cybersécurité est un **consortium de 21 partenaires**. Il propose de mettre en place de **nouvelles formations** en cybersécurité à destination des **spécialistes et non spécialistes**, du **secondaire au doctorat**, en **présentiel et en ligne**, du **module introductif à la formation diplômante**. Il propose également de produire des **contenus audio-visuels, ludiques et informatifs de qualité et variés** qui serviront pour la sensibilisation et l'acculturation du plus grand nombre ainsi qu'aux diverses formations des membres du consortium et au-delà.*

*Le domaine de la cybersécurité est un secteur clef pour les économies nationales : les cyberattaques apparaissent dans le **Top 10 des risques business** selon le Forum Economique mondial et leur nombre ne cesse d'augmenter. Toutefois, la filière cybersécurité **manque de talents** et souffre d'un **déficit d'image qui nuit à son attractivité,** ce qui se traduit par une insuffisance voire absence de candidats à certaines formations existantes. Pour répondre à cette situation, le projet Talents Cybersécurité vise à **promouvoir les métiers en travaillant l'attractivité de la filière**.*

*Le projet Talents Cybersécurité distingue trois leviers d'action : **attirer / acculturer, orienter et former**. Il s'agira non seulement de sensibiliser très tôt les élèves du secondaire et de former plus d'étudiants à la cybersécurité mais aussi en de rendre la filière attractive et de faciliter l'orientation.*

*Avec les partenaires CY Cergy Paris Université, Université Sorbonne Paris Nord, Université Paris 1 Panthéon-Sorbonne, Université de Lorraine, académie de Versailles, iXCampus, Association groupe ESSEC, OpenClassrooms, WebForce3, CNED, UNIT, Root me, ClassCode et PIX un dispositif de formation ambitieux sera mis en place, touchant tous les publics et tous les niveaux. **L'offre de formation diplômante**, pour les spécialistes ou non, de la licence au doctorat sera développée mais également **les certificats à destination des salariés** en up ou re skilling. En outre, le **référentiel de certification des compétences** en termes de cybersécurité de PIX sera renforcé. De **nombreuses ressources seront disponibles en licence libre de droit** afin de bénéficier à l'ensemble de l'écosystème : une bibliothèque de cas d'usage, des exercices pratiques de hacking éthique, des contenus de formation des formateurs, ou encore de nombreux modules de formation. Ainsi, ce sont plus de 17 000 personnes qui seront formés d'ici à la fin du projet et plus d'un million de personnes sensibilisées.*

*Avec les partenaires Radio France, TOD, Gobelins, Women4Cyber et Cgenial, **le grand public, les jeunes, les salariés et les femmes seront sensibilisés** par la production et la diffusion de contenu audiovisuel de qualité visant à faire connaître la filière et ses métiers. **Les élèves, apprentis et étudiants profiteront de ces contenus pour leur formation.** L'audience des contenus sera accrue via l'implication de médias à grande audience tels que Radio France ou France TV et les réseaux sociaux.*

*Enfin, avec le partenaire Gobelins, une **méta-plateforme d'orientation** sera mise en place et avec Onisep **l'information sur les métiers cyber** seront créées et disponibles pour les collégiens et lycéens.*

*Le projet Talents Cybersécurité sera déployé sur **60 mois.** Le budget total du projet s'élève à 53 702 108 €. L'aide demandée d'un montant de 26 680 140 € servira à développer de nouvelles formations et modules (86%), à créer des contenus en termes d'attractivité (6%) et d'orientation (9%). Les 27 021 968 € restants sont constitués de co-financements, d'apports des partenaires et des revenus générés par l'animation des contenus. **Grâce à l'élan généré par la subvention, la montée en maturité du dispositif sera assurée et sa pérennité à terme.** Cet AMI représente le moyen de rassembler les membres du consortium autour de ce projet ambitieux pour développer la filière cybersécurité en France et répondre au besoin de massification des formations.*

1. DESCRIPTION DU PROJET DE DISPOSITIF(S) DE FORMATION

1.1. PRESENTATION DU CONTEXTE

Les métiers de la cybersécurité sont en forte tension. L'enquête « Profil de la cybersécurité » menée par l'ANSSI en 2021 faisait état d'environ 15 000 postes vacants en 2019. Par ailleurs, il est aujourd'hui **difficile d'identifier des enseignants et formateurs disposant de l'expérience nécessaires pour démultiplier les compétences ainsi que produire et diffuser des contenus pédagogiques de qualité**.

L'écosystème de la cybersécurité en pleine mutation souffre ainsi d'un déficit d'image. Les formations en la matière ne sont pas assez remplies, voire sont obligées de fermer faute de candidats. Tandis qu'en Ile-de-France, 10 000 jeunes suivent des formations dans le secteur du numérique au niveau du bac, seul un nombre très faible d'entre eux s'oriente par la suite vers la filière cybersécurité, d'après la DGESCO[1]. En outre, le secteur est très largement masculin : 89% des professionnels actuels sont des hommes et seul 2 à 7% des effectifs suivant des options du numérique au lycée sont féminins. Au sein des entreprises, de nombreux DRH pensent que seuls des profils ingénieurs ou techniques peuvent se diriger vers les métiers de la cybersécurité, ce qui se traduit par **une orientation insuffisante et donc une perte de ressources compétentes et indispensables à la filière**. De plus, au regard de la montée en puissance du numérique et de la gestion des données, les connaissances et les compétences liées à la cybersécurité sont devenues l'affaire de tous. Il est ainsi nécessaire de les sensibiliser afin de favoriser une meilleure orientation pendant l'embauche et en cas de reconversion et/ou d'évolution de carrière.

Le Président de la République a annoncé en février 2021 la mise en place d'une stratégie nationale de cybersécurité via la mobilisation d'1 Md d'€. Dans ce cadre, l'Etat impulse la création du Campus Cyber**. Un des objectifs majeurs de cette stratégie nationale est de répondre aux enjeux en matière de compétences et de formation pour la filière cybersécurité. L'objectif est de créer 37 000 emplois à horizon 2025.**

1.2. CHEF DE FILE ET PHILOSOPHIE DU DOSSIER

Initié par le Président de la République, le Campus Cyber, lieu totem de la cybersécurité de 26 000m² rassemble 1 800 experts nationaux. **Parmi ses 200 acteurs issus d'une pluralité de secteurs d'activité, il fédère des entreprises (**grands groupes, PME), **des services de l'État** (ANSSI, ministère de l'Intérieur, ministère de l'éducation, ministère de l'enseignement supérieur et de la recherche, etc.)**, des organismes de formation, des acteurs de la recherche** (INRIA, IMT, CEA, CNRS, etc.) **et des associations** (Women4Cyber, CEFCYS, CESIN, etc.)[2]. Le Campus Cyber met en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs. **Un réseau de Campus Cyber régionaux est en cours de développement** : les Hauts-de-France à Lille ont le premier Campus labellisé. Le développement des échanges entre la recherche et les entreprises est au cœur du projet Campus Cyber. Opéré par Inria pour le compte de la communauté académique (CNRS, CEA, IMT), un **programme de transfert de la recherche publique dédié à la R&D et à l'innovation, permet une plus grande implication auprès des entreprises de la cybersécurité**. Le volet formation de ce programme a

[1] Direction Générale De L'enseignement Scolaire
[2] Voir annexe 1

pour objectifs de produire des contenus pédagogiques pour des formations en cybersécurité répondant au besoin des entreprises et exploitant les compétences et savoir des établissements et grandes universités de recherche, ainsi que de promouvoir les carrières dans le domaine. En outre, la diversité d'acteurs composant le Campus Cyber facilite les liens, notamment en termes de formation et d'emploi.

Après un travail de réflexion mené depuis 12 mois par une cinquantaine de membres du Campus Cyber (écoles, entreprises, acteurs publics, recherche), le Campus Cyber se positionne comme chef de file du projet « Talents cybersécurité ». **(1) Attirer / Acculturer, (2) orienter et (3) former telle est l'approche proposée par ce consortium car la filière cybersécurité fait face à une triple problématique :**

- **Le manque d'attractivité lié à une image erronée et à une méconnaissance du sujet :** le consortium développera du contenu et des programmes en matière d'attractivité, du contenu informatif et recensera les ressources existantes.
- **L'orientation insuffisante liée à une absence de connaissance de la diversité des métiers qui la compose :** le consortium développera des contenus informatifs sur les métiers et favorisera l'accès à des parcours de formations via une plateforme d'orientation.
- **La nécessité de création de nouveaux cursus pour répondre aux besoins en compétences en constante évolution et en ressources humaines des acteurs économiques :** le consortium travaillera avec les acteurs de l'écosystème pour développer des nouveaux cursus qui répondent à l'évolution de leurs besoins.

Ainsi, les actions de la feuille de route PIA cybersécurité auxquelles répond le consortium sont :

- Action 1 : développer l'offre de formation diplômante de niveau licence, master, doctorat via *CY Cergy Paris Université, Université Sorbonne Paris Nord, Université Paris 1 Panthéon-Sorbonne, Université de Lorraine, iXCampus, Association groupe ESSEC.*
- Action 2 : favoriser la reconversion et montée en compétences des professionnels via *OpenClassrooms, WebForce3, CNED.*
- Action 3 : certifier les compétences (durant le secondaire et le supérieur) via *PIX.*
- Action 4 : favoriser une meilleure connaissance des métiers et des formations pour les élèves et étudiants via *ONISEP, Gobelins, Académie de Versailles*
- Action 5 : travailler sur l'image de la filière et renforcer les vocations féminines via *Radio France, TOD, Fondation CGenial, Gobelins, Women4Cyber, Académie de Versailles.*
- Action 6 : construire des ressources éducatives communes et d'apprentissage par l'expérience via *UNIT, Root me, ClassCode, OpenClassrooms.*
- Action 7 : développer la recherche en cybersécurité via *CY Cergy Paris Université*.

1.2.1 Développement de programmes de formation diplômants et certifiants

L'objectif de cet axe est de créer des formations en cybersécurité accessibles à tous en s'adressant à quatre cibles différentes qui appellent des types de formations distincts :

- **Le grand public**
- **Les élèves, apprentis et étudiants en formation initiales : techniques ou non techniques**

- **Les salariés : les ingénieurs, développeurs et informaticiens en formation / de métier ou les salariés non techniques**
- **Les enseignants et formateurs**

<u>Action 1, 2 et 7 (Actions concernées de la feuille de route formation de la stratégie nationale cyber sécurité)</u>. CY Cergy Paris Université (CYU) et CY Tech pilote un **pôle dédié à l'innovation et la transformation digitale dans le domaine de la cybersécurité** dans l'ouest parisien. Les livrables du pôle sont complémentaires des actions d'orientation, de sensibilisation et de développement de briques pédagogiques en ligne développés dans le dossier sur les autres axes : **il s'agit d'accroitre substantiellement le nombre de diplômés de 1er cycle (BUT, bachelor), de 2e cycle (master, ingénieur) et dans le cadre de la formation tout au long de la vie (Mastère spécialisé de la CGE, DU, titre RNCP, VAE).** Cet accroissement s'appuie sur le développement d'une expertise haut niveau en cyber, favorisée par l'écosystème du Campus Cyber couplé à celui du CMQ sécurité d'Argenteuil (95): mise en réseau des chercheurs et professionnels ci-dessus mentionnés sous pilotage du campus cyber, financement de projet émergent en recherche et de chaires partenariales entreprises, recrutement de nouveaux professeurs sur le marché national et international.

L'approche pédagogique innovante du pôle se distingue par l'articulation de 4 dimensions rarement réunies :

- Des **apports académiques de haut niveau** grâce à la présence de chercheurs internationaux
- L'usage de **ressources pédagogiques numériques souveraines** développées par le Campus Cyber et les membres du consortium (décrites ci-après).
- Des **mises en situation systématique** (projets, brief d'entreprises, apprentissage) avec mise en perspective des enjeux de la transition digitale et écologique
- La **philosophie « cyber cross »** (pluridisciplinaire) qui articule les enjeux et exigences de la cybersécurité avec l'ensemble de ses champs d'application.

L'ouverture des nouvelles formations débutera dès septembre 2023, et s'étalera sur les trois années (2023, 2024 et 2025). A l'issue des 5 ans, le projet aura ainsi atteint le régime stationnaire de formation financé par le PIA. **Au total sur les 5 années[3], le projet aura permis de former 6 725 étudiants donc 4 025 en formation initiales et 2 520 stagiaires en formation continue. A l'issue des 5 ans, il formera de manière annuelle et auto-financée 1 800 étudiants dont 1 250 en formation initiale et 630 stagiaires en formation continue.** Le coût total de de cette action de 9,56M€, recherche et expertise incluse et hors frais de gestion, soit 1421€/ étudiant pour cette phase d'impulsion (1228€/étudiant pour les dépenses strictement pédagogiques). A noter que la plupart des formations sont des cursus complets, et pas seulement des modules complémentaires ou de sensibilisation pour des étudiants inscrits dans d'autres cursus. L'enjeu est de former de nouveaux experts, niveau technicien et ingénieur, en cyber et pour la cyber.

Le modèle économique du pôle est très simple et comprend 2 phases : la phase d'initiation et la phase de consolidation.

- **Phase d'initiation** :
    - Chaque premier groupe ouvert d'une nouvelle formation bénéfice **d'un package de démarrage de 250k€** pour la première année (et au pro rata si la formation ne dure

[3] Voir annexe 10

qu'une fraction d'année). Le package de 250k€ permet au lancement de recruter un enseignant chercheur par nouvelle formation, de constituer l'équipe pédagogique avec des ressources internes au consortium et externe (vacataires et entreprises), de financer les frais de la formation pour une année minimum (prestations, location d'espace, petite fourniture).

    - **Puis 100k€ par ouverture de groupe supplémentaire et 100k€ par ouverture d'une année de formation supplémentaire** lorsque le diplôme est construit sur 2 ou 3 ans. Pour les groupes et années supplémentaires, le package de 100k€ permet d'accompagner la montée en puissance de la formation avec le recrutement d'enseignants chercheurs supplémentaires (1/2 par groupe et par année), de la masse salariale et du fonctionnement.
- **Phase de consolidation** :
    - Les ressources propres du programme permettent d'accompagner sa **montée en puissance** (année 1, éventuellement 2 et 3)
    - Et **d'auto-financer et ainsi pérenniser** le programme de formation au plus tard 3 ans après son lancement. Pour les formations initiales, le modèle dominant est celui de l'apprentissage (mais on peut aussi avoir des chaires pédagogiques avec des entreprises du campus cyber), et pour la formation continue (y compris les mastères spécialisés), le modèle est celui des droits d'inscription (financement CPF, entreprise, reconversion et retour à l'emploi, individus).

Le pôle bénéficie d'un large écosystème d'experts, publics et privés, qu'il s'agira a) de faire vivre afin de mieux le mobiliser pour les formations et b) de lui permettre d'évoluer et d'innover régulièrement. Le projet comprend ainsi des **crédits d'émergence** à la fois pour initier des projets de recherche (40k€ en moyenne / projet, puis demandes ANR et Europe, notamment) et initier des chaires d'entreprises (60k€ du PIA pour 240k€ levés, soit 300k€) en pure cybersécurité et « cyber cross ». Ces programmes d'émergence sont financés pendant 4 ans (année 1 du projet = lancement du programme) et sera financé à l'issue du projet par les ressources propres des formations, sous la forme d'une redevance « émergence cyber » de 3% des recettes.

Les actions du pôle se détaillent ainsi[4] :

- **Axe 1 : Mettre en place un programme « émergence » cyber et cyber cross** (PIA 800k€, apport privé direct 960k€, apport direct CYU 440k€).
    - Programmes recherche et entreprises pour l'expertise en cybersécurité et autour de la cybersécurité (cyber cross : interdisciplinarité, partage d'expertise) : pendant 4 ans
    - 7 projets de recherche « émergence » à 60k€ (demande 40k€ et apport CYU 20k€) et 3 projets « émergence + » à env. 200k€ (avec PhD ou Post-doc, demande 100k€ et apport CYU 100k€)
    - 2 chaires cyber cross à 600k€ sur 2 à 4 ans (demande 120k€ et apport complément de 480k€ / chaire).
- **Axe 2 : Accroitre les diplômes de 1er cycle en cybersécurité** (PIA 1,45M€)
    - **Sous-axe 2.1 : création de nouveaux diplômes 1er cycle** (amorçage PIA 0,85M€ pour 920 étudiants, soit 923€/étud.) : 1) Bachelor professionnel au CMQ sécurité avec CY Tech et 2) Licence professionnelle à l'USPN, pour former 1145 étudiants

[4] Voir annexe 10

sur les 5 années du projet et 290 étudiants par an ensuite ; recrutement 5 EC (3 en année 1, puis 1 et 1)
  - **Sous-axe 2.2 : création d'une mineure en cybersécurité** pour les étudiants de CYU (PIA 50k€), passage de 1 à 5 groupe(s) de 40 chaque année, pour toute formation (sciences, sciences humaines et sociales), pour 600 étudiants sur le projet et 200 annuel ensuite.
  - **Sous-axe 2.3 : mise en place d'un « Pass Sup » entre l'académie de Versailles et CYU**, dispositif d'accompagnement d'élèves de 1ère technologique et professionnelle jusqu'à l'obtention d'une licence pro (cours et ateliers de renforcement, suivi personnalisé pour aider à l'élaboration du projet professionnel, des rencontres privilégiées entre étudiants et professionnels et une pédagogie de suivi de projets (PIA 100k€). Les lycées P-TECH seront particulièrement mobilisés.
- **Axe 3 : Accroitre les diplômes de 2e cycle en cybersécurité** (amorçage PIA 5,13M€)
  - **Sous-axe 3.1 : création de nouveaux diplômes et parcours en master 2 ans et en cycle ingénieurs 2 ou 3 ans** (amorçage PIA 1,15M€ pour 1245 étudiants, soit 923€/étud.), à CY Tech, à l'USPN, à l'ECAM-EPMI, pour former 1555 étudiants sur les 5 années du projet et 430 étudiants par an ensuite ; recrutement 6 EC (2 en année 1, puis 3, 1, 1)
  - **Sous-axe 3.2 : création de nouveaux doubles diplômes CY Tech - ESIEE-IT et CY Tech - CY école de design** (amorçage PIA 2,05M€ pour 1440 étudiants, soit 1423€/étud.), avec intégration de l'ingénierie système et du design dans les processus de définition des solutions cyber pour l'industrie ; 480 étudiants / an à l'issue du projet ; recrutement 7 EC (1 en année 1, puis 2, 2, 2)
  - **Sous-axe 3.3 : création de ressources pédagogiques experts et cas d'études** pour les master et parcours Grande Ecole (ESSEC Metalab), PIA 0,73M€
- **Axe 4 : Accroitre les diplômes de formation tout au long de la vie** (amorçage PIA M€)
  - **Sous-axe 4.1 : création de mastères spécialisés et MBA** (amorçage PIA 1,25M€ pour 1040 étudiants, soit 1201€/étud.) diplômes de spécialisation post bac+5 favorisant l'interdisciplinarité et l'intégration des en-jeux cyber dans l'industrie et le public ; 240 étudiants / an à l'issue du projet ; recrutement 6 EC (2 en année 1, puis 2, 2)
  - **Sous-axe 4.2 : création de certifications et modules de FTLV** (amorçage PIA 1,83M€ pour 1400 étudiants, soit 1285€/étud.) 360 étudiants / an à l'issue du projet ; recrutement 3 EC (1 en année 1, puis 1, 1)
  - **Sous-axe 4.3 : création de dispositif de VAE hybride** (amorçage PIA 100k€)
- **Axe 5 : management du pôle** (PIA 0,75M€), 1 chef de projet et 1 coordinateur des actions pédagogiques (profil ingénieur designer) soit 150k€/an.

Le plan RH de recrutement d'enseignants-chercheurs pour la création des nouveaux diplômes (hors certifications et modules ponctuels) est le suivant : 8 pour 2023-2024, 6 pour 2024-2025, pour 2025-2026, 3 pour 2026-2027, soit 23 enseignants-chercheurs avec des profils cyber pour l'essentiel, mais également en IA, data, réseau. Un lissage des recrutements en envisageable pour viser une **moyenne de 6 recrutements par an**. Le vivier de doctorants dans les laboratoires ETIS à CYU et LIPN à USPN, les réseaux nationaux et internationaux de ces labos permettent de garantir ce niveau soutenu de recrutement.

Action 1. **L'Université Sorbonne Paris Nord développera trois types de formation** :

- **Formations diplômantes** spécialistes :
  - **Une licence professionnelle** (PIA 432 000€) métiers des réseaux informatiques et de la télécommunication, accessible avec un bac+2 afin de former des professionnels experts capables d'appréhender des problématiques liées à la production, la transmission et la sécurisation et traitement des données numériques.
  - **Un parcours en 2ème année de master** informatique ainsi qu'un parcours ingénieur pour l'obtention d'un diplôme bac+5 (PIA 702 000€).
- **Formation courte** – 40h (PIA 64 800€) : module à destination des non-juristes qui les aident à prévenir et à réagir aux cyberattaques. Il ne s'agit donc pas de former des juristes, mais de **former des non-juristes à la communication avec les spécialistes du droit**, et ce, dans les trois piliers du droit de la cybersécurité : droit de la sécurité des systèmes d'information, droit de la lutte contre la cybercriminalité, droit de la cyberdéfense nationale.

Action 1. Le champ de **la cyber ne peut s'affranchir de la dimension humaine** qui en est indissociable. De nombreuses opérations d'influence émergentes visant les individus, les groupes sociaux, les entreprises, les institutions et les gouvernements. Il est donc primordial d'envisager cet enjeu majeur en intégrant outre les aspects techniques, les questions d'influence, de psychologie sociale, d'ingérence, mais aussi les enjeux juridiques induits par l'émergence continuelle de nouvelles cybermenaces. Ainsi, **l'Université Paris 1 Panthéon-Sorbonne développera un DU "Influence et Cybersécurité" (160h)** (PIA 550 634€) qui propose une approche innovante par la dimension humaine et technique de la compréhension des enjeux relatifs à la cybersécurité qu'il introduit grâce à l'expertise académique et pluridisciplinaire de l'Université Paris 1[5]. Il innove également par ses **pratiques pédagogiques hybrides combinant enseignements théoriques, cas d'usage, retours d'expérience, cycles de conférences données par des experts reconnus, ainsi qu'une mise en application au moyen d'une simulation réaliste et immersive de cyberattaque**. Ce cursus s'adresse aux **professionnels des secteurs publics et privés** (en poste, prise de poste ou reconversion) désireux de monter en compétence sur les aspects techniques et humains de la cybersécurité, et aux étudiants souhaitant développer cette expertise en complément de leur formation initiale.

Action 1. **L'université de Lorraine** et tout particulièrement sa composante TELECOM Nancy réalisera un ensemble de formations et d'outils pour **développer les compétences des élèves et des formateurs sur les plateformes de tir numérique** (cyber-range – PIA 323 274€). Les outils développés permettront la conception de scenarii et de séquences pédagogiques sur des plateformes multiples et assureront la portabilité de ces scenarii entre plateformes hétérogènes. Ils offriront également un support permettant, grâce à l'apprentissage automatique, de générer des scenarii dynamiques personnalisés par apprenant, en fonction des compétences ciblées et des besoins individuels (PIA 146 409€). Les contenus pédagogiques de formation des formateurs (qui seront amenés à opérer ces plateformes) ***seront accessibles à tous gratuitement, sous licence opensource*** *(Creative Commons – licence CC BY-SA)*.
L'Université de Lorraine et tout particulièrement son laboratoire LORIA développera un ensemble de **contenus logiciels et pédagogiques pour la formation des apprenants sur le domaine de l'analyse de Malwares** (PIA146 409€).

[5] Voir annexe 9

Les actions contribueront au développement conjoint à l'Université de Lorraine, d'un **nouveau cursus d'ingénieur par alternance co-porté par TELECOM Nancy et l'Ecole Nationale Supérieure des Mines de Nancy** (PIA 330 466€). Cette formation a vocation à accueillir ses premiers étudiants en septembre 2024.

Action 1. **Le CNED formera à distance des professionnels non spécialistes en cybersécurité de niveau 4 (Bac) et 5 (Bac+2)**[6] (PIA 695 601€)**.** Les profils visés sont des assistants, techniciens, etc. capables de mettre en place des processus destinés à prévenir et à parer des attaques cybersécurité dans des organisations de type PME, TPE ou collectivités territoriales. Cette solution propose à ces organisations, qui n'ont pas les moyens d'avoir des spécialistes cybersécurité, une formation 100% à distance **via les dernières avancées technologiques** comme un accès à des espaces Lab permettant de s'entraîner à l'Hacking Ethique sous forme de Challenge afin d'acquérir des compétences pratiques dans des environnements sécurisés. **1500 adultes par an** seront formés en Formation Professionnelle Continue (inscrite au RNCP et validé par un diplôme) via un **parcours de formation numérique de 400 heures**, décliné en 4 blocs de compétences. Le CNED déclinera cette proposition pédagogique en **2 modules gratuits d'acculturation**, à distance pour les bacheliers (12h) et les étudiants (20h) (PIA 108 551€).

Action 2. **Formation initiale, re-skilling, cross-skilling, up-skilling,** offre innovante proposée par OpenClassrooms qui s'appuie sur une **pédagogie par projet** et se fonde sur les expertises des membres du consortium. Ce sont **40 cours en accès libre, 45 modules et 3 parcours de formation certifiants (RNCP)** qui seront créés et rendus accessibles dans les 5 années du projet (PIA 3 812 335€). Via une articulation fine avec Root Me, le projet prévoit également la mise à disposition d'**espaces virtuels d'entraînement** facilitant l'interaction avec des **ressources vulnérables** et des **outils** de cybersécurité (PIA 405 792€). Cette offre adresse différents publics cibles - étudiants en formation initiale & en alternance ; demandeurs d'emplois ; salariés des PME et grandes entreprises, pour **former plus de 15 000** personnes à l'horizon 2030. Chaque étudiant suivant un parcours de formation bénéficie de l'accompagnement **100% individualisé via un mentor dédié**, ce qui limite les risques de décrochage[7]. L'intégralité des cours produits dans le cadre du projet **seront accessibles à tous gratuitement, sous licence opensource (Creative Commons) et formeront des "communs numériques"*.*** Ils pourront ainsi servir aux acteurs de l'enseignement supérieur et au réseau des professionnels de la formation qui pourront les utiliser notamment pour **la conception de cursus hybrides**.

Action 6. **ClassCode** mobilisera son expertise dans la production collaborative de **ressources éducatives libres** (licence CC BY-SA) pour produire un **MOOC**[8] **à destination des enseignants et du grand public**[9] (PIA 364 990€). Autrement dit, ces travaux viseront à créer des synergies entre l'expertise en recherche, le milieu professionnel ainsi que la **pédagogie active pour produire un parcours d'introduction à la cybersécurité**. Les ressources produites seront partagées en classe comme à la maison et utilisées de manière pratique par n'importe quelle personne souhaitant être un relais de connaissances. Ce **MOOC hybride sera relayé et animé sur les territoires sous la forme d'actions dans les classes** grâce aux partenaires du réseau ClassCode (PIA 64 774€).

[6] Voir annexe 8
[7] Voir annexe 7
[8] Massive Open Online Course
[9] Voir annexe 4

Action 6. La fondation UNIT pilotera la mise en place du **socle commun « CYBER pour l'enseignement supérieur » sous forme de ressources éducatives libres** (REL – licence CC BY-SA) déclinées en micro-contenus autonomes, facilement appropriables et réutilisables par les enseignants et les établissements[10] (PIA 1 117 056€). Le socle vise en priorité les **publics étudiants en Licence**, avec également quelques REL pour le niveau Master. L'objectif est double :

- Permettre à des étudiants d'accéder à une **large bibliothèque des REL relative aux enjeux de la cybersécurité** ;
- Proposer aux enseignants des REL avec lesquelles ils pourront facilement **hybrider leurs enseignements**, tant d'un point de vue pédagogique (ligne éditoriale commune pour les REL) que technologique (compatibilité avec les LMS des établissements d'enseignement supérieur).

UNIT supervisera donc la co-construction des REL, leur indexation, leur diffusion et leur valorisation via son portail, celui de L'Université Numérique et du Campus Cyber. UNIT organisera également des actions de sensibilisation et de communication sur la thématique de la cybersécurité dans l'enseignement supérieur. UNIT apportera son **expertise en pédagogie innovante** (réalité 3D et augmentée, environnement Métavers) afin de toucher au mieux des publics « digital native ».

Action 3. **Pix formalisera un référentiel de cybersécurité avancé** à destination des élèves, des apprentis et étudiants en post-bac et des formateurs, **co-construit avec les membres du Campus Cyber**[11] (PIA 841 016€). Cela permettra de proposer des parcours pour évaluer, développer et certifier les compétences en cybersécurité adaptées à la fois aux compétences des apprenants et aux attentes des secteurs professionnels. **Les compétences acquises seront certifiées via « Pix+ Cyber » afin d'avoir un état réel des compétences à tout moment de la formation.** Pour son déploiement, Pix s'appuie sur son ancrage dans tous les collèges et lycées ainsi que dans **60% des universités françaises** et ses partenariats avec **plus de 150 organismes de formation**. Les ressources pédagogiques et modules de cours réalisés par les autres acteurs du consortium seront exploités par Pix soit en tant que « tutoriel » pour la montée en compétence, soit pour l'orientation vers les formations les plus adaptées au niveau de compétences en entrée de formation. **Seront impliqués dans le projet Inria et Numeum, qui portent par ailleurs le projet de hub français des formations dans le numérique niveau Master et +, et dont la thématique cybersécurité sera développée sous le label du Campus Cyber.**

Action 6. Au-delà des ressources déjà existantes et librement ouvertes à la communauté, **Root-Me PRO** développera les actions suivantes :

- Organisation et animation d'un évènement de type **« Capture The Flag » (CTF)** simple et accessible aux lycéens uniquement (PIA 165 024€) ;
- Organisation et animation d'un évènement de type **« Capture The Flag » d'un niveau plus avancé**, accessible aux étudiants préparant un diplôme supérieur dans une université partenaire (PIA 113 184€) ;
- Création d'un **parcours de formation d'initiation débouchant sur un certificat de compétences** et mélangeant une sélection de contenus théoriques gratuits (sur OpenClassrooms par exemple) et de challenges pratiques gratuits sur la plateforme publique Root-Me (PIA 17 496€) ;

[10] Voir annexe 5
[11] Voir annexe 6

- Création d'un **parcours de formation spécifique** utilisant les environnements de formation de Root-Me PRO ouverts à toutes les Universités participantes (challenges pratiques et cours théoriques en collaboration avec OpenClassrooms par exemple) et débouchant sur un certificat de compétences (PIA 19 440€).

1.2.2 Orienter les nouveaux talents vers la filière cybersécurité

L'objectif de cet axe est de faire découvrir aux jeunes **la diversité des métiers de la cybersécurité en suscitant leur curiosité, en les incitant à se projeter dans ces métiers et en gagnant en compétences**. L'orientation vers les formations menant aux différents métiers de la cybersécurité sera facilitée en rendant l'information accessible sur une méta-plateforme dédiée.

Action 4. **L'Onisep construira plusieurs supports d'orientation**, permettant une meilleure appropriation des informations par les élèves du secondaire :

- **Une publication imprimée dans la collection Zoom Métiers** (PIA 59 899€). Il s'agira de retranscrire des témoignages de jeunes professionnels, femmes et hommes, qui détaillent leur métier et leur parcours. L'essentiel sur le recrutement, l'évolution de carrière et les stratégies d'orientation sera délivré à échelle nationale (collèges et lycées, notamment en technologie, en enseignement moral et civique, en enseignement aux médias et à l'information) ;
- **Un e-Zoom Métiers** (PIA 56 963€) proposant des fonctionnalités en ligne permettant de trier, sélectionner et exporter l'information afin d'inciter les jeunes à être actifs dans leur exploration ;
- **20 fiches métiers** (PIA 5 650€) qui présenteront synthétiquement des métiers de la cybersécurité. Les fiches métiers seront rédigées en deux formats : le format « Découverte », adapté aux collégiens et le format « + d'infos », en version longue.
- **10 films métiers de la collection de référence de l'ONISEP** (PIA 39 000€). Ces films courts complèteront les fiches métiers et illustreront le e-Zoom.

Action 4. Les académies directement impliquées par le Campus Cyber et les INSPE pourront **sensibiliser et former les enseignants et les Psy En des CIO** qui interviennent dans les collèges et les lycées sur les métiers de la cybersécurité afin de mieux accompagner les jeunes dans leur projet d'orientation.

Action 4. Une plateforme d'orientation numérique sera conçue et développée par les Gobelins, **interfaçable avec les plateformes des partenaires, notamment l'ONISEP, Talents du numérique**[12] **et la plateforme numérique développée dans le cadre du projet de plateforme Digital Skills French Hub co-porté par Inria et Udice** (PIA 493 344€)**.** Les Gobelins développeront ce projet dans un contexte de projet pédagogique pour la partie conception et dans le cadre du programme Alliance en mobilisant des jeunes diplômés freelance encadrés pour la partie production et maintenance. Le Laboratoire Ergo-design de l'école sera également mobilisé pour les tests utilisateurs aux différentes étapes du projet. **Ce système sera ainsi conçu pour faciliter l'intermédiation entre les apprenants, les entreprises et les organismes de formation**. Il sera basé sur une matrice métiers / compétences développée par les membres du Campus Cyber

[12] Voir lettre de soutien

(publics et privés) sous la forme de Communs de la Cyber. Cette plateforme d'orientation donnera également l'accès à l'information sur les métiers de la cybersécurité et l'ensemble des outils nécessaires pour apporter un service d'orientation et d'accompagnement. Elle permettra également de sourcer les enseignants en mettant en relation les organismes de formation avec, a minima, les **1 800 experts présents au Campus Cyber**. Concernant la recherche, cette plateforme aura une double utilité : **sensibiliser à l'apport de la recherche dans la construction d'un parcours professionnel et sensibiliser aux métiers cyber de la recherche. Elle constituera aussi un lieu de mise en relation pour les bourses CIFRE.** C'est pourquoi INRIA s'engage à financer son développement en partie (80 000€).

Action 5. Pour susciter la curiosité et l'intérêt des collégiens et lycéens, notamment les filles, la Fondation CGénial proposera chaque année à des établissements de **créer avec les élèves des projets numériques autour de la cybersécurité (démarche expérimentale en lien avec l'étude d'objets connectés)** (PIA 144 050€). Via https://www.cgenial-connect.fr, plateforme facilitant la **mise en relation des acteurs de l'éducation et des entreprises** (témoignages de rôle model), la fondation proposera des visites de sites industriels ou de production, ainsi que des profils collaborateurs des métiers scientifiques et techniques prêts à intervenir dans les classes (les professionnels seront formés en amont des interventions scolaires) (PIA 17 788€). Ces actions seront mises en place en Ile-de-France dans un premier temps puis sur d'autres territoires concernés via le réseau de Campus Cyber Territoriaux.

Action 5. L'association Women4Cyber France **participera à la création des podcasts « cyber puissantes »** de Radio France. De plus, elle pilotera la mise en place de plusieurs projets :

- **Un boot camp « Formation pour les formateurs »** (PIA 308 880€) : deux sessions par an à intégrer au Plan national formation (PNF) et aux Plans Académiques de Formation (PAF), dans les locaux du Campus Cyber. Stage d'été accéléré d'un jour à destination des enseignants, professeurs principaux, inspecteurs, conseillers d'orientation, des responsables d'orientation académique et des chefs d'établissements dans le but de les sensibiliser aux métiers de la cybersécurité.
- **Un boot camp « Immersion et mentorat »** (PIA 49 440€) décentralisé pour les collégiens et lycéens : activités aux contenus immersifs proposés aux colonies de vacances, collectivités territoriales, mais aussi à intégrer aux dispositifs École ouverte, ou Vacances apprenants pour atteindre notamment des établissements en zone d´éducation prioritaire et cités éducatives.
- **Des activités immersives seront également proposées dans le cadre d'un module d'orientation des jeunes au Service National Universel** (PIA 73 360€). Nous proposons d'inscrire au programme de la semaine de cohésion une animation de 2 heures, afin de sensibiliser le jeune public aux métiers de la cybersécurité.

Action 5. Le Campus Cyber organisera des **job fair** dans ses locaux à destination des étudiants, des DRH des entreprises et des écoles. Les différents contenus produits par les acteurs du consortium seront utilisés lors de ces sessions. En outre, le Campus Cyber organisera aussi des moments de **sensibilisation et de formation dans ses locaux à destination des enseignants et des formateurs** (PIA 200 000€).

1.2.3 Création de contenus audiovisuels attractifs à visée informative et pédagogique

L'objectif de cet axe est de **promouvoir les métiers et les formations de la cybersécurité pour attirer de nouveaux talents et pallier la pénurie de profils dans le domaine**. Ainsi, tout l'enjeu de ces travaux sera de créer des contenus fortement incarnés et de les décliner à 360° sur l'ensemble de l'écosystème digital.

Action 4 et 5. **Radio France produira et diffusera des contenus à destination du grand public**. Pour créer un phénomène d'identification et toucher le plus grand nombre, plusieurs contenus « d'incarnations » seront réalisés, soit avec des personnalités publiques, soit avec des professionnels de la cybersécurité pour créer une appropriation affinitaire :

- **Fiction « cyber attack »** (PIA 438 320€) : créer une marque de fiction audio de référence qui sera déclinée à 360°sur les réseaux pour illustrer la présence au quotidien de la cybersécurité ;
- **Cyber puissantes** : valoriser les personnalités féminines « rôle modèles » qui sont au premier rang de la cyber sécurité (PIA 73 360€) ;
- **Chaîne Twitch « cyber attack »** (PIA 467 360€) : informer sur l'actualité et les secrets de la cybersécurité pour toucher la cible des gamers sur les réseaux sociaux ;
- **Vidéos en immersion** (PIA 127 200€) : illustrer que tous les parcours peuvent mener aux métiers de la cybersécurité pour toucher les jeunes qui s'interrogent et leurs parents ;
- **Podcast en immersion** (PIA 155 040€) : profiter de l'audio pour parler des métiers et des personnes que l'on ne peut pas montrer à l'image. Ces audios seront à destination de tous les réseaux audios (Spotify/Deezer/Apple) ;

Action 4 et 5. TOD-The Oligarchs Digital, filiale de la société de production du bureau des légendes, proposera de mettre les participants **en immersion sur le thème de la cybersécurité** afin de sensibiliser aux enjeux et métiers cybersécurité. Il vise différents cœurs de cibles stratégiques :

- **Un escape game mobile à destination des étudiants et jeunes adultes,** disponible pour les universités et les salons étudiants sur l'ensemble du territoire. Utilisant l'approche de la gamification, l'objectif est de sensibiliser et parler de la cybersécurité sans aspect technique (PIA 197 100€) ;
- **Un escape game numérique à destination des salariés** en format 100% en ligne. En une heure les collaborateurs devront réussir en équipe une mission dans l'univers de la cybersécurité. Cet outil permet un apprentissage d'une bonne hygiène numérique par le jeu et la fiction (PIA 259 200€) ;
- **Un serious game de gestion de crise à destination des étudiants, cadres de la fonction publique, chefs d'entreprises de PME et cadres dirigeants,** afin de former à la gestion des crises cyber (PIA 475 200€) ;
- **Un spot fictionné de 30 secondes à destination du grand public** à diffuser sur FranceTV à fort engagement émotionnel, qui fera écho au monde connecté dans lequel nous évoluons et aux métiers / formations de la cybersécurité (PIA 261 600€).

Action 4 et 5. L'école des **GOBELINS, par le bais de différents dispositifs narratifs audio-visuels, propose des contenus de sensibilisation du grand public et des étudiants**, aux menaces et aux risques informatiques, ainsi qu'aux métiers associés. GOBELINS se propose de concevoir, dans le cadre de **projets pédagogiques**, quatre types d'expériences.

- **Cyber-Skills**, un dispositif ludique interactif pour se familiariser avec les compétences clés des métiers de la cyber (public Bac +2 à Bac +5) (PIA 28 640€).
- **Cyber-Stories**, une série d'une quinzaine de films courts de motion design qui racontent des istoires personnelles et des témoignages sur les risques informatiques (PIA 22 800€).
- **Cyber-Viz**, une série de films de motion design en VR 360 scénarisant des données infographiques et factuelles sur l'univers de la sécurité informatique (PIA 20 400€).
- **Cyber-Wall**, un dispositif audio-visuel de datavisualisation créative mises à jour en temps réel sur l'univers de la cybersécurité et des risques informatiques (sources ouvertes) (PIA 27 560€).

<u>Action 4 et 5.</u> Toujours dans le cadre d'actions d'immersion et de gamification **Campus Cyber développera un jeu vidéo** sous forme de jeu de rôle qui traite des menaces cyber et des moyens d'y remédier. Ce jeu vidéo sera diffusable et jouable en autonomie et son expérience pourra être prolongée en atelier pour renforcer l'impact sur les participants (PIA 162 456€).

1.3. RESULTATS ET MESURE DE L'IMPACT

Un bilan annuel de mesure d'impact pour les actions non terminées couplé à un bilan pour les actions terminées permettra de valider l'atteinte des objectifs. Ce dernier sera mis à disposition sur le site du Campus Cyber.

Concernant la formation, le projet ambitionne **de former en 5 ans plus de 17 000 personnes**, dont environ 12 900 jusqu'en bac +3, 3 700 jusqu'en bac+5 et presque 900 au-delà. Une partie conséquente des personnes formées jusqu'en bac +3 le seront via des enseignements hybrides et cible la formation continue. Les profils concernés seront **spécialistes mais aussi non-spécialistes**. Cette dernière catégorie sera également au cœur de formation de sensibilisation générale à la cybersécurité qui ambitionnent de former 740 000 personnes sur 5 ans. Par ailleurs, 30 000 éducateurs seront formés aux enjeux de cybersécurité **à l'aide des actions conjointes de Class Code**. La fondation Cgenial formera **200 enseignants** à une utilisation pédagogique du kit cybersécurité, à utiliser avec les élèves. En outre, les **compétences développées pourront être analysées** grâce au développement d'épreuves de certification de PIX, déployable dans les lycées et les universités. Grâce aux contenus audiovisuels, ludiques, informatifs ainsi que les modules de formation générale aux enjeux de la cybersécurité, **plus d'un million de personnes seront sensibilisées** sur 5 ans, notamment via l'implication de Radio France et France TV.

De manière générale, les contenus déployés doivent permettre de constater **une évolution des représentations des métiers et des enjeux de la cybersécurité**, une **augmentation des connaissances sur les entreprises et leurs activités**, un **développement de l'esprit critique**, un développement chez les jeunes des **compétences en algorithmie et en programmation**. La présence de Radio France assure un phénomène médiatique autour de ces enjeux. Chaque vidéo sera l'occasion de parler des risques ainsi que des formations et débouchés existants en renvoyant sur la plateforme Campus Cyber. Les émissions broadcast permettent de communiquer dans la durée sur **l'actualité cyber, les opportunités professionnelles et la mise en avant des métiers auprès de collaborateurs** pouvant faire le choix de se reconvertir. Ce projet permet de mutualiser les moyens de communication pour toucher un public de **plusieurs centaines de milliers de personnes**.

1.4. DIFFUSION DES DISPOSITIFS

Les membres du Campus Cyber sont autant de relais de diffusion des dispositifs de formation, des contenus d'orientation et d'attractivité nouvellement conçus. C'est ainsi sur un **réseau de plus de 200 membres et adhérents que le consortium va s'appuyer dès le début du projet pour déployer et mettre en place des partenariats tels que des campagnes de communication autour des dispositifs de formation conçus.** Notons également que d'autres partenaires présents dans le consortium s'appuieront également sur leur réseau respectif pour adresser les différents publics visés.

Le consortium a **également le soutien de structures essentielles dans la mise en place d'offres de formation finançables visant des publics pluriels**. Le consortium compte ainsi sur le soutien de la **DGESCO, de la DGESIP, de l'académie de Versailles et du rectorat de la région Ile-de-France**, permettant ainsi d'être un relai direct avec les établissements scolaires. Avec le concours des entreprises partenaires, des relais d'attractivité sur le territoire, sous la forme de Comités locaux école entreprise (CLEE) Cybersécurité, autour d'établissement scolaires particulièrement engagés dans le domaine, serviront à la diffusion de culture cyber auprès des élèves. D'autres acteurs tels que le **MEDEF, l'OPCO Atlas et Numeum** sont soutiens du projet Talents Cybersécurité[13] et garants de la **diffusion des outils de sensibilisation cybersécurité auprès des entreprises et de leurs salariés**. Outre un apport financier pour le projet, ces soutiens assurent une pénétration efficace des formations développées sur un marché réclamant de nouveaux outils efficaces, abordables et largement diffusables. Côté attractivité, **la participation de Radio France au projet et le soutien de France TV** assurent la bonne diffusion des informations afin d'attirer de nouveaux profils vers la filière cyber.

2. ORGANISATION ET PILOTAGE DU PROJET

2.1. ORGANISATION DU CONSORTIUM

Le consortium fait intervenir une multiplicité d'intervenants (structures indépendantes, PME, ETI, organismes publics, universités, écoles, associations) fédérés par un projet commun de formation et de valorisation du domaine de la cybersécurité. **Les partenaires ont été soigneusement sélectionnés en fonction de leur expertise pour diffuser, former et communiquer autour de la cybersécurité**. Au sein du consortium, chaque acteur est placé sur un pied d'égalité et est en charge des actions qui lui incombent. Ce mode de fonctionnement fédérateur est à l'image du fonctionnement interne du chef de file : Campus Cyber.

CAMPUS CYBER Rassemblant des entreprises, services de l'État, organismes de la formation, acteurs de la recherche et des associations, le [Campus Cyber] est le lieu totem national, propice à la collaboration, la formation et à l'innovation face à la menace cyber.

<Class'Code> [Class'Code], initié par Inria, forme les professionnels de l'éducation et de l'animation afin d'initier les filles et les garçons de 8 à 14 ans à la pensée informatique.

[13] Voir lettres de soutien

OpenClassrooms est un site web de formation en ligne qui propose à ses membres des cours certifiants et des parcours débouchant sur des métiers en croissance.

Pix est une structure à but non lucratif constituée en Groupement d'intérêt public ayant pour mission d'accompagner l'élévation du niveau général de compétences numériques.

TOD-The Oligarchs Digital est la filiale de flux, documentaires, programmes courts, production web de TOG-The Oligarchs Group.

Radio France comptabilise un important audimat : tous les jours 15 millions de français de tous âges sur tout le territoire et totalise près de 100 millions d'écoutes de podcasts mensuels.

GOBELINS, l'école de l'image est un établissement d'enseignement supérieur en cinéma d'animation, création visuelle et production d'images.

La fondation C'Génial œuvre depuis 15 ans pour rapprocher le monde de l'éducation de celui des entreprises.

L'association Women4Cyber France fait de la promotion des métiers cyber auprès des femmes et des talents féminins auprès du secteur de la cyber.

L'ONISEP, éditeur public de référence en matière d'orientation en France, cible les collégiens/lycéens et leurs enseignants.

Le CNED est un organisme de formation 100% en ligne qui délivre des formations certifiantes, permettant à chacun de se former sur un plan scolaire et professionnel.

CY Cergy Paris Université est un établissement d'enseignement supérieur et de recherche.

Université de Lorraine est un établissement d'enseignement supérieur et de recherche.

Université Paris 1 Panthéon-Sorbonne est un établissement d'enseignement supérieur et de recherche.

Université Sorbonne Paris Nord est un établissement d'enseignement supérieur et de recherche.

Académie de Versailles gère la politique éducative sur les départements des Yvelines, de l'Essonne, du Val d'Oise et et des Hauts-de-Seine.

La Fondation Partenariale UNIT accompagne la transformation numérique de la société. Elle fédère environ 80 Universités et Écoles d'Ingénieurs, soit près de 400 000 étudiants et environ 2000 enseignants. Elle est membre de l'Université Numérique qui associe ses partenaires en Santé et Sport, Humanités, Économie-Gestion, Environnement et Enseignement technologique.

Root me est une communauté de plus de 500 000 joueurs qui dispose d'une plateforme dédiée à l'apprentissage en ligne de la sécurité informatique.

Association groupe ESSEC est un métalab pour les données, la technologie, la société et l'entrepreneuriat éclairant.

iX Campus est un centre d'excellence réunissant des entreprises industrielles de haute technologie, des start-ups innovantes, l'école de design CY et CT Tech.

WebForce 3 est un réseau de 50 écoles et centres de formation d'apprentis en France, Belgique et Maroc qui propose des formations aux métiers du numérique vers des personnes éloignées de l'emploi.

2.2. PILOTAGE DU PROJET

Une équipe de trois personnes sera recrutée par Campus Cyber (PIA 1 361 400€) **:**

- Un chef de projet qui sera garant du pilotage du planning et du budget pour l'ensemble des productions du consortium de manière cohérente. Il préparera les comités de pilotage ;
- Un chargé de mission qui gèrera la mise en place quotidienne des actions portées par le consortium, en lien avec le chef de projet ;
- Un assistant.

En outre, **le Campus Cyber met à disposition de nombreux espaces et ressources humaines** permettant au projet des partenaires de fonctionner et d'être moins onéreux.
Au-delà de ce projet, le Campus Cyber dispose d'un responsable RSE, les locaux sont HQE et le sujet de la sobriété numérique est central au sein des travaux des groupes de travail. Ces problématiques seront donc au cœur des travaux menés par le projet Talents Cybersécurité.

L'intégralité des membres du consortium prendront part à la gouvernance du projet Talents Cybersécurité. Campus Cyber en tant que chef de file sera impliqué dans chacun des trois volets du projet. Deux comités seront mis en place[14].
Le **comité de pilotage** exercera un suivi du projet : niveau des dépenses, état d'avancement, retombées chiffrées, cohérence des contenus avec la vision globale. Il regroupera :

1) Les membres du consortium du projet Talents Cybersécurité (20 membres, hors chef de file)
2) Les membres de droit : ces membres sont des acteurs proches de Campus Cyber ou des soutiens financiers / support stratégique :
   - **OPCO Atlas** (soutien financier et expert formation) : opérateurs de compétences ayant pour mission d'améliorer l'accès des salariés à des formations professionnelles et les entreprises dans l'analyse et la définition de leurs besoins en matière de formation ;
   - **Coordinateur du Groupe de Travail formation** / **Représentant collège formation :** au sein du CA de Campus Cyber, cet acteur portera les idées et besoins pour l'écosystème ;
   - **Chef de projet du consortium**
   - **Directeur Général Délégué chargé de l'écosystème du Campus Cyber.**

[14] Voir annexe 2

Le **comité stratégique** émettra un avis sur l'orientation prise par le consortium, la qualité des contenus et particulièrement des dispositifs de formations et les actions d'attractivité et d'orientation. Cela permettra de s'assurer que les dispositifs et formations mises en place correspondent au besoin du marché. Ce second comité, en lien étroit avec le premier, se composera de :

- **DGESCO** (soutien et représentant pédagogique) : direction générale de l'enseignement scolaire, à l'origine des politiques éducatives et pédagogiques visant à assurer les programmes d'enseignements scolaires.
- **ANSSI** : autorité nationale en matière de sécurité et de défense des systèmes d'information ;
- **INRIA** (soutien financier et représentant de la recherche) : institut national de recherche en sciences et technologies du numérique.
- **DGESIP**
- **France Université** (en attente de confirmation d'accord)

Les différents comités seront mis en place dès les premiers mois du projet et se réuniront trimestriellement afin d'assurer une gouvernance claire et optimale sur la totalité des cinq années. Le mode de résolution des conflits et le processus de décision pour les comités seront définis dans un accord de consortium.

2.3. PERENNITE DES DISPOSITIFS MIS EN PLACE

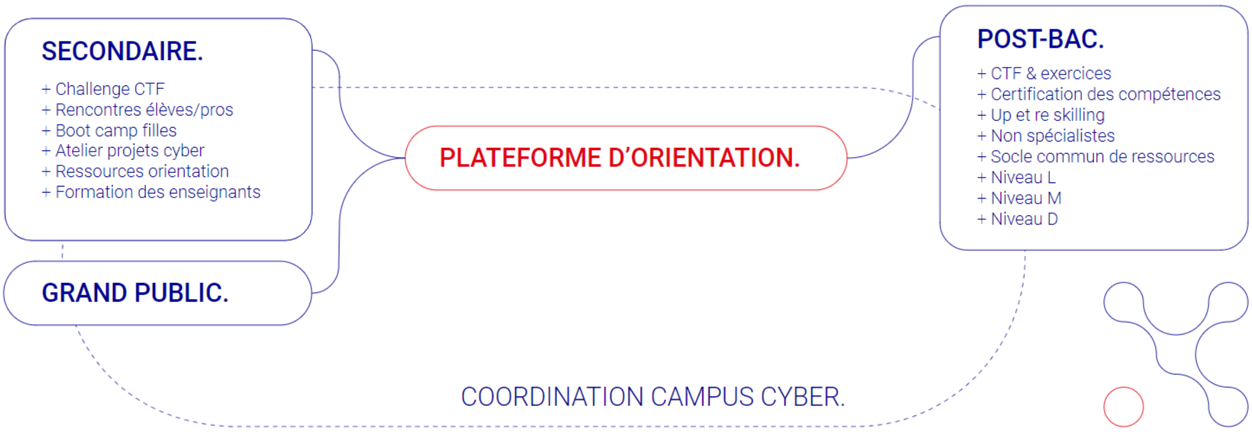
Le projet Talents Cybersécurité est prévu pour une **durée de 60 mois au total**. Les actions de ce projet sont tournées vers des dispositifs de formations visant des publics pluriels ainsi que vers les programmes d'attractivité et d'orientation sont nécessaires afin d'inscrire durablement ces nouvelles offres. Le **budget total s'élève à 53 702 108 €**, composé du coût éligible de chaque partenaire. **L'aide demandée d'un montant de 26 680 140 € couvre la mise en place des formations et dispositifs**, soit les dépenses de conception et les premières promotions d'apprenants. La part du projet non subventionnée par l'AMI CMA est couverte par différents moyens[15] :

- Les **fonds propres** de certains partenaires de type entreprise ou la **valorisation** matérielle, immatérielle ou encore humaine de certains partenaires ;
- Les **revenus générés** par le déploiement des outils pouvant être commercialisés (formations, contenus d'attractivité diffusés, etc.)
- Le **soutien financier** d'acteurs hors du consortium, publics et privés.

La subvention prend en charge les **coûts conséquents d'investissement** tandis que les autres sources de financement permettent de s'assurer de la **continuité de l'équilibre du budget au-delà des 5 ans**. Les diverses actions de formation des formateurs (actuels et nouveaux, notamment via les doctorants) assurent une **pérennité dans l'enseignement et sa massification.** Les **ressources libres** seront à disposition de l'ensemble de l'écosystème. Les contenus d'attractivité seront pour les autres **au cœur des dispositifs de formation** déployés par les membres du consortium. Les ressources d'orientation seront disponibles sur le site de l'ONISEP et dans les établissements scolaires. La **mise à jour et maintenance** de la plateforme sera prise en charge par le Campus Cyber. Enfin, les différentes formations seront matures et **ancrées dans le paysage éducatif** si bien qu'elles auront la capacité de fonctionner au-delà des 5 ans du projet, notamment en ayant recours à des formations en apprentissage (couts pris en charge par les entreprises) ou bien via des fonds propres ou mécénat.

[15] Voir annexe 11 pour la répartition

ANNEXES



Annexe 1 : Les parties prenantes du Campus Cyber

RÉPARTITION PROVISOIRE POUR SEPTEMBRE 2022 : 164 MEMBRES.

Membres de droit
ANSSI - Etat
Bull – Atos
Capgemini
Orange Cyberdefense
Sopra Steria
Thales

Institutionnels
ACYMA
ANSSI
CNIL
Ministère des Armées
Ministère de l'Economie des Finances et de la Relance
Ministère de l'Intérieur
Ministère de la Justice

Industriels
Airbus Cybersecurity
Avisa Partners – CEIS
HeadMind Partners
HubOne
Squad
Wavestone

Recherche Publique
CEA
CNRS
IMT
Inria
Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation

Campus Territoriaux

Associations
ACN
CESIN
CEFCYS
Club 27001
Clusif
Hexatrust
Hub France IA
Numeum
OSSIR
Afnor Normalisation
AFNIC
Cinov numérique
Forum des Compétences
Gitsis
GPMSE
InterCert France
Luatix
Pôle d'excellence Cyber
Systematic Paris-Région

Formation
ESILV – Léonard de Vinci
EFREI Paris
Epita – Groupe Ionis
Galileo Global Education France
HS2
Ministère de l'Education nationale et des Sports
Simplon.Co
Ecole 2600
ESAIP
ESIEA
Ikai – Oteria School
IT-AKADEMY
Orsys
Quest Education group
Sup de Vinci
WEBFORCE3

RÉPARTITION PROVISOIRE POUR SEPTEMBRE 2022 : 164 MEMBRES.

ETI & PME	
ACE Capital Partners	The Green Bow
ACG Cybersecurity	Utac
Advens	Withings
All4tec	Yes We Hack
Almond	Ziwit
Cybel Angel	**Accuracy**
EGERIE	**Afnor Certification**
Formind	**Algosecure**
Gatewatcher	**Centreon**
Geoide Crypto&Com	**Erium**
IMS Networks	**HAAS Avocats**
I-Tracing	**IN Group**
Micropole – Go Cloud & Security	**Intrinsec Sécurité**
Numeryx	**MC2i**
Quarkslab	**OVH**
Red Alert Labs	**Photomaton – ME**
Risk & Co	**Systemis**
Sekoia	**Yogosha**
TEHTRIS	

Startups	
Aleia	**Allistic**
Becycure	**ASPIS**
Cabinet Louis Reynaud	**Board of Cyber**
Certi-Trust	**Data Protection Expertise**
Cleyrop	**Cryptonext**
Cyber4U	**Datascientest**
Cyberjobs	**Glimps**
Cybervadis	**Inquest**
Cycover	**Iriguard**
Dataxium	**Neotrust**
Eternilab	**OperaCyber**
Harfanglab	**Partenaire GC**
Leanear	**Patrowl**
ShareID	**Predimya**
Sesame-IT	**Qorum Invest**
Zama	**Sahar**

Bénéficiaires	
AEMA groupe	Air France
Alstom	Altarea
Apave	ArcelorMittal
Arkema	Axa
Banque de France	BNP Paribas
Bolloré	Bouygues
BPCE	**CMA CGM**
CNP Assurances	Covéa Next
Euro-Information	EDF
Française des Jeux	GRTgaz
HAROPA PORT	Hermès
Kering	La Poste
L'Oréal	LVMH
RATP	Renault
Safran	Sanofi
Schneider Electric France	SNCF
Société Générale	Sodexo
Suez	TotalEnergies
Veolia	

CAMPUS CYBER

NOS 111 RÉSIDENTS.

ACCENTURE	ATOS (BULL)	CESIN	EGERIE	HEADMIND PARTNERS
ACG CYBERSECURITY	AVANGARDE CONSULTING	CISCO	EPITA	HERMÈS
ADVENS	AXA	CLUSIF	ESILV	HEXATRUST
AFNOR CERTIFICATION	BANQUE DE FRANCE	CMA CGM	EURO-INFO-CREDIT MUTUEL	HS2
AIRBUS CYBERSECURITY	BECYCURE	CRÉDIT AGRICOLE	FDJ	INFOBLOX
ALEIA	BNB PARIBAS	CYBER BOOSTER	FORTINET	INRIA
ALGOSECURE	BOUYGUES	CYBERARK	GALILEO GLOBAL EDUCATION FRANCE	INSTITUT MINES-TÉLÉCOM (IMT)
ALMOND	BPCE	DATA PROTECTION EXPERTISE	GATEWATCHER	IRIGUARD
ALSTOM	CAPGEMINI	DATAXIUM	GENERALI FRANCE ASSURANCE	ISEP
ALTER SOLUTIONS	CDC INFO	DELOITTE	GRTGAZ	I-TRACING
ANSSI	CEA	DUST MOBILE	HAAS AVOCATS	JO PARIS 2024
ARCELORMITTAL	CERTI-TRUST	EFREI PARIS	HARFANGLAB	KEYFACTOR (PRIMEKEY)

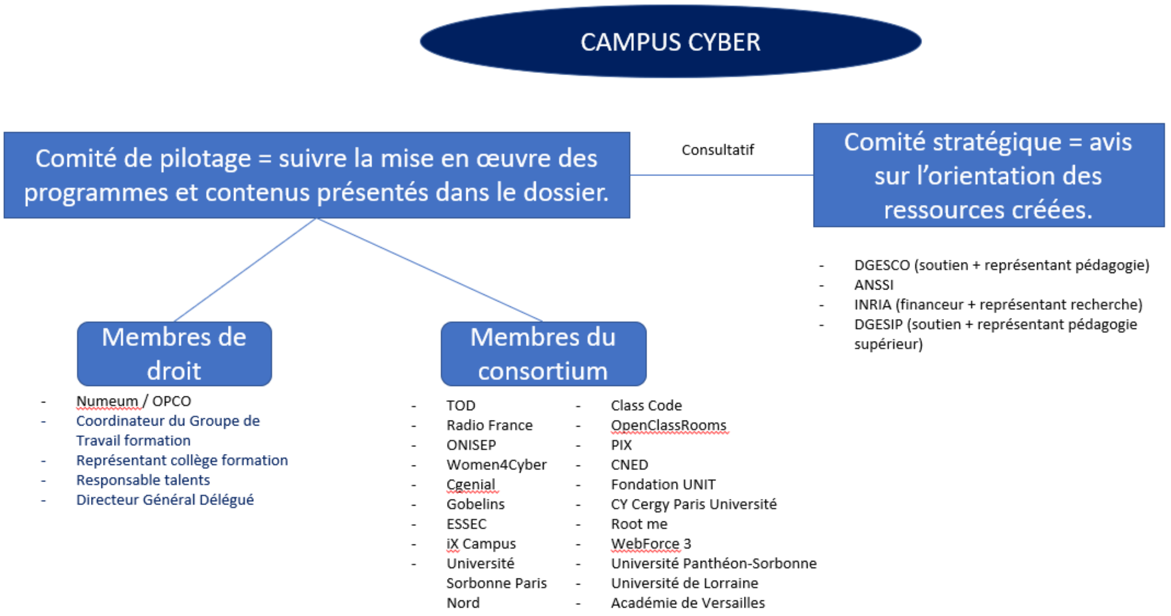
NOS 111 RÉSIDENTS.

KYNDRYL	OPERA CYBER	SEKOIA	TANIUM	ZF
LA BANQUE POSTALE	ORANGE CYBERDEFENSE	SENTINELONE	TEHTRIS	
LA POSTE	ORCA	SET IN STONE	THALES	
L'ORÉAL	OTERIA CYBER SCHOOL	SIEMENS	TOTALENERGIES	
LVMH	PALO ALTO NETWORKS	SMART4 ENGINEERING	TREND MICRO	
MALTEM	PÔLE D'EXCELLENCE CYBER	SNCF	UPFRONT TECHNOLOGIES	
MINISTÈRE DE L'INTERIEUR	PWC	SOCIÉTÉ GÉNÉRALE	VARONIS	
MINISTÈRE DES ARMÉES	QORUM INVEST	SODEXO	VECTRA	
NEOTRUST	RED ALERT LABS	SOPRA STERIA	WAVESTONE	
NUMERYX	SAFRAN	SOSAFE	WF3	
ONEVISAGE	SANOFI	SQUAD	WOMEN4CYBER	
OPENCYBER	SCHNEIDER ELECTRIC FRANCE	STORMSHIELD	YESWEHACK	

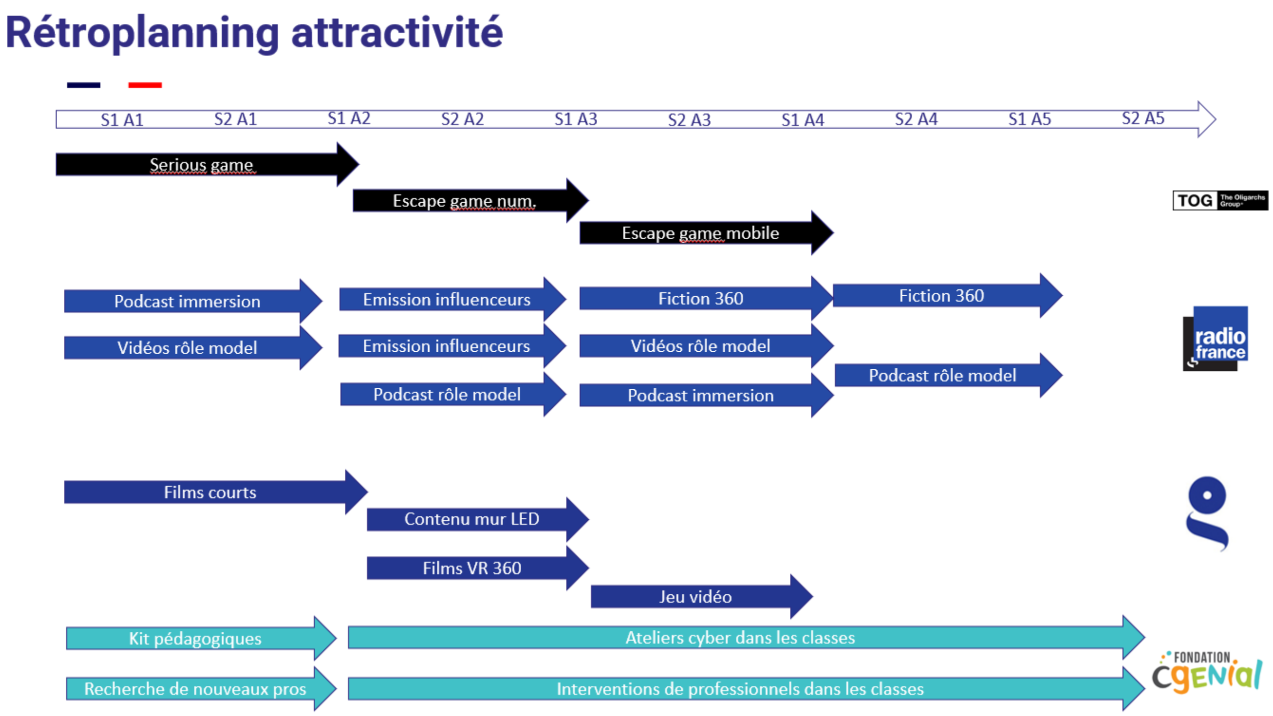
NOS 40 PARTENAIRES.

AFNIC	CYBERARK	IBM	PALO ALTO	SYNETIS
AIR LIQUIDE	CYMBIOZ	KEREIS	PMU	TANIUM
AWS	DELL	KEYFACTOR (PRIMEKEY)	PÔLE D'EXCELLENCE CYBER	TELEFÓNICA TECH
AXIS COMMUNICATIONS	DG CONSULTANTS	LES RIAMS	PROOFPOINT	TRUSTSEED
BESSÉ	ENEDIS	M2I	SAILPOINT	VINCI
BT BLUE	ENGIE	MICROSOFT	GROUPE SEB	VMWARE
CHECK POINT	GENERALI FRANCE ASSURANCE	NOZOMI NETWORKS	SENTINELONE	WITHSECURE
CISCO	GOOGLE CLOUD	ORACLE	SOSAFE	ZF

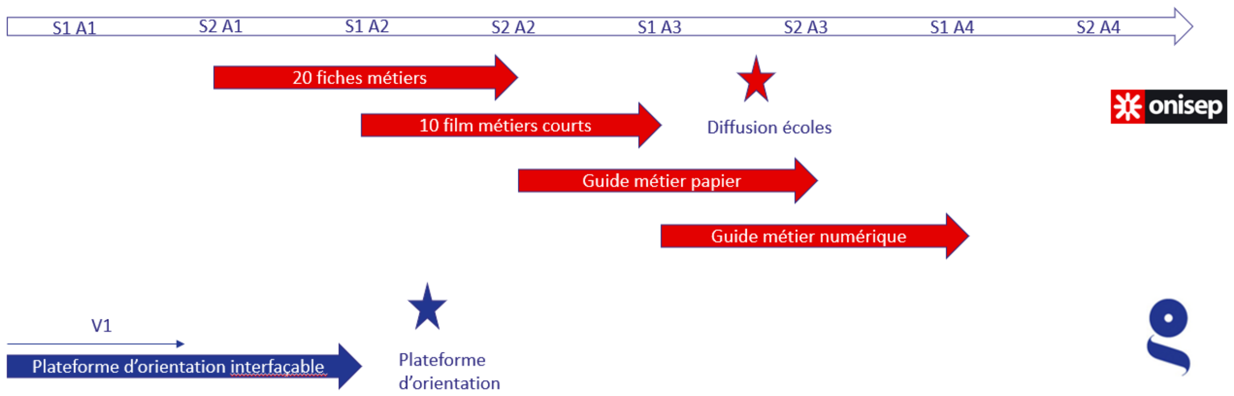
Annexe 2 : Gouvernance



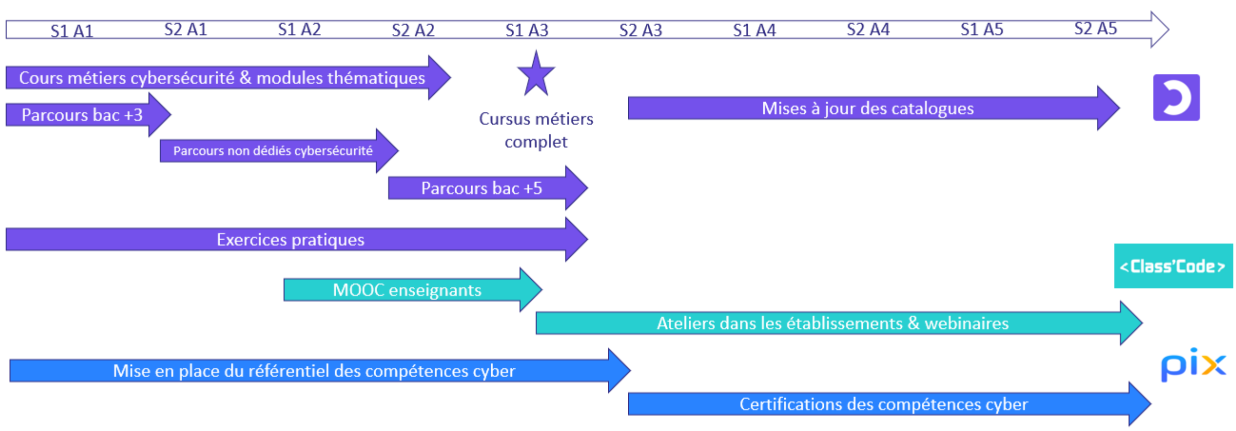
Annexe 3 : Retro-Planning



Rétroplanning orientation



Rétroplanning formation



Annexe 4 : méthodologie de production de Class Code

Les contenus de Class'Code sont basés sur la production collaborative.

- **Première phase d'analyse des besoins** : un état de l'art du sujet et de discussions avec les commanditaires pour définir une commande claire et qui sera pertinente pour le public cible.
- **Formation d'un comité de pilotage** et d'un **comité scientifique** de spécialistes. Ce dernier est consultatif et permet d'assurer de la conformité scientifique des productions. Le comité de pilotage est quant à lui chargé de valider les décisions éditoriales et de diffusion.
- La matière pédagogique est récoltée grâce à des **groupes de travail**, qui peuvent être thématiques et qui associent **des experts du sujet traité, des ingénieurs pédagogiques, et professionnels de l'éducation nationale et populaire.** Cette matière pédagogique est affinée et ensuite séquencée dans un parcours d'apprentissage. Cette logique de co-production en groupe de travail permet d'assurer de la pertinence des productions, de leur utilité vis à vis du public cible et de leur qualité pédagogique et scientifique. Les contributeurs

peuvent également être sollicités pour participer à la **formation des bénéficiaires**, dans une logique d'**hybridation des contenus**, ou pour la création de **ressources annexes** (wébinaires, ateliers, conférences, workshops…). La formation de cette communauté de professionnels et de spécialistes est assurée, notamment pour assurer la continuité des contenus, leur diffusion et leur mise à jour.

Annexe 5 : méthodologie de production de UNIT

- Les REL sont validées scientifiquement, pédagogiquement et techniquement et seront les **livrables des appels à projets annuels** proposés les trois premières années.
- UNIT reproduira le schéma pédagogique du projet « Hybridation » PUNCHY qui s'appuie sur **H5P**, outil de création de contenus interactifs. Cet outil est largement répandu et surtout **compatible avec le LMS Moodle**, utilisé par 90% des établissements d'enseignement supérieur. UNIT identifiera dans son réseau et celui de L'UN des auteurs contributeurs pour couvrir la thématique de manière transversale et dans une logique métier.
- Une démarche **générale, systémique et collective** sera mise en place. Elle vise la création de **ressources numériques à large potentiel de réutilisation** et d'adaptation à des contextes divers, supports de formations complètes, qui ont vocation à devenir des documents de référence. Pour cela, PUNCHY part du terrain en s'appuyant sur **des groupes d'enseignants** responsables de formations. Ils définissent les contenus nécessaires pour s'adapter à des formations comparables mais souvent différentes dans le détail, ainsi que les conditions d'une large acceptabilité des ressources par de nombreux enseignants.
- **Pour faciliter l'appropriation des ressources par les enseignants** qui n'ont pas participé à leur conception, celles-ci seront organisées de façon modulaire par **assemblage de micro-contenus** faciles à ajouter ou supprimer.
    - <u>Définition d'un micro-contenu</u> : unité pédagogique élémentaire, numérique, visant à l'apprentissage d'une notion. Il peut être utilisé de manière autonome ou inséré comme composant d'une ressource numérique plus globale. Un micro-contenu est **autonome, réutilisable, décontextualisé et assemblable**. L'association de micro-contenus permet de créer de nouvelles ressources à la carte, selon les choix pédagogiques de l'enseignant.
- Le projet s'appuie sur l'ensemble des acquis, ressources et partenaires **des 6 Universités Numériques Thématiques de L'UN** et de leurs membres qui regroupent une grande partie de l'enseignement supérieur français. La démarche proposée a vocation à s'étendre à toutes les disciplines et à toutes les formations hybrides ou non, en formation initiale, continue, en alternance, en France comme dans la francophonie. Elle vise, **sur les 24 mois du projet, à développer au moins trois parcours de formations,** à en compléter d'autres, et à en générer beaucoup plus à terme par un **effet d'entrainement et d'adhésion à la démarche de PUNCHY.**

Au total, le projet inclut la création de ressources correspondant à **1 000 heures équivalent présentiel, dont 250 heures pour UNIT.**

Annexe 6 : méthodologie de production de Pix

- **Elaboration et mise en œuvre de la stratégie de déploiement au service de l'orientation et de la formation :** Parcours d'évaluation des compétences permettant d'orienter vers des formations ou vers de la certification ; mise à disposition d'espace pour les participants aux tests et preuves de concept ; rapport de preuves de concept sur 2 périmètres ;
- **Structuration et définition du référentiel de compétences** : Référentiel de compétence (domaines et sujets) ;
- **Création des épreuves, déclinaison opérationnelle du référentiel d'évaluation Pix+ Cyber** : Référentiel d'évaluation structuré en sujets et niveaux avec des épreuves et tuto pour chaque acquis ;
- **Design et mise en œuvre de la certification Pix+ Cyber** (amorçage) : Mode opératoire de la certification Pix+ Cyber ; Centres de certification agréés et formés sur le territoire permettant la certification Pix+ Cyber ; 1500 personnes certifiées dans le cadre du projet

Annexe 7 : précisions formations OpenClassrooms

OpenClassrooms porte un modèle pédagogique innovant :

- **La pédagogie par projet :** un parcours de formation OpenClassrooms est composé d'une succession de projets professionnalisants à réaliser. Un projet est une véritable mise en situation professionnelle et donne lieu à la production d'un livrable, rendant compte de l'acquisition des compétences visées. Au fil de sa formation, l'étudiant constitue ainsi un portefeuille de réalisations à valoriser auprès de futurs employeurs.
- **Un mentorat individualisé :** chaque étudiant suivant un parcours de formation bénéficie de l'accompagnement d'un mentor dédié pour réaliser les livrables des projets. Cet accompagnement est 100% individualisé. Avec l'aide de son mentor, l'étudiant est pleinement engagé dans sa formation ce qui limite les risques de décrochage.
- **La conception inversée des formations :** l'ingénierie pédagogique d'OpenClassrooms procède de manière inversée en commençant par rechercher les métiers les plus demandés sur le marché du travail, en en extrayant les compétences, et finalement en concevant les projets et les cours qui permettront de faire acquérir des compétences aux apprenants.
- **Des cours sous licence libre Creative Commons :** OpenClassrooms s'est fixé comme mission de "Rendre l'éducation accessible**"**. Une des traductions concrètes de cet engagement est de produire les cours sous licence libre. Gratuits, ils sont visionnés par plus de **300 000 personnes par mois**.
- **La certification des micro-compétences :** Le débat actuel au niveau européen sur les "micro-justificatifs" (*micro-credentials*) tourne autour de l'enjeu de normaliser la reconnaissance des micro-compétences et de créer un référentiel. Les micro-compétences sont particulièrement attendues dans les métiers de la cybersécurité. C'est notamment l'une des réflexions du groupe de travail "European Cybersecurity Skills Framework" porté par l'ENISA, avec lequel OpenClassrooms interagit.

Concrètement, le contenu produit par OpenClassrooms dans le cadre du consortium s'organisera autour de trois vecteurs de formation :

- **Cours :** pour obtenir des connaissances sur un sujet spécifique.
  - Chaque cours traite d'un sujet spécifique et peut être suivi à la carte, **en accès libre**.

    - La durée des cours peut varier **de 2 à 20h** selon leur densité.
    - La difficulté varie et des prérequis sont parfois indiqués avant le visionnage.
- **Modules :** pour acquérir des compétences et un savoir-faire sur un activité donnée.
    - D'une durée **de 12 à 40 heures**, chaque module vise à la réalisation d'une activité donnée, qu'elle soit récurrente sur le marché dans sa globalité ou au sein d'un secteur en particulier.
    - Ces modules bénéficient d'une **pédagogie par projet** et chaque apprenant y est accompagné par un **mentor**.
- **Parcours certifiants :** pour préparer son entrée sur le marché du travail ou une reconversion.
    - De niveau **bac+2 à bac+5**, les parcours se réalisent **de 12 à 18 mois** à plein temps ou à temps partiel en apprentissage.
    - L'apprenant suit un ensemble de cours et **réalise un ensemble de projets représentatifs d'un métier donné.**
    - Les parcours certifiants mobiliseront l'apprenant sur des situations variées, lui permettant d'acquérir l'ensemble des compétences qui lui seront nécessaires à son arrivée sur le marché du travail ou à la réussite de sa reconversion.

Tout au long des cinq ans, **un contenu diversifié sera produit pour être mobilisable à la carte par des niveaux de compétence très hétérogènes, de la simple acculturation sur l'univers de la cybersécurité à l'expertise la plus pointue** sur la sécurité des objets connectés, des développements, du Cloud et des SI industriels notamment. Les angles d'approche aussi seront complémentaires, des fondamentaux techniques sur les tests d'intrusion ou les investigations numériques par exemple, à la thématique de la gouvernance cybersécurité sur l'intégration de la sécurité dans les projets, les référentiels normatifs et réglementaires, la gestion de crise et l'organisation de la cyberrésilience notamment. Ce contenu servira aussi la création et la mise à jour de parcours certifiants RNCP de niveau 6 et 7 (équivalents Bac+3 à Bac +5) préparant à des métiers en tension et/ou émergent. Ce sera dans un premier temps le cas des métiers d'analyste cybersécurité SOC et de gestionnaire de la sécurité des données, des réseaux et des systèmes d'ores-et-déjà identifiés. Les métiers de développeur, intégrateur, technicien informatique et administrateurs seront ensuite concernés.

Annexe 8 : précisions formation CNED

Le parcours d'apprentissage est digital et porté par une plateforme numérique (Moodle). Des essentiels au format papier le complètent et accompagnent l'apprenant dans sa démarche de mémorisation et de préparation aux épreuves lors de ses révisions.

Titre niveau 4/5 "Gestionnaire de cybersécurité TPE/PME" : 400 heures de formation

- **L'entrée en formation** : s'attache à donner à l'apprenant un sentiment de sécurité et des clefs pour développer son autonomie et soutenir sa motivation. L'unité « Bien démarrer » a pour objectif son engagement dans la formation, la prise en compte de son individualité et le développement de son autonomie.
- **Le système d'apprentissage** : s'attache à stimuler la montée en compétences de l'apprenant, permet une individualisation de parcours, maintient le sentiment de sécurité, favorise son autonomie et soutient sa motivation. L'apprenant accède à ses modules d'apprentissage structurés en 4 blocs de compétences métier. Pour valoriser l'acquisition de compétences transverses et motiver les parcours des apprenants, le CNED propose dans ses parcours de formations des Open Badges.
- **La professionnalité** se construit en lien avec l'expérience en milieu professionnel : peut être acquise par son vécu professionnel ou lors d'un stage de 8 semaines à temps plein (sauf dispense).
- **Un accompagnement des apprentissages et du parcours** : suivi individualisé de l'apprenant, réalisé en médiation par des spécialistes de leur domaine et des conseillers-experts (équipe administrative et pédagogique) et facilité par l'utilisation des outils et technologies numériques.
- **Entrainement et préparation aux épreuves**

Modules d'acculturation à la cybersécurité pour les bacheliers et les étudiants. Ces 2 modules courts viennent compléter un parcours de formation initiale pour les bacheliers (12 heures) et les étudiants (20 heures). L'objectif est, entre-autres, de permettre à ces apprenants de :

- Comprendre ce qu'est la cybersécurité
- Développer une culture de la cybersécurité
- Découvrir les enjeux de la sécurité numérique
- S'initier aux actions de prévention/curation

A la fin de chaque séquence **une synthèse des contenus est téléchargeable afin de garder une trace des apprentissages et une évaluation formative** est proposée afin de mesurer les acquisitions de connaissances.

Annexe 9 : précisions formation Université Paris 1 Panthéon-Sorbonne

Le DU "Influence et Cybersécurité" : modules de formation : (160h). Direction conjointe : Christine Dugoin-Clément (IAE), Célia Zolynksi (Paris 1), Alain Celisse (Paris 1)

- Module n°1 : **Communication, information et influence** (15h). Responsable : Christine Dugoin-Clément (Paris 1)
- Module n°2 : **Prise de décision** (15h). Responsable : Christine Dugoin-Clément (Paris 1)
- Module n°3 : **Enjeux économiques et intelligence économique** (15h). Responsable : Rémy Février (CNAM)

- Module n°4 : **Enjeux humains et risques organisationnels** (15h). Responsable : Christine Dugoin-Clément (Paris 1)
- Module n°5 : **Enjeux juridiques et stratégies d'influence** (15h). Responsable : Célia Zolynski (Paris 1)
- Module n°6 : **Approche technique et influence : réseaux sociaux, systèmes d'information, intelligence artificielle** (15h). Responsable : Alain Célisse (Paris 1)
- Module n°7 : **Approche dynamique du droit de la cybersécurité** (15h). Responsable : Stéphane Prévost Boyard (référent cybermenace, Police nationale)
- Module n°8 : **Approche dynamique de la cybercriminalité** (15h). Responsable : Stéphane Prévost Boyard (référent cybermenace, Police nationale)
- **Mémoire** (20h)
- **Conférences obligatoires** (5h)
- **Simulation avec un cas** "Comment réagir en cas de cyberattaque" de type apprentissage par inoculation de type "Table test exercises" (5h)

Format horaire 17h30 - 20h30 (post formation et journée de travail)

Annexe 10 : précisions formations pôle CY

CY Cergy Paris Université (CYU) et CY Tech pilote un **pôle dédié à l'innovation et la transformation digitale dans le domaine de la cybersécurité** dans l'ouest parisien. Ce pôle regroupe les graduate schools de CYU CY Tech, « Arts et Humanités », « Droit et Sciences politiques », « Education », les établissements publics et privés associés à CYU (notamment ESSEC avec son META-LAB, ESIEE-IT, ECAM-EPMI, ENSEA), le campus des métiers et des qualifications (CMQ) d'Argenteuil sur la sécurité, l'école WebForce3 (WF3), l'écosystème et campus ixcampus à St Germain-en-Laye. Le **lien entre CYU et l'USPN** permettent de renforcer la synergie des établissements au profit du projet Talents Cybersécurité porté par le Campus cyber : Labex commun en modélisation mathématique, CMQ Sé-curité commun, liens entre les laboratoires d'informatique ETIS de CYU et LIPN de l'USPN.

C**e pôle mobilise plus de 300 enseignants chercheurs** dans les domaines de la cybersécurité, de la data, de l'intelligence artificielle (principalement UMR CNRS CYU et USPN, ESSEC, ESIEE-IT), un réseau de **plus de 400 enseignants et professionnels des entreprises** du secteur de la cybersécurité et de ses domaines connexes, un appui de plus **200 enseignants chercheurs dans les domaines d'application de la cybersécurité** tant en sciences (UMR CNRS en maths et physique quantique, électronique, génie civil) qu'en sciences humaines et sociales (UMR CNRS en économie, UMR CEREMA sur le transport, UMR CNRS et Justice en droit pénal et sécurité, linguistique, politique et gouvernance), et un lien privilégié avec le Pôle Judiciaire de la Gendarmerie Nationale (PJGN) avec lequel CYU a créé une fédération de recherche et d'expertise.

Par rapport au dossier DIGIT@CY déposé par CY en première vague, l'intégration du projet au sein de celui du campus cyber et les précisions complémentaires apportées permettent de répondre aux recommandations du jury, à savoir :

- Un pôle de formation intégré au campus cyber, bénéficiant de l'écosystème de ce dernier, de ses capacités de pilotage et de mise en réseau, permet d'éviter la constitution d'un institut à part ;

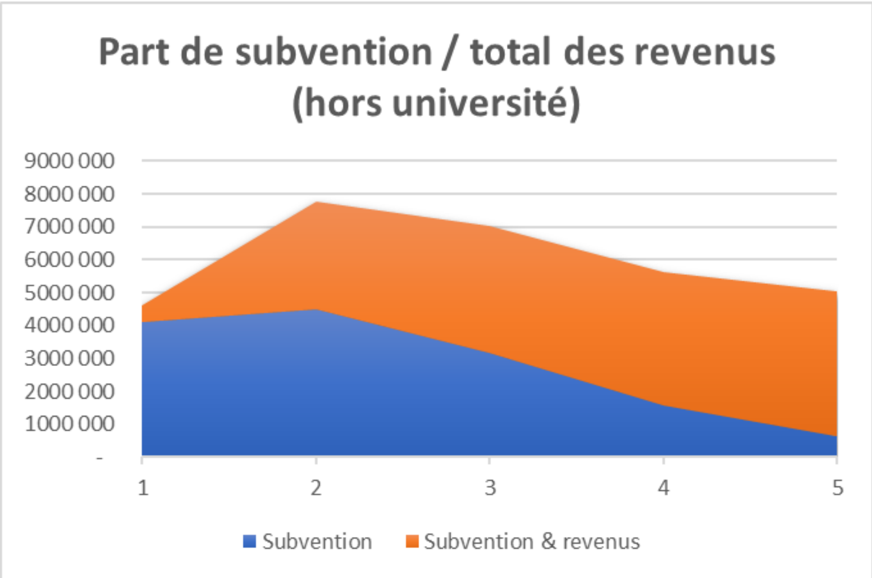
- Le campus cyber déploie un plan à la fois local et national de mise en visibilité des métiers de la cyber qui manquait au projet initial DIGIT@CY ; cet aspect permettra également enrichir le CMQ sécurité et les actions de l'académie de Versailles en direction de la cyber qui joueront le rôle d'amplificateur des actions du projet Talents cybersécurité ;
- La montée en puissance du pôle de formation est décrit dans le tableau ci-dessous, le détail du financement action par action, ainsi que le ratio coût d'impulsion / étudiants formés par le projet ; ces actions sont indépendantes des financements PIA3 obtenus pour le CMQ sécurité, mais l'action 1er cycle «Bachelor » permettra d'étendre le programme d'action du CMQ au-delà du plan d'action financé par le PIA3 ;
- Le campus cyber répond aux enjeux d'attractivité posés par le jury et accroit notre réseau de ressources expertes au delà de nos propres contacts ; le plan RH de recrutement d'enseignants-chercheurs est détaillé dans le corps du projet ;
- L'approche pédagogique est précisée dans le corps du projet ; la production de ressources par le consortium talents cybersécurité permet d'enrichir la mise en œuvre de la modularisation et la création de parcours au sein du pôle.

Le déploiement sur les filières et dans le temps des actions de formation du pôle sont détaillés dans le tableau suivant. Le détail de chacune des actions est indiqué dans le fichier excel de l'annexe financière.

Formations	Partenaire / Ecole	Nb Heures	Année 2023-2024	Année 2024-2025	Année 2025-2026	Année 2026-2027	Année 2027-2028	Nb étudiants /groupe	Nb étudiants formés pdt le projet	Nb étudiants annuel à la fin du projet	Subvention demandée
Action 1 : Mettre en place un programme « émergence » cyber et cyber cross											
Programme "émergence" cyber et cyber cross	CYU		x	x	x	x	x				800 000
Action 2 : Accroitre les diplômes de 1er cycle en cybersécurité											
Action 2.1. Création de nouveaux diplômes post-bac en 3 ans en apprentissage (Bachelor professionnel au CMQ sécurité avec CY Tech)											
Bachelor 1ère année	CMQe Sécurité	650	1	2	2	2	2	40	360	80	350 000
Bachelor 2ième année	CMQe Sécurité	550	1	1	2	2	2	40	320	80	250 000
Bachelor 3ième année	CMQe Sécurité	400		1	1	2	2	40	240	80	250 000
									920	*240*	*850 000*
Action 2.2. Création d'une mineure en cybersécurité pour les étudiants de CYU											
Licence 3 de sciences	CYU	50	1	2	3	4	5	40	600	200	50 000
Action 3 : Accroitre les diplômes de 2e cycle en cybersécurité											
Action 3.1. Création de nouveaux diplômes et parcours en master (2 ans) et en cycle ingénieurs (2 ou 3 ans) à CY Tech et l'ECAM-EPMI											
M1 CY Tech (Master et ingénieur)	CY Tech	600	1	2	3	3	3	40	480	120	450 000
M2 CY Tech (Master et ingénieur)	CY Tech	500		1	2	3	3	40	360	120	350 000
Filière cybersécurité en 3ème année du cycle ingénieur	ECAM-EPMI	450	1	2	2	2	2	45	405	90	350 000
									1245	*330*	*1 150 000*
Action 3.2. Création de nouveaux doubles diplômes CY Tech - ESIEE-IT et CY Tech - CY école de design											
2ème année ingénieur "Ingénierie de la Cybersécurité" (bac+4)	CY Tech et ESIEE-IT	650		1	2	2	2	30	210	60	350 000
3ème année ingénieur "Ingénierie de la Cybersécurité" (bac+5)	CY Tech et ESIEE-IT	450			1	2	2	30	150	60	250 000
ème année ingénieur "Intelligence Artificielle pour la Cybersécurité" (bac+	CY Tech et ESIEE-IT	650			1	2	2	30	150	60	350 000
ème année ingénieur "Intelligence Artificielle pour la Cybersécurité" (bac+	CY Tech et ESIEE-IT	450				1	2	30	90	60	250 000
Ingénieur Cybersécurité et Design 1ère année	CY Tech et CY design	650	1	2	2	2	2	40	360	80	350 000
Ingénieur Cybersécurité et Design 2ième année	CY Tech et CY design	650		1	2	2	2	40	280	80	250 000
Ingénieur Cybersécurité et Design 3ième année	CY Tech et CY design	450			1	2	2	40	200	80	250 000
									1440	*480*	*2 050 000*
Action 3.3. Création de ressources pédagogiques experts et cas d'études pour les Master et parcours Grande Ecole (ESSEC Metalab)											
Soutien à la pédagogie (METALAB)	ESSEC		x	x	x	x	x				980 000
Axe 4 - Accroitre les diplômes de formation tout au long de la vie											
Action 4.1. Création de Mastères spécialisés et MBA											
Mastère Spécialisé en cybersécurité	CY Tech et ESIEE-IT	500	1	1	2	2	2	40	320	80	350 000
Mastère Spécialisé en cybersécurité et systèmes intelligents	CY Tech / iXCampus	500	1	1	1	1	1	40	200	40	250 000
Mastère Spécialisé de cyber criminalistique	CY Tech	500	1	1	1	1	1	40	200	40	250 000
Mastère Spécialisé d'expertise judiciaire des données	CY Tech	450		1	1	1	1	40	160	40	150 000
MBA "Cybersécurité & IoT"	CY Tech	400		1	1	1	1	40	160	40	250 000
									1040	*240*	*1 250 000*
Action 4.2. Création de certifications et modules de FTLV											

Ecole sur "Les bases"	iXCampus	200	1	1	1	2	2	20	140	40	105 000
Ecole sur "Les bases pour les femmes dans le cyber"	iXCampus	200	1	1	2	2	2	20	160	40	105 000
Formation - "Analyste sécurité"	iXCampus	40	1	1	1	2	2	20	140	40	50 000
Une prépa-apprentissage aux métiers de la cybersécurité : #FabrikTaCyber (public décrocheurs)	WebForce3	230	1	1	1	1	1	20	100	20	120 000
echnicien supérieur systèmes et réseaux » (bac+2) - alternance / certificatic	WebForce3	662	1	1	1	1	1	20	100	20	250 000
Administrateur infrastructures sécurisées (bac+3) - alternance	WebForce3	740	1	1	1	1	1	20	100	20	250 000
Développeur d'applications à dominante cybersécurité (RNCP Bac+2) - Formation en ligne	ESIEE-IT	450	1	1	2	2	2	30	240	60	350 000
Expert en cybersécurité année 1 (RNCP bac +4) Temps plein ou Apprentissage - Formation en ligne	ESIEE-IT	450	1	1	2	2	2	30	240	60	350 000
Expert en cybersécurité année 2 (RNCP bac +5) Temps plein ou Apprentissage - Formation en ligne	ESIEE-IT	450		1	1	2	2	30	180	60	250 000
									1400	*360*	*1 830 000*
Action 4.3. Création de dispositif de VAE hybride											
VAE hybride	CYU		1	2	3	4	6	5	80	30	100 000
Action 5 : Management du pôle DIGIT@CYBER											
Coordination du pôle et des actions pédagogiques du pôle DIGIT@Cyber	CYU		x	x	x	x	x	x			500 000
TOTAL									6725	1880	**9 560 000**

Annexe 11 : part de subvention dans le projet global



ADDENDUM AU DOCUMENT SCIENTIFIQUE CMA 2023	Acronyme du projet TAL-CYB

ANNEXE

REPONSE AUX RECOMMANDATIONS DU JURY

Nous remercions le jury pour l'ensemble de ces remarques positives sur notre dossier retravaillé selon ses remarques. Nous nous assurerons de la mise en œuvre de l'ensemble du projet tel que validé par le jury en mettant un point d'orgue à travailler de la manière la plus collaborative possible, notamment en produisant des ressources libres d'accès pour bénéficier à toute la communauté.

Nous avons bien pris en compte les recommandations du jury et resterons attentifs à leur mise en œuvre en lien avec les autorités nationales adéquates.

- Concernant la formation des formateurs, elle est un des points clé du dossier. Ayant déjà entamé les formations en lien avec le DGESCO en septembre et octobre dernier, nous continuerons de renouveler l'expérience et ce dès la rentrée 2023. Nous nous assurerons, en lien avec l'écosystème, que cette formation est adéquate avec les besoins du secteur et ses évolutions dans les années à venir. Nous avons signé une convention avec la DGESCO au mois de mai dernier, ce qui assure une réelle coordination entre nos deux établissements dans la durée. Par ailleurs, la DGESCO est impliquée dans le groupe de travail formation du Campus Cyber pour favoriser l'effort collectif. Des affiches présentant les métiers de cybersécurité seront notamment mises en place dès la rentrée 2023 dans tous les collèges de France en lien avec la réforme des collèges.
- Concernant l'accentuation de l'effort en matière de formation précoce aux mathématiques, l'ensemble des ressources d'attractivité créée par le consortium poursuivront un même objectif : celui d'acculturer, et ce dès le plus jeune âge (primaire) aux métiers de la cybersécurité afin de créer des vocations pour tous les métiers, techniques et non techniques. Par ailleurs, le passage à l'échelle des actions de l'association CGénial dans les écoles avec ses projets numériques et cybersécurité participera à la formation des jeunes garçons et jeunes filles aux compétences techniques nécessaires aux métiers de la cybersécurité.

La participation des opérateurs de l'AMI CMA ainsi que des ministères en charge des thématiques de formation sera clé dans l'alignement et la poursuite des objectifs mentionnés ci-dessus.