GOUVERNEMENT
Liberté
Égalité
Fraternité

4e Programme d'investissements d'avenir (PIA 4)

Volet « dirigé »

Cybersécurité

Le cahier des charges est disponible ici : https://anr.fr/CMA-2021

AMI Compétences et Métiers d'Avenir
Volet 1

La stratégie d'accélération « Cybersécurité »

La stratégie nationale en cybersécurité s'articule autour de 4 axes :

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

De plus, une des cibles principales de la stratégie est de doubler le nombre d'emplois dans la filière d'ici 2025, soit 37 000 emplois supplémentaires. Cet objectif implique naturellement un effort de formation important.

La réponse aux besoins de formation de la filière

Coût estimé du volet formation de la Stratégie nationale Cybersécurité

Le budget estimé pour financer le volet formation de la Stratégie Nationale cybersécurité est de 140M€.
- Il n'est pas concevable de vouloir créer 37 000 emplois dans la filière sans une formation a plusieurs niveaux ambitieuses.

- 25%, soit environ 9250 personnes, seront formées afin de devenir des spécialistes du domaine, et ce, à tous les niveaux de bac +2 à bac +8. La recherche sera impactée via le financement de 100 thèses

- La formation massive des non spécialistes (610 000 étudiants par an), permettra de donner un socle indispensable sur la cybersécurité à de nombreux étudiants, même ceux dont les domaines d'études peuvent paraître éloigner du sujet,

- La formation professionnelle par l'intermédiaire de formations courtes pour permettre la montée en compétences de 10 000 salariés.

La filière fait face à un déficit de main d'œuvre alors qu'elle peut être un **débouché pour tous les niveaux, de baccalauréat professionnel à doctorant,** ainsi que pour différents domaines de formations (techniques, commerciales, juridiques, etc.).

La formation représente donc une part importante de la stratégie sur deux aspects :

- Former davantage de personnes aux métiers de la cybersécurité incluant toute les déclinaisons de niveau de spécialisation (bac pro, bac+2, bac+3, bac+5, bac+8 et formation continue) en fonction des postes visés pour répondre à la très forte demande en compétences du secteur et soutenir sa croissance.
- Former le plus grand nombre aux enjeux, dangers et gestes simples de la cybersécurité à la fois pour soutenir la demande mais aussi, et surtout, pour élever le niveau de sécurité global du pays.

La stratégie propose également d'établir un meilleur diagnostic sur le long terme des besoins, métiers et formations existants et de communiquer pour orienter les étudiants de manière plus efficace.

Trois mesures concernent directement l'axe formation :

- Mise en place d'un observatoire qui analysera les besoins en compétences et l'adéquation

avec les formations existantes pour le secteur de la cybersécurité,
- Création de formations courtes en cybersécurité,
- Renforcement et/ou multiplication de l'offre de formation spécialisée en lien étroit avec l'expertise des acteurs de la filière, sur la base d'une consolidation des besoins et de la demande des employeurs du secteur.

La stratégie d'accélération en cybersécurité doit inciter financièrement le système de l'enseignement supérieur à :

- **action 1 :** adapter et développer l'offre de formation à la cybersécurité au niveau Bac+3 (BUT, licence, licence professionnelle), au niveau Master (SHS, droit, santé, informatique, …) et Ingénieur, afin de répondre aux enjeux de la stratégie d'accélération, aux besoins du monde professionnel et de la recherche ; ce besoin sera évalué grâce aux résultats de la mesure 18 sur l'expression des besoins et aux cibles fixées par le monde de la recherche ;
- **action 2 :** construire un lien fort avec le monde professionnel, de manière à former les étudiants sur des cas d'usage réels, les préparant ainsi à une meilleure adéquation avec les besoins du monde industriel ;
- **action 3 :** lier en partie les actions de formation aux enjeux de la recherche, dans la mesure où la formation supérieure technologique repose pour part sur la participation à des projets de recherche (par exemple à l'occasion d'un doctorat ou lors de la préparation d'un master "orienté recherche") ;
- **action 4 :** créer une offre de formation tout au long de la vie en cybersécurité et nouer des passerelles avec le système de formation professionnelle continue, en proposant une montée en compétences (up-skilling) ou des reconversions professionnelles (re-skilling) dans les métiers de la cybersécurité ;
- **action 5 :** structurer l'offre de formation, la rendre lisible et attractive pour les jeunes afin de les engager vers les formations mises en place ; une attention particulière devra être accordée à la communication envers le public féminin ;
- **action 6 :** former tous les étudiants de l'enseignement supérieur aux enjeux de la cybersécurité, notamment en lien avec leur domaine disciplinaire.
- **action 7 :** accélérer la création de l'observatoire des compétences et des métiers cyber grâce à une étude.

Chiffrage estimé

Un des objectifs principaux de la stratégie vise à créer 37 000 emplois dans la filière qui représentent autant de personnes à former. On peut prévoir qu'environ 25% seront des spécialistes cyber issus de la formation initiale ce qui correspond donc à 9 250 spécialistes cyber à former en 5 ans. La répartition que l'on peut anticiper dans un premier temps (en attendant les éléments plus précis de l'observatoire) serait 10% bac pro, 15% bac+2, 30% bac+3, 44% bac+5, 1% bac+8.

Soit un chiffrage estimé (à 60€ de l'heure de formation, préparation de contenus et supports partageables inclus) :

- Bac pro : 950 étudiants à 200 heures de formation cyber par classes de 30 soit 380k€
- Bac +2 (BTS) : 1 400 étudiants à 500 heures de formation cyber par classes de 30 soit 1,4M€
- Bac +3 (L et LPro) : 2 800 étudiants à 800 heures de formation cyber par classes de 30 soit 4,48M€
- Bac +5 (Master) : 4 000 étudiants à 1800 heures de formation par classes de 25 soit 17,28M€
- Bac +8 (Doctorats) : 100 étudiants (110 k€ pour le salaire + 20 k€ fonctionnement, par thèse), soit 13 M€.

- Dans le cadre de ces formations pour spécialistes, un « overhead » de 20% (a priori) est estimé pour leur mise en place et leur fonctionnement, soit 7,3M€.

Soit un total de 44M€ pour la **formation initiale spécialisée en cybersécurité** sur les 5 prochaines années.

De plus, il est essentiel de former à la cybersécurité de manière large les non spécialistes, une grande partie des emplois à créer dans la filière correspondant à ce type de profils (entre 25% et 50%) et le niveau global de cybersécurité reposant de manière large sur les utilisateurs. Cela correspond à former 610 000 étudiants par an, soit 3 050 000 étudiants sur 5 ans.

- niveau L : 60 € de l'heure de formation (incluant la réalisation de supports partageables) * nouveaux bacheliers (350 000) pour 12 heures de formation par classes de 30 = 8,4M€/an soit 42M€ sur 5 ans
- niveau M : 260 000 étudiants * 60€ de l'heure pour 12 heures de formation par classes de 25 = 7,5 M€/an 37,5M€ sur 5 ans
- Formation professionnelle et auprès du grand-public (plusieurs MOOC selon les niveaux) MOOC : 1M€
- Dans les cadre de ces formations pour non spécialistes, un « overhead » de 10% (a priori) est estimé pour leur mise en place et leur fonctionnement, soit 8M€.

Soit un total de 88,5M€.

Formation tout au long de la vie : la montée en compétences des salariés déjà en activité s'effectuera via des actions courtes délivrées par les acteurs de la formation : **3M€** par an pour former 15 000 personnes.

Enfin, pour la sensibilisation dans le secondaire la formation continue, une montée en puissance de **PIX à hauteur de 6M€** sera nécessaire.

Une enveloppe de **200k€** est envisagée dans le cadre du volet « diagnostic » de l'AMI « compétences et métiers d'avenir » afin d'anticiper le rôle de l'observatoire et permettre une analyse des besoins en compétences et en métiers émergents sur le sujet de la cybersécurité.

Le coût total s'élève donc à **141,7 M€**.