RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

conseil national de l'industrie

Contrat stratégique de filière Industries de sécurité 2024-2027

Mars 2025

Sommaire

Editorial du président

Les industries de sécurité ont la particularité d'être très liées à des problématiques régaliennes. Ce sont des industries qui naturellement ont un rôle essentiel pour la souveraineté et la résilience de la Nation.

A travers ce deuxième contrat, la filière souhaite affirmer sa capacité et sa volonté de progresser au plus haut niveau pour assurer son développement économique et répondre aux impératifs de résilience et de sauvegarde des intérêts fondamentaux de la Nation, en s'appuyant sur un dialogue étroit et permanent entre l'industrie et l'État.

Les industriels de la filière, qui bénéficient d'un socle très solide de compétences d'excellence et d'une grande capacité d'initiative, visent à travers ce deuxième contrat à mobiliser avec l'État les grands leviers à leur disposition pour concrétiser des objectifs-clés à leur portée en matière de développement et de compétitivité, comme de souveraineté, de résilience et de décarbonation. Après une concertation qui s'est voulu plus large que lors de la précédente édition, le contrat s'est construit autour des grands marqueurs suivants :

- intensifier au sein du contrat stratégique de filière (CSF) le dialogue avec l'État, notamment sur les sujets où la position de celui-ci conditionne les solutions ou influe sur les modèles économiques de l'industrie, et conduire une réflexion stratégique permanente sur son avenir ;
- progresser avec exigence vers des solutions de qualité, innovantes, compétitives et éthiques, en intensifiant le dialogue avec les marchés cibles. Les cibles sont : les forces de sécurité intérieure et acteurs du continuum de sécurité, les collectivités territoriales, les grands évènements, les utilisateurs de l'identité numérique, les établissements de santé, les PME (pour leur besoin en sécurité) et les entités critiques pour les besoins de résilience ;
- rechercher au sein des évolutions du cadre réglementaire, les opportunités qui peuvent se dessiner. On peut notamment penser aux marchés qui pourraient être induits par la mise en œuvre de la directive sur la résilience des entités critiques (REC) et de la seconde directive sur la sécurité des réseaux et de l'information (NIS 2) ;
- renforcer le soutien aux PME de la filière et le lien avec la recherche pour poursuivre l'édification d'une base industrielle forte et souveraine ;
- développer les actions transverses pour renforcer l'esprit de filière.

La filière « industries de sécurité » propose ainsi pour les trois prochaines années de travailler selon les quatre axes stratégiques suivants :

- Axe 1 : favoriser la croissance d'une filière compétitive et d'excellence au plan national et international.
- Axe 2 : élaborer une feuille de route technologique pour garantir la maîtrise des technologies d'avenir clés et des technologies critiques.
- Axe 3 : renforcer l'attractivité des emplois, anticiper et répondre aux besoins en compétence de la filière.
- Axe 4 : accompagner la transition écologique de la filière « industries de sécurité » vers une production décarbonée et réduite en impact énergétique.

Marc DARMON

La filière des industries de sécurité

Les chiffres-clés ici présentés sont issus de l'observatoire de la filière « industries de sécurité » de 2022.

La filière « industries de sécurité » est cruciale dans notre économie et dans notre société en pleine mutation numérique.

La filière « industries de sécurité » réunit l'ensemble des acteurs à même de répondre aux enjeux de sécurité suivants, qui constituent le périmètre de la filière :

- la lutte contre le terrorisme et la grande criminalité ;
- la sécurité du quotidien et secours aux personnes ;
- la protection des infrastructures et des réseaux (dimensions physique et cyber) ;
- la gestion de la crise quelle que soit son origine (naturelle, technologique, malveillante), à l'échelle nationale et à l'échelle territoriale ;
- la protection des frontières de l'Union européenne ;
- la cybersécurité.

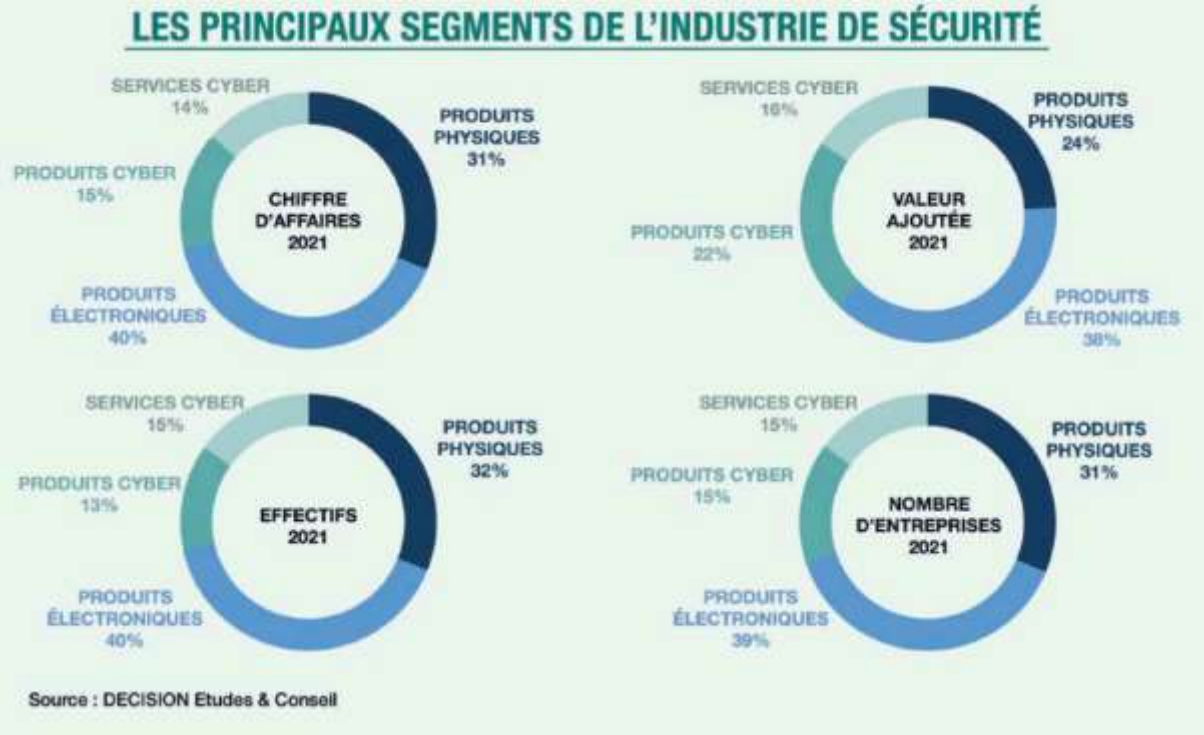
Elle regroupe ainsi la sécurité physique (véhicules et plateformes, vêtements de protection, équipements et fourniture - y compris la sécurité incendie, ainsi que les outils d'interdiction physique d'accès, etc.), la sécurité électronique et numérique (identité numérique, systèmes et sous-systèmes électroniques de confiance, de sécurité incendie, de surveillance, communication, traçage, etc.), ainsi que la cybersécurité (produits / logiciels et services).

Une filière en cours d'unification par les produits

La filière « industries de sécurité » est cruciale dans notre économie et dans notre société en pleine mutation numérique. Les produits et services qu'elle regroupe sont destinés aussi bien aux marchés professionnels (État et secteur public, infrastructures critiques, entreprises, PME) qu'au grand public (ordinateurs, smartphones, maison, véhicules, objets connectés, etc.).

Les produits électroniques demeurent le premier segment de la filière avec 40 % du chiffre d'affaires en 2021. Cependant, avec une croissance annuelle moyenne de près de 10 % sur la période 2018-2021, la cybersécurité prend de plus en plus d'importance dans la filière et représente en 2021 près de 30 % de son chiffre d'affaires total, soit 9,1 milliards d'euros[1]. En comparaison, la cybersécurité représentait moins de 5 % du chiffre d'affaires de la filière au début des années 2000 et devrait égaler, en chiffre d'affaires, les produits électroniques à l'horizon 2025-2030.

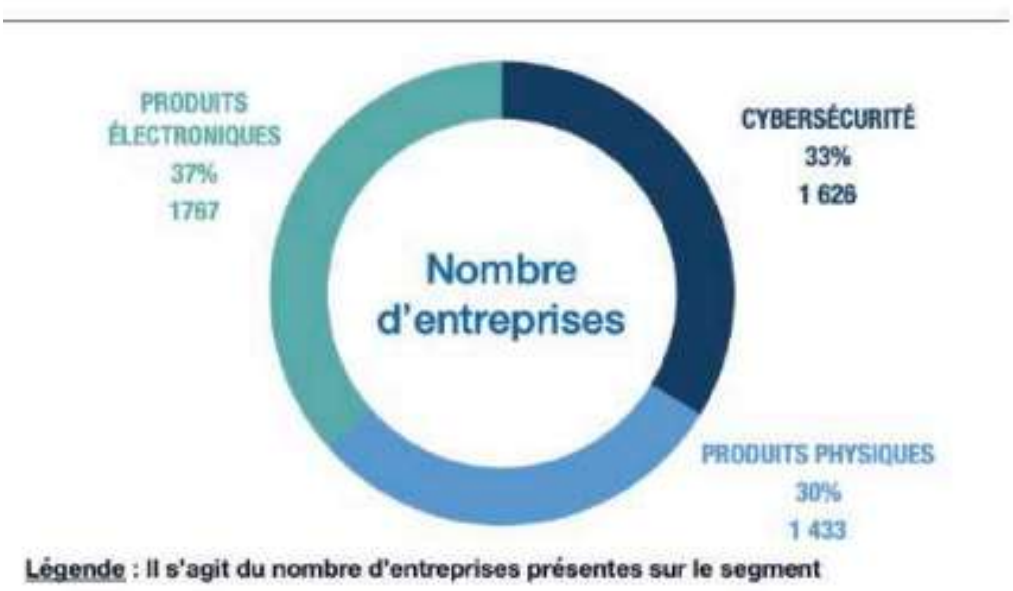
[1] Les chiffres de la cyber prennent en compte les produits et les services contrairement à ceux des autres sous-segments.



La filière « industries de sécurité » regroupe un écosystème d'entreprises de toutes tailles, qui s'établissait, en 2021 (dernière année dont les chiffres sont disponibles), à **4 402 entreprises,** dont :

- 90 grandes entreprises
- **91 ETI (Entreprises de Taille Intermédiaire)**
- 1 723 PME (Petites et Moyennes Entreprises)
- 2 498 micro-entreprises, générant moins de 2 millions de CA en 2021

Source – Observatoire de la filière « industries de sécurité » 2022 (DECISION Etudes et Conseil)



La filière « industries de sécurité » en France en 2021, représentait :

- 31,9 milliards d'euros de chiffre d'affaires, soit 4,3% de croissance annuelle moyenne entre 2016 et 2021 ;
- 12,9 milliards d'euros de valeur ajoutée ;
- un total de 157 000 employés ;
- un chiffre d'affaires réparti à 40% pour la sécurité électronique, 31% pour la sécurité physique et 29% pour la cybersécurité.

Elle était marquée par une forte dynamique de rachats/consolidation (en moyenne 35 rachats par an sur la période 2020-2022).

Source – Observatoire de la filière industrielle de sécurité 2022 (DECISION Etudes et Conseil)

→ *L'industrie de sécurité est une filière industrielle française à part entière*

En 2020, en termes de valeur ajoutée, la filière « industries de sécurité » reste par rapport à 2017 à la 12ème place des industries manufacturières françaises (sur 16), entre la filière « produits informatiques, électroniques et optiques », et la filière « bois, papier et imprimerie ». En termes d'emploi, la filière « industries de sécurité » demeure aussi par rapport à 2017 à la 10ème place des industries manufacturières françaises (sur 16), entre l'industrie « bois, papier et imprimerie » et l'industrie « produits informatiques, électroniques et optiques ».

La France se situe à la 3ème place au niveau mondial, loin derrière les États-Unis et la Chine, à une position proche de celle des industries japonaise, allemande et britannique et concurrencée par les industries sud-coréenne et israélienne en forte croissance.

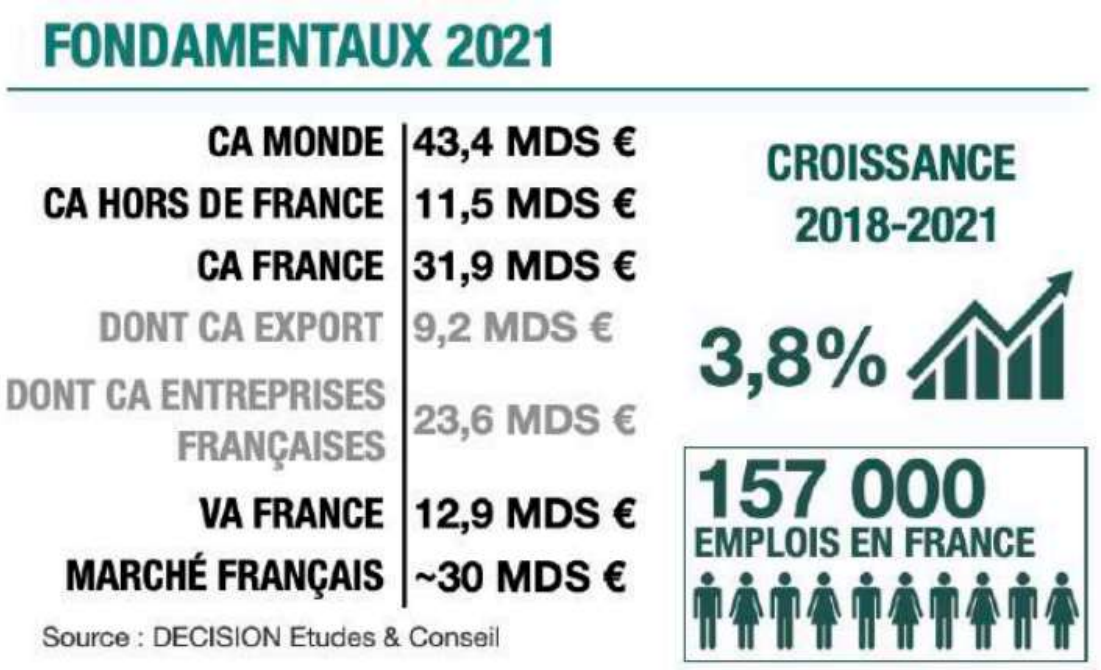
Les produits de sécurité intègrent de plus en plus une composante physique, une composante électronique et une composante cyber. De façon similaire, les acteurs de la filière se positionnent de plus en plus sur ces trois segments.

Leurs croissances sont donc fortement corrélées, en particulier celles de l'électronique et de la cybersécurité. **En d'autres termes, l'unification de la filière est en train de s'opérer par les produits.** La cybersécurité, qui comprend une très forte part de travail humain, augmente mécaniquement le taux de valeur ajoutée de la filière.

L'industrie de sécurité est affectée par deux facteurs majeurs :

- la miniaturisation couplée à la baisse des coûts des composants électroniques, conduisant à une croissance toujours plus importante de la part des systèmes ou sous-systèmes électroniques dans les produits de sécurité ;
- la transformation digitale, conduisant à une croissance toujours plus importante de la part des logiciels dans les outils de sécurité.

Le croisement de ces deux facteurs conduit progressivement les acteurs de la filière à se positionner sur l'ensemble des segments : physique, électronique et cyber. **La distinction physique/électronique/cyber est en conséquence progressivement appelée à avoir de moins en moins de sens, et à long terme, il est probable que chaque architecture de produit soit globale avec une composante physique, une composante électronique et une composante cyber. Cette tendance touche même les services privés de sécurité.**



Une filière où l'innovation technologique est le principal moteur de croissance

Grâce notamment à l'excellence française en matière de recherche et développement, la majorité des grandes entreprises et entreprises de taille intermédiaire (ETI) françaises des industries de sécurité sont positionnées sur les segments haut de gamme de leurs marchés en proposant des solutions à la pointe de ce que la technologie rend aujourd'hui possible. La France excelle en particulier dans les domaines suivants : intelligence artificielle (IA) et machine learning, cryptographie, technologies post-quantique. La France est également en bonne position en blockchain et en sécurisation des objets connectés.

Les développements technologiques ont une incidence sur la filière « industries de sécurité » de deux façons :

- par le biais d'innovations globales qui génèrent de nouveaux marchés : les innovations issues des industries électronique et numérique ont ainsi une incidence sur presque tous les secteurs des économies modernes et génèrent, de ce fait, de nouveaux marchés pour l'industrie de la sécurité, dans les domaines notamment de la sécurité des objets connectés, de la souveraineté de la donnée, des identités numériques de confiance, de la transformation digitale, moteur de la plupart des segments de la cybersécurité ;
- par le biais d'innovations propres à la filière qui génèrent de nouveaux produits : les innovations issues des industries sécurité en elle-même génèrent de nouveaux produits, de nouvelles applications et donc de la croissance, dans les domaines notamment de la cryptographie, des éléments sécurisés (secure elements), de l'IA, des plateformes robotiques (dont drones), de l'analyse en temps réel des données d'observations locales et large zone, de la blockchain.

Une filière à forte valeur ajoutée

La filière « industries de sécurité » est une filière à forte valeur ajoutée et à haute intensité d'innovation qui participe au développement industriel de la Nation et qui est fortement exportatrice. **C'est une des filières les plus productives du conseil national de l'industrie avec un taux de valeur ajoutée rapporté au chiffre d'affaires de 41% en 2020.** En d'autres termes, la filière « industries de sécurité » est la filière industrielle dont le degré de création de richesse, c'est-à-dire de transformation des produits au cours de l'activité, est le plus élevé. Ainsi, l'augmentation du chiffre d'affaires de cette filière se traduit en moyenne par un plus fort taux d'activité transformatrice sur le sol français en comparaison des autres filières industrielles françaises.

Ce phénomène s'explique principalement par les facteurs suivants :

- le pourcentage de l'activité dédiée aux services est relativement élevé, que ce soit à travers les activités d'installation de matériels physiques et électroniques (13% du chiffre d'affaires total en 2021), ou à travers les services de cybersécurité (conseil, audit, formation, etc.) qui ont représenté 14% du chiffre d'affaires total en 2021 ;
- la cybersécurité dans son ensemble correspond à près de 29% du chiffre d'affaires total de la filière de sécurité en 2021. Or, les services de cybersécurité mais également les produits de cybersécurité impliquent une très grande partie de travail humain hautement qualifié (développement de logiciels, notamment) expliquant un taux de valeur ajoutée très élevé.

La filière « industries de sécurité » est une des filières qui bénéficie des meilleures perspectives de croissance pour les années à venir : la croissance annuelle moyenne de la filière est au-dessus des 5% depuis 10 ans sauf en 2020 du fait de la pandémie de la Covid-19. Toutefois, l'industrie a bien rebondi dès 2021 avec 5% de croissance annuelle. Cette tendance de croissance devrait se maintenir sur la période du contrat grâce aux nombreuses innovations technologiques dont la filière est porteuse, et aux événements d'envergure accueillis par la France.

Bilan des réalisations du contrat stratégique de filière de 2020 à 2022

Le précédent contrat était construit autour de cinq projets structurants dont le bilan harmonisé peut être fait :

Projet 1 : La sécurité des grands évènements et des Jeux olympiques et paralympiques Paris 2024 (JOP 2024)

Dans le cadre de ce projet, le contrat stratégique de filière des industries de sécurité (CSF IS) a permis la constitution d'une « équipe France » pour répondre de façon coordonnée aux marchés liés à la sécurisation des grands évènements, au travers d'offres innovantes associant des grands groupes, des PME et ETI. Les partenariats ainsi formés permettent l'élaboration d'une offre réplicable à l'export.

En partenariat avec le secrétariat général de la défense et de la sécurité nationale (SGDSN) et le ministère de l'intérieur et des outre-mer, près de 200 expérimentations mettant en avant des entreprises et solutions françaises à 95%, et portées à 75% par des PME ont, par ailleurs, été menées. Ces expérimentations se sont traduites par des acquisitions dans le cadre des JOP 2024 et à l'élaboration d'offres exportables.

Projet 2 : La cybersécurité et la sécurité de l'internet des objets

Les travaux du CSF-IS 2020-2022 ont permis la mise en place d'un comité de pilotage réunissant bimestriellement les industriels fournisseurs de solutions, les utilisateurs publics et privés et l'administration. Ce comité a pu être mobilisé par l'administration afin de faire valoir les intérêts de la filière dans le cadre de l'élaboration de différents plans (France Relance, Stratégie d'accélération cyber, Grand défi cyber, etc.)

En partenariat avec la direction générale des entreprises (DGE), le « comité cybersécurité » a contribué à l'organisation de l'édition 2021 et 2022 de la « Journée autonomie et souveraineté numérique » qui réunit chaque année les acheteurs publics et les offreurs de solutions.

Dans la même démarche de mise à disposition de l'offre auprès des acheteurs publics, un catalogue de solutions et services pour les collectivités territoriales, les établissements de santé et les organismes au service des citoyens a été publié, s'appuyant sur les standards définis par France Relance.

Projet 3 : L'identité numérique

Un partenariat a été mis en place dans le cadre du CSF IS réunissant l'Imprimerie nationale, l'administration et les industriels de la filière. Ce partenariat a permis la production des spécifications initiales, étendues au système d'information de la carte nationale d'identité électronique (CNIe) courant 2021 pour aboutir au lancement de la nouvelle CNI en 2022.

Projet 4 : Les territoires de confiance

Afin de répondre aux enjeux éthiques du numérique et du traitement des données, en particulier dans le cas d'applications aux collectivités territoriales, une charte éthique liant l'industrie et les utilisateurs de technologies de sécurité a été adoptée en 2021.

Un groupe de travail mixte, réunissant les collectivités territoriales et les industriels a été constitué dès 2020. Ce groupe a permis la définition d'une feuille de route partagée pour la constitution de territoires « smart & safe ». Dans la continuité de cette feuille de route, un recueil des besoins et un premier cahier des charges ont été définis afin d'élaborer une offre sous forme de plateforme de services à destination des collectivités, modulable en fonction des besoins.

Enfin, un guide sectoriel pour la protection des établissements de santé a été produit par les industriels de la sécurité, couvrant les trois segments de la filière (sécurité physique, sécurité électronique et cybersécurité).

Projet 5 : Le numérique de confiance

Le principal objectif du groupe de travail « numérique de confiance » consistait à permettre la production d'une offre de cloud de confiance compétitive. Dans ce cadre, le groupe de travail, mobilisé par l'administration, a rendu des avis pour l'élaboration de la stratégie d'accélération « cloud », l'établissement de la doctrine de l'État « Cloud au centre » et la version 3.2 de la certification « SecNumCloud ».

Les axes stratégiques et les objectifs du contrat

A. Les axes stratégiques du contrat

La filière « industries de sécurité » propose pour les trois prochaines années de travailler en commun selon les quatre axes stratégiques suivants :

Axe 1 - Compétitivité et souveraineté : favoriser la croissance d'une filière compétitive et d'excellence au plan national et international

Renforcer la compétitivité des PME et des ETI de la filière : le développement d'une industrie de sécurité puissante nécessite l'accès des PME et ETI en croissance aux financements. Dans une filière où les enjeux stratégiques sont importants, notamment les enjeux de souveraineté, les acteurs majeurs de la filière ont un rôle actif à jouer en tant qu'investisseur, en particulier lors de la phase de capital développement où les tickets sont souvent relativement importants.

Enjeux :

- *accompagner les entreprises à fort potentiel jusqu'à la phase d'industrialisation ou d'entrée en bourse, pour faire émerger au moins 5 à 10 grands champions industriels français de la sécurité dans le monde ;*
- *accroître le nombre d'ETI pour développer l'innovation, la croissance et l'emploi.*

Concevoir et valoriser au plan national et international des offres de solutions et de services de sécurité innovantes et compétitives dans les trois segments de la filière « industries de sécurité » (physique, électronique et cyber) sur les marchés stratégiques suivants : *forces de sécurité intérieure et acteurs du continuum de sécurité (sécurité des frontières et innovations d'usage), collectivités territoriales, grands évènements, cas usage autour de l'identité numérique, PME, entités critiques.*

Enjeux :

- *favoriser la multiplication des usages autour de l'identité numérique de confiance issue de la CNIe en impliquant plus largement les PME et les start-ups afin de renforcer l'écosystème français de l'identité numérique ;*
- *proposer aux collectivités territoriales une offre de sécurisation en particulier pour leurs services identifiés comme essentiels et renforcer la résilience des collectivités territoriales ;*
- *développer des modes innovants de sécurisation des différentes typologies de frontières ;*
- *offrir aux forces de sécurité intérieure et acteurs du continuum de sécurité un gain opérationnel et humain autour du triptyque capacitaire « détecter, exploiter, agir » ;*
- *répondre aux besoins et aux spécificités des PME en matière de cybersécurité et, plus globalement, contribuer, à travers ce chantier ciblé sur les PME, à développer une filière d'excellence ;*
- *capitaliser sur les solutions développées par la filière dans le cadre des JOP 2024 pour d'autres grands évènements, y compris à l'étranger ;*
- *favoriser l'accès à de nouveaux marchés et augmenter les parts de marché à l'export.*

S'appuyer sur la normalisation et la certification pour développer les avantages comparatifs de la filière à l'international : investir dès aujourd'hui le champ de la normalisation en matière de sécurité permet de défendre les intérêts des entreprises de la filière, innovantes, dans le domaine des futures technologies de sécurité.

Enjeux :

- *renforcer la présence de la filière dans les instances européennes et internationales de normalisation pour en faire un outil important d'influence dans la conquête de marché ;*
- *promouvoir des schémas de certification dans le cadre des organismes compétents et anticiper leurs évolutions. .*

Axe 2 - Maîtrise des technologies et innovation : élaborer une feuille de route technologique pour garantir la maîtrise des technologies d'avenir clés et des technologies critiques

Enjeux :

- *maintenir une filière « industries de sécurité » à la pointe de l'innovation en s'appuyant sur un écosystème de recherche performant ;*
- *contribuer à la souveraineté industrielle et numérique du pays ;*
- *maîtriser les technologies dites « critiques », c'est à dire indispensables à la sécurité et à la résilience de la Nation et nécessitant une politique industrielle spécifique de par leur caractère sensible.*

Axe 3 – Développement des compétences et de l'attractivité de l'industrie

Renforcer l'attractivité des emplois, anticiper et répondre aux besoins en compétence de la filière : les métiers de l'industrie et du numérique en général souffrent d'un déficit d'attractivité alors que de nombreux emplois sont actuellement à pourvoir dans ce secteur.

Un déficit d'attractivité auquel s'ajoute un décalage croissant entre les besoins en compétences et celles effectivement disponibles sur le marché du travail.

Enjeux :

- *identifier dans la durée les évolutions des métiers et des compétences, ainsi que les besoins de formations qui en découlent ;*
- *renforcer ainsi la structuration de la filière en matière d'emplois et de compétences ;*
- *faire connaître et valoriser la diversité des métiers de la filière « industries de sécurité », en particulier auprès du public féminin et renforcer plus généralement le caractère inclusif et la diversité de la filière.*

Axe 4 – Transition écologique

Accompagner la transition écologique de la filière « industries de sécurité » vers une production décarbonée et réduite en impact énergétique : il est aujourd'hui impossible d'ignorer l'urgence écologique et les enjeux de transition qui en découlent. L'ensemble de l'économie, y compris les industries de sécurité, doit engager sa planification écologique.

Quelques chiffres-clés : en 2020, le numérique représentait 2,5% de l'empreinte « carbone » annuelle de la France, 10% de sa consommation électrique annuelle et environ 27% de l'épuisement des ressources abiotiques naturelles. Les émissions de gaz à effet de serre du numérique pourraient augmenter de plus de 60% d'ici 2040 si rien n'est fait.

Enjeux :

- *il s'agit ici des enjeux définis par la feuille de route du conseil national de l'industrie, appliqués à la filière « industries de sécurité » :*
- *produire moins et mieux, adapter les sites industriels et chaînes d'approvisionnement aux conséquences des changements climatiques pour renforcer la sobriété et l'adaptation des processus industriels ;*
- *poursuivre les efforts d'efficacité énergétique et la transition vers les sources d'énergie renouvelables, tout en développant la production industrielle en France pour assurer la transition énergétique des industrie de sécurité.*

B. Les modalités d'évaluation du contrat

Objectif 1 - Augmenter le nombre d'ETI de la filière industrie de sécurité

Accroître le nombre d'ETI revêt un caractère décisif pour développer l'innovation, la croissance et l'emploi. De manière globale pour l'économie française, cette taille d'entreprise est insuffisamment représentée dans le tissu économique national : 5 400 ETI en 2021 soit presque deux fois moins qu'en Allemagne (12 000 ETI, constitutives du *Mittelstand*) et qu'en Grande-Bretagne (10 000 ETI). Pour la filière industries de sécurité, on dénombre, en 2021, 91 ETI sur 4 400 entreprises dont 1 723 PME.

Objectif 2 – Faire émerger 5 à 10 nouveaux champions industriels français de la sécurité dans le monde d'ici 2026

La filière est déjà composée de leaders mondiaux sur les segments de la sécurité électronique (Thales, Airbus D&S), de la gestion des identités et des accès (Thales, Idemia, IN Groupe), des plateformes de sécurité (Naval Group, Airbus Helicopters, Dassault Aviation), des services de cybersécurité (Thales, Atos, Orange Cyberdefense, Capgemini, Sopra Steria), et de la sécurisation des paiements (Worldline). L'objectif est d'étoffer cette liste.

Objectif 3 – Renforcer l'excellence de la filière « industries de sécurité »

Faire progresser les 4 indicateurs suivants : chiffre d'affaires, chiffres d'affaires à l'export, part de marché à l'export, part de la filière française dans les achats de commande publique.

Les chantiers du nouveau contrat

Compétitivité et souveraineté. Projet structurant n°1

Renforcer la compétitivité des PME et ETI de la filière à fort potentiel en favorisant l'accès au financement et en renforçant l'accompagnement de leur croissance

Contexte

Les PME constituent une grande part de la filière « industries de sécurité ». Accompagner leur croissance et accroitre, par suite, la part d'ETI qui la compose constitue ainsi un enjeu pour la filière dans sa globalité, ainsi que pour le renforcement de sa capacité à innover et à créer des emplois à haute valeur ajoutée domiciliés en France.

Or, au sein de la filière, les PME sont souvent confrontées à un certain nombre de problématique, telles que :

- **le manque de financements.** Les PME éprouvent des difficultés à trouver les financements nécessaires à leur croissance. Si les levées de fonds sont en plein essor en France, dans le même temps, de nombreuses « pépites » françaises sont rachetées par des sociétés étrangères faute de financements français suffisants. Le développement d'une filière « industries de sécurité » puissante nécessite l'accès des PME et ETI en croissance aux financements ;
- **le manque de valorisation de leurs produits.** Les PME ont du mal à se positionner sur les marchés face à des concurrents plus importants en termes de taille et vers lesquels se tournent souvent les acheteurs-cibles par facilité ou par manque de visibilité quant aux produits proposés par les PME ;
- **le manque de relais auprès des acteurs publics.** Les acteurs industriels éprouvent des difficultés à identifier clairement un point d'entrée au sein des administrations, face à la multiplicité des dispositifs et actions ;
- **la difficulté à accéder aux données et aux conditions d'emploi réelles des solutions qu'elles développent** en raison de leur sensibilité.

Objectifs

Objectif 1 -- Stimuler la croissance des PME de la filière en facilitant leur accès à des financements de moyen terme et en les éclairant sur la diversité des dispositifs existants.

Pour éviter que des entreprises stratégiques ou à fort potentiel de croissance se retrouvent sous l'influence de capitaux étrangers, voire rachetées, il est nécessaire que les acteurs majeurs de la filière jouent un rôle actif en tant qu'investisseur[2], en particulier lors de la phase de « capital-développement » où les tickets sont souvent relativement importants.

[2] A noter l'existence de Défense Angels qui est le premier réseau d'investisseurs privés dédié au financement de start-up et de PME stratégiques.

Objectif 2 -- Accompagner le changement d'échelle des PME.

A ce titre : favoriser les coopérations entre PME/ETI, structurer et rationaliser les développements de façon à éviter le morcellement et le saupoudrage des efforts de recherche et développement sur des projets ou thèmes identiques.

Objectif 3 – Valoriser les PME de la filière et leurs produits dans les marchés publics.

Ce levier permettra de faire face à la concurrence accrue des grands groupes ou des géants étrangers, et ainsi éviter une fuite des compétences tout en maintenant une souveraineté de la filière.

Pilotage

Jérôme JOUANNO – SAFE,
William LECAT – AURIGA PARTNERS,
Dorothée DECROP – Hexatrust

Livrables attendus et calendrier prévisionnel

Objectif 1 : Stimuler la croissance des PME et des ETI de la filière en facilitant leur accès à des financements de moyen terme et en éclaircissant la multiplicité des dispositifs existants.	
Livrable 1	Organiser la production et le partage de données utiles aux PME de la filière « industries de sécurité » en matière d'aides et de dispositifs financiers existants et de structures d'accompagnement : proposition d'outils et de supports visant à mieux identifier les dispositifs et les démarches permettant d'accompagner les PME dans leur croissance.
Livrable 2	Favoriser la création d'un fonds d'investissement stratégique visant à pouvoir assurer (en fonds propres ou quasi-fonds propres) la phase « capital développement » (levées de fonds importantes supérieures à 50 millions d'euros) de PME/ETI à fort potentiel de croissance et innovantes.
Objectif 2 : Accompagner le changement d'échelle des PME.	
Livrable 3	Mettre en place un accélérateur[3] avec Bpifrance, co-construit par les acteurs de la filière, destiné à faciliter la croissance des PME prometteuses ayant vocation à devenir des entreprises de taille intermédiaire (ETI), leaders dans filière « industries de sécurité ».
Objectif 3 : Valoriser les PME de la filière et leurs produits dans les marchés publics, pour faire face à la concurrence accrue des grands groupes ou des géants étrangers.	
Livrable 4	Valoriser l'offre de solutions et de services des PME de la filière en communiquant sur les acteurs de la filière, notamment auprès des acteurs de la commande publique.
De façon transverse à ces quatre livrables, favoriser l'accès des PME (et autres acteurs pertinents de la filière) à des « bacs à sable » représentatifs des besoins réels, à fins d'expérimentation et de démonstration de performance.	

[3] Pour information, le GICAT a mis en place en 2017 l'accélérateur Generate qui soutient les star-ups de défense et de sécurité.

Livrables	Calendrier
Livrable 1	Premier semestre du contrat
Livrable 2	Tout au long de la période du CSF
Livrable 3	2025
Livrable 4	Tout au long de la période du CSF

Modalités d'évaluation du projet

- Création d'un accélérateur pour les PME de la filière « industries de sécurité » : l'accélérateur pourra être spécifique à la filière ou proposer un périmètre plus large en lien avec un ou plusieurs autres CSF ;
- Nombre de PME de la filière dont le dirigeant est entré dans un dispositif d'accélération et suivi sur un panel des indicateurs de transformation pour l'entreprise : croissance et emplois créés dans les PME accélérée, notamment.

Compétitivité et Souveraineté. Projet structurant n°2

Concevoir et valoriser au plan national et international des offres de solutions et de services de sécurité innovants et compétitifs sur les trois segments de la filière « industries de sécurité » (sécurité physique, sécurité électronique, cybersécurité) sur les marchés stratégiques suivants : *forces de sécurité intérieure et acteurs du continuum de sécurité (sécurité des frontières, innovation d'usage), collectivités territoriales, utilisateurs de l'identité numérique, grands évènements, PME, entités critiques*

Contexte

S'agissant **des forces de sécurité intérieure et des acteurs du continuum de sécurité**, les membres de la filière ont identifié les deux thématiques suivantes : la sécurité aux frontières, d'une part, et l'innovation d'usage d'autre part, ces deux thématiques étant jugées stratégiques en termes d'opportunités de marché.

En matière de **sécurité des frontières**, la filière souhaite centrer son action sur le développement des concepts de frontière fluides et de frontières intelligentes autour des deux thématiques suivantes :

- gérer les contrôles d'identité des voyageurs aux points de passage, le flux des voyageurs aux frontières terrestres et dans les aéroports ;
- appliquer et maintenir une surveillance des frontières françaises notamment maritimes, jusqu'à la zone économique exclusive (notamment lutte contre les trafics illicites, tel que le pillage des fonds marins et la pêche illicite. L'enjeu d'interopérabilité et de coopération entre la France et les pays frontaliers mais aussi entre les différentes forces de sécurité françaises est dimensionnant.

En matière de **« innovation d'usage »**, l'enjeu est de proposer des solutions dont l'innovation est partie intégrante, coconstruites avec l'ensemble des forces de sécurité dans une logique d'adaptation de la réponse au plus près des besoins et d'interopérabilité renforcée. Cette thématique prend en compte les trois segments de la filière (protection physique, protection électronique et cybersécurité) et pourra, le cas échéant, s'étendre à tous les acteurs du continuum de sécurité (polices municipales, services de sécurité de certains grands opérateurs, notamment).

Alors que **les collectivités territoriales** ont déjà fait l'objet d'une attention particulière dans le premier contrat stratégique de filière 2020-2022, elles demeurent un point d'attention majeur à plusieurs titres :

- le sujet de la protection des données a ainsi pris de l'ampleur au sein des collectivités, y compris les plus petites, au vu de la multiplication des contentieux suite aux fuites de données ;
- les expérimentations à venir dans le cadre de la loi JOP 2024 en matière de vidéo ayant recours à de l'intelligence artificielle pour la détection d'événements prédéterminés pourraient modifier profondément le cadre dans lequel les collectivités ont recours à la vidéoprotection ;
- les exigences de cybersécurité imposées aux collectivités territoriales seront prochainement significativement renforcées en application de la seconde directive sur la sécurité des réseaux et de l'information (NIS 2).

Le déploiement de **l'identité numérique** est essentiel pour permettre à chacun de prouver son identité à tout moment, dans son parcours digital mais aussi en toute circonstance de la vie courante requérant une identification électronique. L'identité numérique a également pour vocation d'apporter de la confiance à chaque utilisateur de services en ligne et de protéger les usagers comme les fournisseurs de services contre toute usurpation d'identité. Elle est donc au cœur de la souveraineté numérique, de la lutte contre la fraude et de la protection des données personnelles et de la vie privée, que ce soit dans les usages publics ou privés.

L'ambition des acteurs de la filière « industries de sécurité » est de contribuer à répondre à ces enjeux majeurs, en proposant des solutions de confiance permettant des parcours d'identification numérique simples, accessibles, sécurisés et respectueux du droit fondamental à la protection des données à caractère personnel.

S'agissant de la sécurité **des grands évènements**, la filière est engagée depuis 2018 dans la définition d'une offre française pour la sécurisation des JOP 2024. Un groupe mixte de travail a été créé, réunissant les industriels et les acteurs étatiques. Cinq grands groupes (Airbus, Atos/Eviden, Idemia, Orange, Thales) se sont ainsi organisés en consortium dans le cadre du CSF afin de coconstruire plusieurs livrables dans un esprit de solidarité, les grands groupes ayant charge d'embarquer les start-ups et PME de la filière. Ainsi, une proposition générale de sécurité (étude comparative et prospective des dispositifs mis en œuvre dans le cadre d'autres grands évènements) a été réalisée dès juillet 2019 et un programme d'expérimentation a, dans la continuité de cette démarche, été déployé par le ministère de l'intérieur autour de six grandes priorités (centre de commandement et hypervision, cybersécurité, vidéoprotection, frontières intelligentes, lutte anti drone, OSINT/Renseignement).

L'objectif est désormais, de bâtir, sur la base de cette expérience, un plan « export » pour la sécurisation des grands évènements internationaux, en lien avec la construction d'une architecture et d'une offre souveraine française.

S'agissant **des PME**, la place des systèmes d'information et technologies numériques est de plus en plus prépondérante dans leur fonctionnement. Dans le même temps, cette ultra-connexion et la dématérialisation des échanges représentent autant d'opportunités pour les cybercriminels. Or, les PME sont bien souvent plus démunies que les grandes entreprises face à la menace cyber en raison d'un manque de connaissances, de moyens ou encore de spécialistes en interne. Les conséquences sont d'autant plus importantes pour ces structures : 71% des PME ayant été sujettes à une cyberattaque ne s'en remettent pas et déposent le bilan dans les 3 ans[4].

L'environnement juridique, notamment européen, joue un rôle incitatif dans la montée en gamme des PME pour se protéger face à cette menace cyber grandissante. Il importe donc d'apporter aux PME des offres de solutions industrielles, packagées et simples à mettre en œuvre, nécessitant peu de compétences interne à l'entreprise, notamment pour celles qui seront concernées par la mise en œuvre de la seconde directive sur la sécurité des réseaux et de l'information (NIS 2).

La présence de dispositions dans les contrats commerciaux entre « donneur d'ordre » et « sous-traitants » imposant à ces derniers de démontrer un certain niveau de protection constitue un autre accélérateur pour les PME.

Le développement de la cyber assurance représente également un levier de renforcement de la protection des PME et représente un marché majeur pour les industriels de la cybersécurité tant en volume que d'un point de vue stratégique, le volume étant estimé à trois millions de PME.

[4] Idem

S'agissant de **la résilience des entités critiques**, cette thématique s'inscrit principalement dans le cadre de l'objectif « s'assurer de la protection des infrastructures et des informations les plus sensibles » de la stratégie nationale de résilience[5].
En effet, dans un contexte marqué par le retour des conflits de haute intensité, la persistance de la menace terroriste, l'émergence de nouveaux risques (hybrides, cyber) et des risques systémiques induits par les conséquences du changement climatique, une stratégie interministérielle – la stratégie nationale de résilience – a été validée par le cabinet de la Premier ministre en avril 2022, afin de mettre en cohérence l'ensemble des actions publiques, autour de trois objectifs principaux, déclinés en 73 actions, assorties d'indicateurs de suivi.

Négociée sous présidence française, et adoptée en décembre 2022, la directive européenne REC est une évolution majeure de la politique de l'Union européenne en matière de protection de ses infrastructures, qui devra être transposée d'ici à octobre 2024.

Les enjeux de souveraineté sont au cœur des solutions capacitaires qui peuvent être apportées notamment en matière de processus, de compétences, de capteurs et d'outils numérique par exemple pour le contrôle d'accès mais aussi pour les outils de planification froide ou chaude, de remontées d'incidents et de mitigation du risque.

Objectifs

Objectif 1 : Développer, au plan national, une offre de solutions et de services de sécurité innovants ciblées au profit notamment de marchés jugés stratégiques (sécurité des frontières, innovation d'usage pour les acteurs du continuum de sécurité, collectivités territoriales, utilisateurs de l'identité numérique, sécurisation des grands évènements, offre cyber PME, résilience des entités critiques)

Les objectifs selon les marchés ciblés se déclinent de la manière suivante :

Marché ciblé	Objectifs identifiés
Sécurité des frontières	• Développer l'axe « frontières intelligentes » par l'exploitation de solutions technologiques afin d'offrir aux forces en charge de la gestion et de la protection des frontières un gain opérationnel et humain autour du triptyque capacitaire « détecter, exploiter, agir ». • Contribuer au renforcement de la surveillance des frontières maritimes.
Innovations d'usage pour les acteurs du continuum de sécurité	• Placer les opérationnels de la sécurité, du secours, de la gestion de crise et les forces spéciales (policiers, gendarmes, douaniers, pompiers, GIGN, BRI, RAID) au cœur des préoccupations des industriels de sécurité, en favorisant un partenariat entre ces parties prenantes dès la phase de conception d'un produit ou d'un service de sécurité. • Identifier d'autres clients que les forces de sécurité pour ces solutions (éventuellement via les travaux sur l'export ou autres clients sectoriels).
Collectivités territoriales	• Intégrer davantage les collectivités territoriales dans les réflexions (via les associations d'élus notamment) afin de disposer d'une vision agrégée des besoins de celles-ci en matière de sécurité et de résilience des territoires. • Définir la nature des solutions en réponse à ces besoins RH (mobilisation du personnel) ou technologiques.

[5] 1. 20220315_NP_SGDSN_Document cadre_SNR_FR.pdf

Marché ciblé	Objectifs identifiés
	• Approfondir la création d'une plateforme numérique intégrant les solutions technologiques mobilisées afin d'assurer un pilotage sécurisé des différents services fournis et axée sur le renforcement de la résilience. • Assurer la cyber protection des collectivités locales dans la continuité de France Relance/ France 2030.
Utilisateurs de l'identité numérique	• Dynamiser l'écosystème national de l'identité numérique autour des usages, via les start-ups et PME notamment en capacité de générer des usages innovants, de l'e-wallet et des services de confiance associés.
Sécurisation des grands évènements	• Identifier les technologies critiques, c'est-à-dire des technologies présentant un risque de non-disponibilité et devant être détenues en souveraineté (cf. projet structurant n°5). • Elargir la cible des marchés publics à potentiel. • Permettre une réutilisation des solutions développées par la filière dans le cadre des Jeux Olympiques (JO) pour d'autres évènements, notamment à l'étranger. • Augmenter la part française dans les consortia porteurs de projets européens. • Continuer d'intégrer les différentes composantes de la filière, notamment les PME / Start-Ups / ETI.
PME – Avec un focus sur les besoins en matière de cybersécurité	• Répondre aux besoins et aux spécificités des PME en matière de cybersécurité. • Et plus globalement, contribuer à travers ce chantier ciblé sur les PME à développer une filière d'excellence.
Résilience des entités critiques	• Dans le cadre de la stratégie nationale entamer un travail sur trois chantiers principaux pour anticiper ces changements au profit de la filière : ○ identifier les solutions de sécurité pouvant répondre à ces nouveaux enjeux ; ○ parmi ces solutions, sélectionner les technologies critiques c'est-à-dire des technologies présentant un risque de non-disponibilité et devant être détenues en souveraineté (premier cercle national ou deuxième cercle au sein de l'UE) ; ○ mettre en place des actions d'influence au sein des institutions européennes et vis-à-vis des États-membres pour la promotion d'une vision française et la création de valeur pour la filière.

Objectif 2 : Diversifier et étendre, au plan international, les marchés de la filière « industries de sécurité », notamment pour ceux jugés stratégiques : sécurité des frontières, innovation d'usage, collectivités territoriales, établissements de santé, offre cyber PME, entités critiques.

Cet objectif pourra être atteint en agissant sur les facteurs suivants, en collaboration notamment avec Business France :

- avoir une meilleure connaissance des marchés étrangers et des moyens d'y pénétrer ;
- prioriser les zones géographiques / marché cibles à l'export ;
- avoir une meilleure connaissance des dispositifs de soutien à l'export ;
- développer la reconnaissance de la filière française auprès des marchés internationaux, notamment au travers d'une marque « Made in France » et de la valorisation d'évènements français, européens, internationaux phares ;
- assurer une coordination de la filière « industries de sécurité » notamment dans les réponses à des programmes complexes et multidisciplinaires.

Pilotage

Sécurité des frontières	Lionel LE CLEI – Thales Etienne LOTH – Soprasteria
Innovation d'usage pour les acteurs du continuum de sécurité	Laetitia BOURSE – AIRBUS Laurent DENIZOT – Egidium
Collectivités territoriales	Richard KALCZUGA – THALES Dominique LEGRAND AN2V
Utilisateurs de l'identité numérique	Yann HAGUET - IN GROUPE Christophe CIANCHI – BCA Smart Marie FIGARELLA – Thales
Grands évènements	Yannick RAGONNEAU – Vona Philippe LECLERC – SAFE
PME	Benjamin SERRE – ORANGE Michaël MONNEREAU - Qontrol
Résilience des entités critiques	Patrick GUYONNEAU – ORANGE Thierry DELVILLE – CAPGEMINI /CDSE
Volet international	Jean de la RICHERIE - Airbus / Séverine MEUNIER – Airbus Yannick RAGONNEAU – Vona Dorothée DECROP – Hexatrust

Livrables attendus et calendrier prévisionnel

Objectif 1 : Développer, au plan national, une offre de solutions et de services de sécurité innovants ciblés sur les marchés jugés stratégiques : sécurité des frontières, innovation d'usage, collectivités territoriales, utilisateurs de l'identité numérique, sécurisation des grands évènements, résilience des entités critiques.	
Livrable 1	Déterminer les besoins des marchés cibles identifiés par les acteurs de la filière « industries de sécurité ».
Livrable 2	Construire une offre innovante, compétitive et appropriée, combinant les trois grands segments : produits de sécurité physique, produits et services électroniques et numériques et produits et services de cybersécurité.
S'agissant des marchés cibles PME et collectivités territoriales, en particulier sur le volet « cyber », les travaux suivants ont été identifiés comme préalables pour remplir l'objectif 1 :	
Livrable 3	Décliner la taxonomie de l'ANSSI (parcours Cyber) suivant les marchés et usages des utilisateurs visés (NIS2, DORA…)
Livrable 4	Définir un référentiel commun pour évaluer la maturité cyber de certaines catégories d'acteurs (les PME, les établissements de santé et les collectivités territoriales) sur la base de la taxonomie unique de l'ANSSI, et fédérer les PME de la filière cybersécurité autour de son utilisation.

Objectif 2 : Diversifier et étendre, au plan international, les marchés de la filière « industries de sécurité », notamment pour ceux jugés stratégiques : sécurité des frontières, innovation d'usage, collectivités territoriales, utilisateurs de l'identité numérique, sécurisation des grands évènements, résilience des entités critiques.	
Livrable 5	Élaborer une feuille de route stratégique afin de structurer l'action et le développement des entreprises, en particulier des PME, à l'international.
Livrable 6	S'appuyer sur les évènements-clés dans le domaine des industries de sécurité.

Livrables	Calendrier
Livrable 1	2024 / 2026
Livrable 2	2024 / 2026
Livrable 3	Premier semestre du contrat
Livrable 4	Premier semestre du contrat
Livrable 5	Tout au long de la période du CSF
Livrable 6	Tout au long de la période du CSF

Engagements des industriels de la filière

Marché ciblé	Objectifs identifiés
Sécurité des frontières	• Faire en sorte que les grands groupes intègrent 40/50% des innovations des PME dans leurs solutions.
Innovations d'usage pour les acteurs du continuum de sécurité	• Faire en sorte que les grands groupes intègrent 40/50% des innovations des PME dans leurs solutions.
Collectivités territoriales	• Organiser une session annuelle pour mettre en lumière les travaux en y conviant les collectivités territoriales, les opérateurs et les fournisseurs de solution (cyber et fonctionnel). • Définir et mettre en œuvre un/des produits minimum viables pour tester avec les entités opérationnelles des collectivités, la pertinence d'une « plateforme digitale de sécurité territoriale » pour de nouveaux services et une résilience accrue selon le schéma directeur du SGDSN. • Mesurer les gains opérationnels et les économies d'échelle.
Utilisateurs de l'identité numérique	
Sécurisation des grands évènements	• Développer des solutions compatibles avec les libertés publiques et individuelles et acceptables par les citoyens. • Financer des plans d'étude, d'accompagnement et d'expertise entre 2023 et 2026, avec un budget compris entre 2 et 5 millions d'euros. • Maintenir les 70 000 emplois français et en créer de nouveaux. • Mettre en place une plateforme de démonstration et de preuve de concept au profit des opérateurs publics et privés.

Marché ciblé	Objectifs identifiés
	• Définir une architecture de référence dans différents domaines technologiques tels que la cybersécurité, les centres de commandement, la vidéoprotection, l'audio protection, la lutte anti-drone, le renseignement en sources ouvertes, la cybercriminalité, la gestion des flux et des foules, la menace nucléaire, radiologique, biologique, chimique et explosifs (NRBC-E), le contrôle aérien en basse altitude et la surveillance aéroportée des sites et de leurs abords.
PME – Avec un focus sur les besoins en matière de cybersécurité	• Mener un travail avec les assurances pour qu'elles aient un effet incitatif sur les PME (cf. les travaux en cours par le Ministère de l'économie, des finances et de la souveraineté industrielle et numérique avec les assurances pour contribuer à élaborer un référentiel commun aux assurances). • Suivre l'AMI Cyber PME (à venir) et mettre en œuvre la mission PME confiée au Campus Cyber.
Résilience des entités critiques	

Engagements des industriels de la filière sur le volet international :

- partager les opportunités et les évènements identifiés à l'ensemble de la filière ;
- participer à des évènements valorisant l'offre française à l'export ;
- faire en sorte que les grands groupes de la filière incorporent les PME françaises en cas de positionnement sur un marché à l'international ;
- constituer une équipe France pour valoriser l'excellence de la filière dans toute sa diversité (PME, start-ups, ETI, grands groupes) ;
- intégrer systématiquement plus de PME dans les délégations à l'étranger ;
- se fédérer pour une feuille de route stratégique commune à l'internationale ;
- assurer une participation sur plusieurs années aux évènements stratégiques, afin d'en faire des évènements de rayonnement à l'international et de promotion de la filière française ;
- davantage capitaliser sur les actions déjà menées (invitations de délégations, coopérations initiées etc.).

Modalités d'évaluation du projet :

- part significative de sociétés françaises dans les plans d'acquisition ;
- part de star-ups, PME et ETI dans les plans d'acquisition ;
- chiffre d'affaires des projets signés dans le cadre de contrat étatique ;
- chiffre d'affaires des projets signés avec les collectivités territoriales ;
- chiffre d'affaires des projets signés dans le cadre des entités critiques.

Compétitivité et Souveraineté. Projet structurant n°3

Accompagner les établissements de santé dans leur sécurisation, y compris celle de leurs systèmes d'information, dans la digitalisation du parcours santé et dans l'acquisition de dispositifs médicaux à forte composante numérique et de connectivité, y compris en partenariat avec le CSF Santé.

Contexte

Comme tous les secteurs, **la santé** connait aujourd'hui un formidable essor du numérique, qu'il s'agisse des soins, de la gestion administrative ou des usages importés par les patients. Tout au long du parcours de soins, la donnée de santé est partout : au cabinet, comme à l'hôpital ou à la maison - une omniprésence qui s'est accrue avec la crise sanitaire.

Les cyber-risques sont à l'image de cet essor : ils augmentent. Et les établissements de santé y sont d'autant plus vulnérables qu'ils sont chaque jour particulièrement sollicités et sous tension. Stratégiques pour le pays, inégalement matures face au numérique et source exponentielle de données personnelles, ils constituent une cible privilégiée pour les attaques malveillantes, avec un impact d'autant plus fort que la santé et la vie des patients sont en jeu. Une cyberattaque peut en effet non seulement perturber le quotidien des professionnels, mais aussi mettre en péril la prise en charge des patients : systèmes biomédicaux paralysés ; plateaux techniques indisponibles ; données de programmation des soins détruites ; systèmes de messageries en panne ; données de gestion et de ressources humaines perdues ; données personnelles de santé usurpées.

La cybersécurité est indispensable pour transformer notre système de santé en toute confiance[6]. Lutter contre les déserts médicaux, décloisonner les parcours de soins, désengorger l'hôpital, faciliter la prévention, proposer une nouvelle offre de services ou accélérer la médecine personnalisée. Ces avancées ne pourront se développer que si notre système de santé est capable d'élever le niveau de résilience et de sécurité de ses données et de ses échanges.

Le volet numérique du « Ségur de la Santé » comprend la cybersécurité dans ses priorités dotées de financement. Il s'inscrit dans une démarche plus large « task force 2023 », à laquelle l'ANSSI est partie prenante. Dans le prolongement de la feuille de route du numérique en santé, 2Mds€, dont 600M€ dédiés au médico-social, ont été accordés pour soutenir le développement massif et cohérent du numérique en santé en France.

Le développement d'une offre de solutions industrielles visant spécifiquement ce secteur est impératif compte tenu des particularités de ce type d'établissement, tant au niveau de leurs structures que de leurs enjeux.

La filière « industrie de santé » dans sa composante numérique[7] est un secteur d'avenir, l'actualité nous le démontre chaque jour. La numérisation du système de santé français doit permettre l'émergence d'une médecine plus personnalisée, plus sécurisée, faisant la part belle à la prévention et à l'anticipation des pathologies, pour concourir à une meilleure prise en charge des patients.

La santé numérique fait partie des priorités du plan France 2030 et bénéficie à ce titre d'un soutien financier de plus de 650M€.

[6] « Cybersécurité dans le secteur de la santé et du médico-social : une priorité nationale pour réussir la transformation numérique » - Agence du Numérique en Santé (Mai 2021)
[7] Stratégie d'accélération « santé numérique » - dossier de presse du 18 octobre 2021

Les enjeux numériques pour la filière santé sont de faciliter l'accès aux données de santé, de développer la confiance numérique en santé et la lisibilité de l'accès au marché, ainsi que de soutenir plus largement le développement d'innovations dans ce secteur.

La France a déjà lancé grâce au « Ségur de la santé » un important chantier de rattrapage de ses infrastructures en matière de sécurité, d'interopérabilité et d'éthique permettant, à terme, une meilleure circulation des données de santé.

→ *Les chiffres-clés du numérique en santé*[8]

- 18,4M de téléconsultations réalisées au total en 2020 contre 140.000 en 20191 ;
- 350 000 applications mobiles de santé, dont 90 000 nouvelles applications en 2020, ont été ajoutées dans le monde sur les stores d'applications ;
- doublement du volume des données de santé hospitalière tous les 73 jours.

Cette digitalisation du système de santé français génère également de grandes vulnérabilités, identifiée par l'ANSSI, compte tenu notamment de l'accroissement des équipements médicaux contenant des objets connectés.

La filière des industries de sécurité dans toutes ses composantes, et éventuellement en coopération avec d'autres CSF (futur CSF numérique de confiance), pourrait ainsi traiter de la **sécurisation de la transition numérique de l'hôpital et plus généralement de la filière de la santé et du médico-social.**

En particulier, l'utilisation de la carte vitale repose sur une vérification d'identité faible, que ce soit en face à face ou en ligne, en découle deux enjeux : permettre à tous les résidents sur le territoire national une identification à distance fiable et contrer les possibilités de fraudes.

Au-delà, le partage d'information sur un patient entre praticiens est très peu automatisé et numérisé, en n'est possible qu'avec le consentement et contrôle du patient. Il convient de trouver des solutions sécuriser qui permettre de répondre à ces exigences.

Enfin, de nombreuses données sur les pathologies pourraient être exploitées à des fins de recherche si elles étaient disponibles de manière numérisés, catégorisées (âge, sexe, etc.) sous réserve bien entendu de leur anonymisation.

Objectifs :

- développer une offre française complète et compétitive pour la sécurisation des établissements de santé y compris celle de leurs systèmes d'information (à court terme) ;
- conduire une analyse prospective des enjeux du système de santé en matière de sécurité physique (à moyen terme).

S'agissant du partenariat avec le CSF Santé :

- mettre en place une concertation avec la filière industrielle santé (dispositifs médicaux) en vue de bâtir une offre française conjointe pour certains dispositifs médicaux à forte composante numérique et de connectivité. ;
- sécuriser la digitalisation de l'hôpital et de la filière de la santé.

[8] Stratégie d'accélération « santé numérique » - dossier de presse du 18 octobre 2021

Pilotage

Jean-Noël de GALZAIN – WALLIX,
Patrick GUYONNEAU – Orange,

Livrables attendus et calendrier prévisionnel :

Livrable 1	Identifier les besoins des établissements de santé, notamment sur la base de l'établissement de profils-type en fonction de leur niveau de maturité cyber.
Livrable 2	Mettre en place les actions nécessaires à la construction d'une offre française regroupant l'intégralité des produits et services « cyber », susceptible de répondre aux besoins des profils-type identifiés lors du livrable 1 et aux besoins du « Ségur de la santé ».
En partenariat avec le CSF Santé	
Livrable 3	Mettre en place une concertation avec la filière « industrie de santé » (dispositifs médicaux) en vue bâtir une offre française conjointe pour certains dispositifs médicaux à forte composante numérique et de connectivité.
Livrable 4	Sécuriser la digitalisation de l'hôpital et de la filière de la santé, notamment via des solutions d'identité numérique.

Engagements des industriels de la filière :

- fédérer l'industrie française autour d'un consortium le plus à même de porter une offre pour le système de santé ;
- concevoir une offre française embrassant toute la chaîne de valeur, répondant aux besoins identifiés, intégrant les meilleures solutions d'origine française et ayant la capacité de passage à l'échelle ;
- réaliser un catalogue des offres spécifiques « Santé » ;
- collaborer avec l'UGAP pour simplifier les modes d'achat pour les hôpitaux ;
- apporter une réponse en provenance de la filière « industrie de santé » en soutenant le déploiement de produits et solutions française et européenne.

Modalités d'évaluation du projet :

- avoir établi 3 ou 4 profils-types d'hôpitaux ;
- faire émerger des offres simples et packagées qui répondent aux besoins des hôpitaux pour chacun des profils, et également applicable aux PME ;
- avoir équipé au minimum 3 hôpitaux-pilotes de l'offre de sécurité nouvellement créée.

Compétitivité et Souveraineté. Projet structurant n°4

Utiliser la normalisation et la certification pour développer les avantages comparatifs de la filière à l'international

Contexte

A ce jour, il est constaté une défaillance dans la présence des acteurs industriels de la filière dans les groupes de travail en charge de l'élaboration des normes. Les domaines de la cybersécurité et de l'identité numérique constituent, notamment, des points d'excellence française et européenne, qui doivent être confortés par une présence renforcée dans les instances de normalisation de ces domaines.

Les acteurs français de la normalisation se trouvent en concurrence avec les modèles allemand, britannique, et américain qui grâce à leur puissance commerciale peuvent imposer leurs normes. Par ailleurs, la certification est aujourd'hui un instrument incontournable pour aider les entreprises, citoyens et administrations à identifier les organisations et les services les plus fiables en termes de sécurité, dans une offre pléthorique et pour aider les professionnels à pénétrer des marchés réglementés ou à se démarquer de la concurrence. Ainsi, à titre d'exemple, l'adoption du Cybersecurity Act en 2019 a marqué une étape majeure dans la construction d'un marché unique de la confiance numérique : outre l'attribution d'un mandat permanent à l'agence européenne pour la cybersécurité (Enisa), ce règlement institue un cadre européen de certification de la cybersécurité, pour les produits, procédures et services.

Objectifs

Objectif 1 -- Élaborer un cadre stratégique afin d'organiser la présence des acteurs de la filière « industries de sécurité » dans les instances et groupes de travail en matière de normalisation et d'évaluation de la conformité en lien avec les sujets de sécurité.

Objectif 2 – Renforcer, en conséquence, la présence des experts français de la filière « industries de sécurité » au sein des organismes nationaux, européens et internationaux de normalisation et de certification en lien avec les sujets de sécurité. En particulier, privilégier les organismes européens tout en se coordonnant avec les développements conduits au niveau de l'ISO/IEC/ITU.

Pilotage

Jean-Pierre QUEMARD – ACN/KAT,
Roland ATOUI – Red Alert Labs

Livrables attendus et calendrier prévisionnel

Objectif 1 : Élaborer un cadre stratégique pour organiser la présence française dans les instances et groupes de travail en matière de normalisation et d'évaluation de la conformité en lien avec les sujets de sécurité.	
Livrable 1	Établir une stratégie d'influence pour les cas d'usage pour lesquels des travaux normatifs sont à prévoir et sont jugés stratégiques, afin de renforcer la participation des industriels du CSF-IS (identité numérique, internet des objets, IA, etc.).

Objectif 2 : Renforcer la présence des experts français de la filière « industries de sécurité » au sein des organismes nationaux, européens et internationaux de normalisation et de certification en lien avec les sujets de sécurité.	
Livrable 2	Déployer des actions de sensibilisation et de communication à destination des industriels de la filière sur l'intérêt de s'investir sur les sujets de normalisation et de certification, et sur les sujets particuliers jugés prioritaires pour lesquels leur mobilisation serait stratégique.

Livrables	Calendrier
Livrable 1	Dès la signature du CSF – Premier semestre du contrat
Livrable 2	Dès la signature du CSF – et tout au long de la période du CSF

Engagements des industriels de la filière :

- associer à chaque expert senior impliqué dans un groupe de normalisation un expert junior afin d'assurer une transmission des savoir ;
- participer activement aux actions de sensibilisation et de communication qui seront déployées, à destination des industriels de la filière, sur l'intérêt de s'investir sur les sujets de normalisation et de certification au niveau international et sur les sujets jugés prioritaires pour lesquels leur mobilisation serait stratégique.

Modalités d'évaluation du projet :

- présence des acteurs de la filière au sein des organismes nationaux et internationaux de normalisation en lien avec les sujets de sécurité : doubler le nombre d'experts français.

Maîtrise des technologies et innovation. Projet structurant n°5

Élaborer une feuille de route technologique en vue d'assurer la maîtrise des technologies-clés d'avenir et des technologies critiques

Contexte :

Deux catégories de technologies sont à distinguer et doivent être clairement identifiées par la filière afin de faire l'objet de plans d'actions adaptés :

- les technologies-clés d'avenir, dont les technologies émergentes ;
- les technologies critiques au sens de la « sécurité nationale ».

Pour la filière « industries de sécurité », préparer l'avenir est essentiel car les usages, les menaces et les risques évoluent constamment. Disposer des savoirs et des **technologies-clés** est indispensable pour garantir la durabilité de la filière industrielle, en lui permettant de s'adapter, voire de se réinventer, en réponse aux nouveaux défis (par exemple : l'ordinateur quantique, les attaques à base d'intelligence artificielle, la sobriété énergétique, les lois extraterritoriales, les enquêtes dans un monde où humains, comme objets, sont connectés, etc.).

Cela nécessite :

- une recherche d'excellence pour ouvrir de nouvelles voies de rupture ;
- une réelle capacité de transfert pour accélérer l'innovation de la filière dans un secteur mondialisé et ultra-compétitif ;
- des interactions fortes entre la recherche et l'industrie pour dialoguer et converger sur les enjeux, les nouveaux risques et les défis scientifiques et technologiques à résoudre.

De nombreux catalogues édités par les structures associatives existent pour promouvoir les briques technologiques de leurs adhérents. Le principal défaut de ces catalogues est qu'ils ne sont pas facilement accessibles, et rarement mis à jour. De plus, aucune notion de performance, ni de comparaison entre les systèmes existants n'est disponible. Cela s'apparente plutôt à des catalogues commerciaux réalisés à l'occasion d'un salon.

Selon la méthodologie retenue lors des travaux réalisés par le comité de filière en 2017, **une technologie critique** peut être définie comme :

- une technologie actuelle essentielle pour la mise en œuvre de missions fondamentales et sensibles de sécurité sur lesquelles pèsent des risques de maîtrise (nombre de fournisseurs très restreints, voire unique, rentabilité insuffisante, risque de prise de contrôle capitalistique, perte de savoir-faire, absence de technologies alternatives ou de contournement possible, etc.) ;
- la définition prise ici pour le terme « technologie » est extensive : il peut s'agir, selon les cas, de composants, de procédés, de sous-systèmes, voire de systèmes entiers, de compétences académiques, etc. L'exercice n'est pas conduit avec une granularité spécifiée mais s'adapte en fonction des sujets aux propositions argumentées.

Il est proposé de travailler sur ces technologies au profit notamment des entités critiques, c'est-à-dire des entités qui fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, la santé et la sécurité publiques, ainsi que l'environnement. Elles doivent être en mesure de prévenir les attaques hybrides, les catastrophes naturelles, les menaces terroristes et les urgences de santé publique, ainsi que de s'en protéger, d'y réagir, d'y faire face et de s'en remettre.

Au plan européen, la directive « résilience des entités critiques » (REC), adoptée en décembre 2022, a pour objectif de réduire les vulnérabilités et de renforcer la résilience des entités critiques présentes dans les États-membres de l'Union européenne.

La directive « REC » prévoit que les États-membres disposent d'une stratégie nationale pour renforcer la résilience des entités critiques, procèdent à une évaluation des risques au moins tous les quatre ans et recensent les entités critiques qui fournissent des services essentiels. Les entités critiques devront détecter les risques pertinents susceptibles de perturber considérablement la fourniture des services essentiels, prendre des mesures appropriées pour assurer leur résilience et notifier les incidents perturbateurs aux autorités compétentes.

La mise en œuvre de la stratégie nationale de résilience, ainsi que la directive « REC » vont nécessiter la mise en place, aux plans national et européen, de nouvelles organisations, de nouveaux outils et de solutions industrielles de sécurité dotés de technologies, parmi lesquelles figurent des technologies dites critiques à identifier.

S'agissant des technologies-clés, il s'agira de constituer un outil d'aide à la décision afin, d'une part, d'élaborer des projets de recherche, développement et innovation associant intégrateurs, acteurs de la recherche, développement et innovation et des PME de la filière susceptibles de souscrire à des cofinancements publics nationaux (France 2030 notamment) et européens et, d'autre part, de conduire des expérimentations.

S'agissant des technologies critiques, la feuille de route stratégique doit constituer un outil d'aide à la décision pour identifier et « sécuriser » les technologies, avec un focus sur les technologies émergentes, jugées stratégiques en termes de sécurité nationale et sur lesquelles pèsent des risques de perte de maitrise au plan national mais aussi européen. Elle doit également permettre d'identifier les forces et faiblesses des solutions françaises, notamment en vue d'un soutien/protection par les pouvoirs publics..

Pilotage

Alexandre HERVIN – SYSTEMATIC,
Jean-Yves GUEDON – IDEMIA,
Bruno CHARRAT – CEA

Livrables attendus et calendrier prévisionnel

S'agissant des technologies-clés	
Livrable 1	Identifier les technologies et solutions clés, d'avenir, innovantes dans les trois domaines de la sécurité physique, des produits électroniques et numériques de sécurité et de la cybersécurité afin d'être en mesure de proposer une offre souveraine.
Livrable 2	Identifier l'évolution des nouveaux besoins technologiques de la filière, qui pourraient être transverses aux trois segments de la filière (sécurité physique, sécurité des produits électroniques et numériques de sécurité et cybersécurité) ; (cf. investigation policière au travers des objets domestiques etc.) et identifier ainsi comment la filière pourrait se positionner sur les technologies-clés repérées.
S'agissant des technologies critiques	
Livrable 4	Constituer la liste des technologies critiques à porter aux plans national et européen.

Livrable 5	Mettre en place des actions d'influence pour promouvoir la diffusion d'une vision française des technologies-critiques et créer ainsi de la valeur pour la filière.
Livrable 6	Conduire une étude permettant d'obtenir une vision des enjeux technologiques consolidés de la filière.

Livrables	Calendrier
Livrable 1	Premier semestre du contrat
Livrable 2	Premier semestre du contrat
Livrable 3	Premier semestre du contrat
Livrable 4	Premier semestre du contrat
Livrable 5	Tout au long de la période du CSF
Livrable 6	Tout au long de la période du CSF

Engagements des industriels de la filière :

- participer aux réunions d'information organisées par la Commission européenne en amont du lancement des appels à projets (AAP) pour les programmes HORIZON EUROPE, DIGITAL EUROPE, etc. ;
- entrer en relation avec les acteurs publics et privés – en particulier ceux présents au CSF – familiers des consortia, de la réponse aux AAP et de la conduite de projets collaboratifs européens, et disposant d'un taux de succès important ;
- promouvoir les pôles de compétitivité comme acteurs pouvant aider à la création de consortium, à l'accompagnement aux projets, à la labellisation.

Modalités d'évaluation du projet :

- évolution du nombre d'industriels français dans les projets européens ;
- évolution du nombre de solutions françaises certifiées aux niveaux européen et américain.

Développement des compétences et de l'attractivité de l'industrie. Projet structurant n° 6

Renforcer l'attractivité des emplois et anticiper et répondre aux besoins en compétences de la filière

Contexte

→ *Attractivité de la filière*

Les métiers et les carrières associées à la filière font l'objet de stéréotypes souvent renforcés par le manque de visibilité et une méconnaissance du secteur de la part du grand public. Il importe ainsi que la filière travaille tant auprès des différentes strates de l'enseignement (secondaire, supérieur) que des entreprises, pour faire connaître et valoriser la diversité des métiers de la filière, en portant une attention particulière aux publics féminins.

→ *Compétences*

Les enjeux de développement de la formation et des compétences de la filière nécessitent et vont nécessiter, à terme, une bonne maîtrise de l'évolution des besoins en compétences pour garantir un positionnement compétitif de la filière.

Il convient donc d'anticiper les besoins et d'adapter les formations en conséquence tout en attirant de nouveaux publics vers les métiers du secteur.

Afin de répondre aux enjeux en termes de compétence, formation et attractivité identifiés par la filière « industries de sécurité », il est proposé que celle-ci s'engage dans la mise en place d'un accord « engagement développement de l'emploi et des compétences » (EDEC) avec la direction générale à l'emploi et à la formation professionnelle (DGEFP).

Un EDEC pour la filière pourrait constituer le cadre technique et financier pertinent pour répondre aux 5 objectifs identifiés par les acteurs de la filière « industrie de sécurité ».

Objectifs :

- **faire connaître les métiers** de la filière auprès des différentes strates de l'enseignement (secondaire, supérieur), des entreprises et des personnes en recherche d'emploi, reconversion et réinsertion. Il y a en effet un véritable enjeu de clarification et de centralisation des informations (cursus, écoles, métiers etc.) ;
- **promouvoir les carrières de la filière** et attirer de nouveaux talents ;
- **analyser et anticiper les besoins en ressources** sur les différents segments de la filière ;
- l**ancer une réflexion** sur la reconversion professionnelle et les potentielles passerelles entre les différents métiers de la filière ;
- **féminiser** la filière « industries de sécurité ».

Pilotage

Edouard JEANSON – CAPGEMINI,
Lilian EUDIER – GICAT

Livrables attendus et calendrier prévisionnel

Livrable 1	Développer une boite à outil permettant d'anticiper et préparer l'évolution des emplois et des qualifications.
Livrable 2	Accompagner les dirigeants d'entreprise de la filière dans la gestion et l'évolution des emplois et des compétences de leurs ressources humaines.
Livrable 3	Porter des actions de communication et de sensibilisation afin de faire connaître et valoriser les métiers et les carrières de la filière.

Livrables	Calendrier
Livrable 1	Dès la signature du CSF
Livrable 2	Premier semestre du contrat – et tout au long de la période du CSF
Livrable 3	Tout au long de la période du CSF

Engagements des industriels de la filière :

- identifier un référent pour participer au groupe de travail « compétences et attractivités des métiers de l'industrie », dans le cadre du conseil national de l'industrie, dont l'objectif est de permettre aux acteurs de « disposer d'un lieu de partage d'information, de mutualisation des bonnes pratiques, d'échanges entre les filières et les pouvoirs publics, de mise en cohérence des travaux existants et futurs et d'élaboration de propositions concrètes des filières à destination des pouvoirs publics ».
- élaborer une charte d'engagements des industriels membres du CSF-IS sur la féminisation des métiers.

Transition écologique. Projet structurant n° 7

Engager la transition écologique de la filière « industries de sécurité » vers une production décarbonée et réduite en impact énergétique

Contexte

Les enjeux de transition environnementale et de sécurité peuvent être complémentaires ou divergents :

- complémentaires lorsque l'amélioration de la cybersécurité permet d'éviter des coûts de remédiation importants tant auprès des usagers que de l'entreprise attaquée ou de la société dans son ensemble ;
- divergents lorsque l'arbitrage implique une préférence qui se fait au détriment de l'un des deux.

A l'heure où l'ensemble de l'économie doit s'engager pour réduire son empreinte environnementale, la filière a souhaité dédier un projet structurant à cet enjeu.

Objectifs

En cohérence avec les orientations et axes définis dans la feuille de route 2023 élaborée par le conseil national de l'industrie, la filière compte :

- être force de proposition et d'incitation pour contribuer au processus de décarbonation de l'industrie et de sobriété énergétique soutenu par le Gouvernement ;
- être porteuse de solutions pour accélérer la transition, en tant qu'industrie vecteur de décarbonation. Par exemple, le développement du recours au réemploi ne peut pas se faire sans prise en compte des enjeux de sécurité : comment faire en sorte que les produits issus de l'économie circulaire ne soient pas source de faille de sécurité ?

Pilotage

Chantal DROULEZ - Awacloud

Livrables attendus et calendrier prévisionnel

Livrable 1	Traduire les enjeux de transition écologique pour la filière « industries de sécurité ».
Livrable 2	Rédiger une feuille de route du code écologique appliqué aux produits de la filière « industries de sécurité », qui pourrait être, dans un premier temps, circonscrite à certains produits prioritaires.
Livrable 3	Élaborer un livre blanc identifiant les axes d'éco-responsabilité dans l'architecture globale des produits de la filière « industries de sécurité » (modularité des services proposés, sobriété énergétique, etc.).

Livrables	Calendrier
Livrable 1	Premier semestre du contrat
Livrable 2	Premier semestre du contrat
Livrable 3	2024 / 2025

Les engagements de l'État

Engagement transverse à l'ensemble du contrat	Renforcer le dialogue et la concertation entre l'État et les acteurs de la filière « industries de sécurité » via l'identification d'un interlocuteur étatique par administration concernée qui servira d'interface avec la filière et, par la mise en place d'échanges réguliers entre les deux parties prenantes. Cet engagement implique d'associer lorsque cela est pertinent les représentants des opérateurs d'importance vitale avec lesquels l'État a un lien particulier.

	Projets structurants	Sous-projet	Engagements de l'État
Compétitivité et Souveraineté	**Projet structurant n°1 : Renforcer la compétitivité des PME et ETI de la filière à fort potentiel en favorisant l'accès au financement et en renforçant l'accompagnement de leur croissance**		• Faire bénéficier la filière des industries de sécurité, des possibilités de financements de structures d'accompagnement type « accélérateurs » et « incubateurs » Bpifrance. Cet engagement ne dispense pas la filière de l'obligation de remplir les conditions de prérequis pour la mise en œuvre de ces financements. • Poursuivre les travaux pour la mise en œuvre d'un cadre favorable pour les PME dans les marchés publics.
	Projet structurant n°2 : **Concevoir et valoriser au plan national et international des offres de solutions et de services de sécurité innovants et compétitifs sur les trois segments de la filière « industries de sécurité » (sécurité physique, sécurité électronique, cybersécurité) sur les marchés stratégiques suivants : forces de sécurité intérieure et acteurs du continuum de sécurité (sécurité des frontières, innovation d'usage), collectivités territoriales, utilisateurs de l'identité numérique, grands évènements, PME, entités critiques**	**Marché cible 1 :** **Sécurité des frontières**	• Analyser les verrous, en particulier juridiques, au développement de solutions de sécurité innovantes et souveraines au profit des forces de sécurité intérieures ; en déduire les évolutions souhaitables dans le respect des exigences éthiques.
		Marché cible 2 : **Innovation d'usage**	• Favoriser une remontée concertée des besoins des forces de sécurité en solutions nouvelles.
		Marché cible 3 : **Collectivités territoriales**	• Poursuivre et renforcer les travaux permettant d'améliorer le cadre de la commande publique, en particulier analyser l'opportunité d'inscrire le mécanisme de licences mutualisées pour les collectivités territoriales à l'échelle nationale. • Inscrire les travaux de la filière dans le volet « collectivités territoriales » de la stratégie nationale de résilience du Gouvernement.

	Projets structurants	Sous-projet	Engagements de l'État
		Marché cible 4 : **« Sécurisation des grands évènements »**	• Partager l'information sur les opportunités pour la filière « industries de sécurité », notamment s'agissant des programmes de financement (nationaux ou européens), les appels à projets, les évènements. • Mobiliser les organisations impliquées autour de la sécurité des grands évènements (État, collectivités territoriales, OIV, organisateurs). • Capitaliser sur le programme de sécurité des grands événements et des Jeux Olympiques 2024, ainsi que sur le plan d'expérimentation porté par le CSF-IS. • Poursuivre la modernisation des moyens actuels de la sécurité publique.
		Marché cible 5 : **PME avec un focus sur les besoins en matière de cyber**	• Mettre en œuvre des dispositifs permettant d'accompagner la montée en compétence de l'ensemble de l'économie, et en particulier des TPE et PME, sur les enjeux « cyber ». • Faciliter la mise en relation avec les dirigeants de PME clientes. • Participer activement à la construction du référentiel unique des menaces et des faiblesses et à la définition de la taxonomie unique souhaitée par la filière cyber.
		Marché cible 6 : **cas d'usage de l'identité numérique**	• Renforcer le dialogue entre État et industriels et clarifier la doctrine de l'État en matière d'identité numérique.
		Marché cible 7 : **résilience des entités critiques**	• Élaborer un support pour bien expliciter le contenu de la directive « REC » afin de permettre aux industriels de bien appréhender les opportunités en matière de solutions. • Élaborer un support pour promouvoir l'offre de la filière au niveau européen.

	Projets structurants	Sous-projet	Engagements de l'État
Compétitivité et Souveraineté / partenariat inter - CSF	**Projet structurant n°3 :** **Accompagner les établissements de santé dans leur sécurisation, y compris celle de leurs systèmes d'information, dans la digitalisation du parcours santé et dans l'acquisition de dispositifs médicaux à forte composante numérique et de connectivité, y compris en partenariat avec le CSF Santé**		• Contribuer au travail d'identification des profils-types « d'établissements de santé ». • Poursuivre l'approche gagnant-gagnant en définissant une stratégie au niveau national de passage à l'échelle à l'ensemble des établissements de santé. • Poursuivre et renforcer les travaux permettant d'améliorer en lisibilité et en homogénéité, le cadre de la commande publique, en particulier sur le « volet sécurité ». • Considérer les travaux du CSF dans les orientations stratégiques des dispositifs de financement existants ou à venir qui seraient pertinents au regard de leur périmètre. • Conduire une réflexion pour un financement de l'investissement des hôpitaux dans la durée.
Compétitivité et souveraineté	**Projet structurant n°4 :** **Utiliser la normalisation et la certification pour développer les avantages comparatifs de la filière à l'international**		• Renforcer la concertation des services de l'État sur les besoins en normalisation concernant le périmètre des industries de sécurité.
Innovation et technologies-clés	**Projet structurant n°5 :** **Élaborer une feuille de route technologique en vue d'assurer la maîtrise des technologies-clés d'avenir et des technologies critiques.**		• Porter, au niveau national et européen, la liste des technologies critiques identifiées notamment pour les solutions françaises répondant aux exigences de la directive « REC ». • Prendre en compte les livrables des feuilles de route « technologies émergentes » dans les programmes d'investissement actuels et à venir.
Compétences et attractivité	**Projet structurant n° 6 :** **Renforcer l'attractivité des emplois et anticiper et répondre aux besoins en compétences de la filière**		• Renforcer les dispositifs permettant de favoriser les reconversions professionnelles et les compétences. • Accompagner la promotion des métiers et des carrières de la filière, y compris auprès du public éducation nationale. • Mettre en place des formations à la cybersécurité pour les enseignants.

	Projets structurants	Sous-projet	Engagements de l'État
			• Poursuivre le renforcement de la prise en compte des enjeux de sécurité dans les formations déjà existantes relevant d'autres domaines que l'informatique et l'ingénierie, et plus largement les formations concernées par l'internet des objets. • Mettre en œuvre des actions permettant de renforcer la prise en compte du risque « cyber » par le grand public.
Transition écologique	**Projet structurant n°7 :** **Engager la transition écologique de la filière « industries de sécurité » vers une production décarbonée et réduite en impact énergétique**		• Mettre en œuvre des dispositifs d'accompagnement de la filière dans sa transition écologique.

Les signataires

Ministre auprès du Ministre d'Etat, Ministre de l'Intérieur
François-Noël Buffet

Ministre chargé de l'Industrie et de l'Énergie
Marc Ferracci

Ministre déléguée chargée de l'Intelligence artificielle
et du Numérique
Clara Chappaz

Président du CSF
Marc Darmon

Organismes Paritaires
CFDT
Rémy Raymondo

Conception : Direction générale des Entreprises
Réalisation graphique : Sircom
Mars 2025