Contrat Stratégique de la Filière

Industries de sécurité

2020/2022

29 janvier 2020

Marc Darmon, Président du CSF Industries de sécurité
Directeur Général Adjoint de Thales, Président du CICS

Éditorial

Le Conseil National de l'Industrie a créé le 22/11/2018 le Comité Stratégique de Filière « Industries de sécurité », cette filière rejoignant ainsi pour la première fois cette instance.

L'industrie française de sécurité est une industrie d'excellence qui réalise 28 Md€ de chiffre d'affaire, majoritairement à l'exportation. Elle est très technologique et représente 130 000 emplois très qualifiés. Elle regroupe des grands leaders mondiaux dans leurs domaines, un tissu dense d'ETI et de PME dynamiques et innovantes, de nombreuses start-up et s'appuie sur une recherche et innovation de niveau mondial.

Répondant à des besoins croissants de protection des entreprises, des collectivités, de l'État, l'industrie de sécurité représente un enjeu économique et de souveraineté majeur. La protection des sites industriels et des territoires, la sécurité des données, la souveraineté du numérique, constituent des défis que la filière doit relever dans un contexte de mutations technologies rapides et d'une concurrence exacerbée.

La création du CSF constitue ainsi une opportunité unique pour relever ces défis en fédérant les énergies – Industrie, État et utilisateurs, autour de projets structurants concrets, à fort impact et focalisés sur les enjeux clés de compétitivité et de souveraineté. L'ensemble des signataires de ce nouveau contrat de filière se sont accordés sur une première liste de cinq projets ambitieux :

La sécurité des grands évènements et des JO Paris 2024	*Assurer la sécurité des Jeux, tout en permettant de structurer et développer la filière via un événement majeur.*
La cybersécurité et la sécurité de l'Internet des objets :	*Positionner l'industrie française comme leader mondial de la cybersécurité et de la sécurité de l'IoT*
L'identité numérique :	*Permettre le développement rapide du déploiement et de l'utilisation de l'identité numérique en France*
Les territoires de confiance :	*Positionner l'industrie française comme leader mondial de la sécurité de la ville intelligente*
Le numérique de confiance :	*Le premier objectif est de permettre à une offre de cloud de confiance compétitive de se déployer*

Concrétisant le potentiel extraordinaire des nouvelles technologies dans le domaine de la sécurité, les offres innovantes et les modèles économiques pertinents résultant de ces travaux seront particulièrement nécessaires à la protection de l'industrie du futur, à la protection du patrimoine, à la souveraineté numérique. Le CSF se veut ainsi un facilitateur contribuant transversalement à toutes les filières pour sécuriser le pacte productif.

S'inscrivant avec volontarisme dans l'ambition du CNI, la filière s'attachera à développer l'innovation et l'emploi à travers ces projets d'envergure.

Enfin, dans un domaine où l'utilisation abusive de données personnelles ou sensibles est particulièrement crainte, l'une des premières actions de la filière industries de sécurité sera de se doter d'une charte éthique qui formulera de façon explicite et claire les valeurs de la filière et expliquera comment elles sont mises en œuvre dans chacun de ses métiers de façon vérifiable.

Sommaire

PRESENTATION DE LA FILIERE

1. Périmètre et chiffres clés de la filière

La filière des industries de sécurité regroupe l'ensemble des entreprises qui développent des produits et des services technologiques de sécurité pour répondre aux malveillances et menaces croissantes et diversifiées, tant physiques que dans l'environnement numérique. Les services de sécurité privée non technologiques ne font pas partie du périmètre. La filière couvre un périmètre technologique large afin de répondre aux enjeux de sécurité dans toutes ses dimensions : cybersécurité, protection des infrastructures et des réseaux, sécurité du transport, secours aux personnes, lutte contre le terrorisme et la grande criminalité, sécurité des territoires, et gestion de crise.

La filière présente trois grands segments qui se combinent pour des solutions globales souvent requises par le marché :

- Produits de sécurité physique
- Produits et services électroniques et numériques
- Produits et services de cybersécurité

Dans son ensemble, la filière représente :

- 4000 entreprises
- 130 000 emplois
- 28 Mds€ de chiffre d'affaires
- Une croissance moyenne de 6% par an
- Un volume d'exportation de 13 Mds€ (> à 50% du CA)

Filière d'excellence très innovante, elle regroupe un vaste écosystème d'entreprises, des grands groupes leaders mondiaux (biométrie, identité numérique, paiements sécurisés, « secure elements », communications sécurisées), aux PME et start-ups innovantes, en passant par les ETI, dont certaines sont très présentes à l'export. A noter que la majorité de l'activité (60%) est réalisée par les pure players de la sécurité, c'est-à-dire les entreprises où la sécurité compte pour 90% de l'activité.

La filière comprend également de nombreux acteurs de la R&D, notamment des pôles de compétitivité (SAFE, SYSTEMATIC, SCS, TES, MINALOGIC, MER) et les grands organismes de la recherche publique (CEA, INRIA, Universités).

2. Enjeux de la filière

La filière dispose de bases solides. Les industriels de la sécurité sont parmi les plus innovants (1,7 milliard d'euros de dépenses de R&D, soit 5% du CA global), dans la moyenne haute en France, et ils se sont forgé une position de leader à l'international, comme l'attestent leurs performances à l'export (50% du CA est exporté).

Cependant, un changement d'ère technologique, industrielle et sociétale est en train de s'opérer avec la révolution numérique, phénomène auquel s'ajoute la mondialisation.

La filière fait maintenant face à des défis nouveaux ou exacerbés. Les entreprises étrangères, très flexibles, rendent la concurrence internationale plus rude. Les innovations de rupture et les usages qui en découlent s'accompagnent de nouvelles menaces qui rebattent les cartes du marché. En outre, le numérique a un impact majeur sur les métiers de la sécurité dont la nature va changer à long terme, ce qui contribue à modifier le marché en profondeur.

La filière fait ainsi face à trois enjeux clés aujourd'hui :

Le premier enjeu est lié au risque que la transformation numérique fait courir à la protection de nos outils de production et de nos données via la domination croissante d'acteurs non européens. Cet enjeu majeur est à la fois économique et de souveraineté et il se décline sur trois axes principaux :

- Le premier est celui de la cybersécurité pour laquelle il faut maitriser une offre nationale et européenne forte et de confiance. L'Internet des objets, dont les usages et l'économie montent formidablement en puissance, introduit un nouveau volet de sécurité à assurer impérativement et ajoute une nouvelle dimension à cet enjeu.
- Le second est celui de l'identité numérique, un instrument de pouvoir économique à travers la maitrise des usages et des données. Développer des identités numériques alternatives à celles des grands acteurs d'Internet est un enjeu majeur pour la filière.
- Le troisième est la nécessité de disposer d'une offre de Cloud de confiance qui ne soit pas soumise à des juridictions non européennes.

Le deuxième grand enjeu est de développer des offres de sécurité innovantes pour les territoires et les sites – sécurité déclinée sur le terrain et pas uniquement numérique, qui permette de nouveaux usages et la synergie avec les autres fonctionnalités et acteurs des territoires connectés. La sécurité des JOP Paris 2024 en sera un terrain d'application par excellence.

Le troisième enjeu majeur est de se positionner en leader sur les ruptures et leurs applications de sécurité : intelligence artificielle, big data, blockchain, informatique quantique, sur les approches conceptuelles qui peuvent conduire à de nouveaux systèmes et écosystèmes garantissant la « security and ethic by design » et aussi sur matériels et composants micro-électroniques de confiance requis.

3. Vision stratégique

La filière s'engage à relever ces défis technologiques, de souveraineté et commerciaux. La France et l'Europe doivent affirmer leurs ambitions à travers des actions fortes. Cela passe avant tout par une forte mobilisation public-privée refondée, à horizon 5 ans, qui apparaît comme une condition *sine qua non* à l'élaboration de réponses adaptées à ces défis.

Au niveau du marché, les objectifs de la filière pour 2025[1] sont de :

- Doubler le chiffre d'affaires de la filière
- Créer 75 000 nouveaux emplois qualifiés
- Maintenir un taux de croissance à l'export supérieur au taux de croissance national

Les actions portées par les projets structurants incarnent certaines de ces réponses notamment :

- Des actions collectives visant à aligner et fédérer les acteurs pour susciter des réponses fortes et coordonnées (Équipe France déclinée sur les thèmes majeurs, labels, chasse en meute, …),
- L'évolution des dispositifs de l'État (réglementation, certification, soutien de l'industrie, faire de l'État un acheteur important et exigeant, …) ;
- L'engagement pro-actif dans l'action Européenne pour la souveraineté technologique, le développement du marché intérieur, et la politique industrielle ;
- L'engagement décisif pour l'innovation sur les sujets clés de demain et la mise en place d'instances creusets de l'innovation et favorisant les synergies.

[1] Niveau de référence : chiffres 2016

Il faut également s'appuyer sur les atouts de l'écosystème et renforcer leur potentiel : l'excellence scientifique et technologique, la capacité d'innovation, le système national de soutien à l'innovation, le système éducatif.

Ces leviers doivent assurer à la filière une position de leader mondial d'ici cinq ans, ce qui signifie :

- Avoir regagné au niveau Français et Européen la souveraineté technologique et numérique (offre numérique de confiance : cloud de confiance, souveraineté des données, sécurité du numérique, identité numérique, …) en ayant mis en place les offres, les réglementations, les soutiens et les incitations, et investi dans les solutions de demain.
- Couvrir l'intégralité des technologies identifiées comme « critiques », notamment dans les domaines de rupture, par des offres nationales ou à défaut européennes.
- Disposer d'offres visibles et différenciantes, ayant fait leurs preuves sur le marché français, et des dispositifs de promotion efficaces (sécurité des JO, sécurité des territoires intelligents, cloud de confiance, …).

4. Gouvernance de la filière

Le président du comité stratégique de la filière Industries de sécurité (CSF Industries de sécurité) est désigné par les pouvoirs publics. Le premier président est Marc Darmon, accompagné d'un délégué permanent. Il a été choisi parce qu'il est président du Conseil des industries de la confiance et de la sécurité (CICS). L'industrie recommande en effet que la présidence du CSF soit exercée par le président du CICS. Cette association industrielle a été créé en 2013 pour coordonner l'ensemble de la filière industrielle. Elle regroupe les fédérations et groupements actifs dans le domaine de la sécurité, ses membres sont aujourd'hui : l'ACN, l'AN2V, la FIEEC, le GICAT, le GICAN, HEXATRUST.

Le comité stratégique de la filière Industrie de sécurité rassemble les principales entreprises industrielles et de service de la filière, les groupements industriels cités ci-dessus, les organisations syndicales de salariés, des représentants des pôles de compétitivités de la filière, des représentants des collectivités locales, ainsi que les représentants de l'État et des établissements publics les plus directement investis dans le soutien de la filière des industries de sécurité.

Le bureau du CSF Industrie de sécurité est composé :

- de représentants de l'industrie proposés par le CICS. Cette représentation est initialement assurée par : M. Darmon (Thales), Y. Delabrière (Idemia), O. Koczan (Airbus), JN de Galzain (Wallix), P. Demigné (Bertin), L. Denizot (Egidium Technologies)
- d'un représentant des utilisateurs : initialement S. Volant, président du CDSE
- de représentants de l'État (MEF, SGDSN (PSE et ANSSI), Ministère de l'intérieur),
- de représentants des organisations syndicales : initialement P. Gotti (CFE CGC) et F. Guillet (CFTC).

Ce bureau se réunit en tant que de besoin et au minimum tous les 3 mois pour piloter l'avancement des projets structurants et des actions mises en œuvre. Chaque projet est mis en œuvre sous la direction d'un chef de projet, assisté d'un copilote et d'un comité de pilotage.

De façon à développer les synergies entre la filière des industries de sécurité et les autres filières industrielles, qui font face à des problématiques de sécurisation ou peuvent intégrer la sécurité dans leurs approches et notamment dans leurs offres globales à l'exportation, le délégué permanent du CSF anime des échanges avec les autres CSF.

Compte tenu de leurs compétences notamment en matière de développement économique, innovation, internationalisation, d'éducation et de leur accès direct aux instances et aux projets

européens, le CSF estime que les régions ont un rôle important à jouer dans ses projets structurants (en particulier ceux des territoires de confiance et de la cybersécurité), notamment pour :

- Contribuer aux analyses stratégiques
- Sensibiliser et mobiliser le tissu économique et l'écosystème sécurité
- Identifier, accompagner et soutenir des projets notamment collaboratifs d'innovation
- Mettre en œuvre de dispositifs favorisant l'export
- Agir sur le volet éducation supérieure et formation continue
- S'assurer du développement d'une compétence régionale adaptée aux spécificités du tissu industriel, des bassins d'emplois et des orientations de politique industrielle et d'innovation de chaque région.

Le CSF développera le dialogue de filière avec les régions et s'appuiera en particulier sur Régions de France dans ce but.

Enfin, en matière de R&D, le CSF entretient des échanges avec le monde de la recherche, sous la direction du président du CSF, secondé par une personnalité de la filière. Cette personnalité pilote également une coordination R&D du CSF en mobilisant les acteurs en son sein et en développant des échanges avec les instances utiles, ministérielles ou autres telles que le CORIMER (filière des industries maritimes).

Le CSF participe également aux groupes de travail transverses du CNI (GT international, GT emplois et compétences).

PROJET STRUCTURANT N°1 : SECURITE DES GRANDS EVENEMENTS ET DES JO PARIS 2024

Le projet vise à développer une offre industrielle globale pour sécuriser les grands événements avec comme champ d'application exceptionnel les Jeux Olympiques et Paralympiques de 2024.

Ce projet d'offre française de sécurité des grands événements représente une opportunité unique, non seulement d'offrir le meilleur niveau de sécurité à nos concitoyens et à l'ensemble des participants internationaux aux Jeux de 2024, de moderniser par l'utilisation de nouvelles technologies les forces de sécurité intérieures, mais aussi de créer une filière industrielle cohérente et solidaire, à même de répondre dans la durée aux besoins de ses forces de sécurité et de se valoriser à l'international.

Contexte :

Depuis quelques années, les filières sport et tourisme reconnaissent que la sécurité est devenue une composante de l'offre globale, en particulier pour les grands évènements sportifs et culturels. La notoriété de ces grands évènements et la présence de nombreux media en font, en contrepartie, des cibles de choix pour les actes malveillants, la criminalité notamment cyber et, notamment, les plus graves tels que terrorisme ou cyberattaques, ce qui engendre une menace forte et très évolutive. Compte tenu sa position de première destination touristique mondiale et sa place dans le concert des nations, la France accueille sur son sol des événements politiques, culturels, économiques et sportifs majeurs comme le G7, le Festival d'Avignon ou la Coupe du Monde de Rugby, plus 30 évènements sportifs mondiaux majeurs ont ainsi été organisés en France cette dernière décennie. Le critère de la sécurité figure dorénavant parmi les premiers éléments de choix d'un pays face à ses concurrents mondiaux.

A cet égard, les Jeux Olympiques et Paralympiques représentent un évènement sportif et de société, mondial et hors norme, d'une visibilité et d'un impact inégalés, sur une durée qui va bien au-delà de celle des Jeux eux-mêmes. En tant que nation hôte, réussir les JOP, sur tous les plans, est à la fois un impératif et une opportunité exceptionnelle de valoriser le savoir-faire et la marque France, en mettant en avant des premières en termes d'usages et de technologies. Assurer la sécurité des JOP est donc un enjeu essentiel, tant sur le plan du renom de la France que de celui de la démonstration du savoir-faire des organisateurs et par conséquent des compétences humaines et techniques de son industrie. Cette mission est cependant complexe car elle combine de nombreuses contraintes : durée de la période à couvrir, sites très nombreux – également au-delà des sites olympiques (fan zones, transports, etc.), public et flux très importants, transparence pour laisser la place à la fête, maîtrise des coûts, calendrier tendu. Elle représente néanmoins une opportunité exceptionnelle pour l'industrie de sécurité française de démontrer sa capacité à répondre à un tel défi et de positionner en conséquence une offre française sur le marché international pour la sécurité des grands évènements.

La sécurité des grands évènements, qu'ils soient sportifs (JO, mondiaux, etc.), culturels (grands concerts), diplomatiques (G7, G20), ou autres, est un thème particulier qui nécessite de mettre en œuvre un ensemble de capacités (contrôle d'accès, gestion des flux, coordination des forces, cybersécurité, etc.) avec des niveaux de performance élevés, sans dégrader l'expérience des participants. De plus, ces capacités doivent, dans la mesure du possible, s'intégrer avec d'autres activités spécifiques de l'événement (billetterie, applications, broadcast, etc.) comme aux activités générales qu'elles soient d'ordre régalien ou privé (visa, transport, hôtellerie, etc.) Les technologies à maitriser pour y exceller sont nombreuses (biométrie, vidéo intelligente, IA, détecteurs, communications, coordination à la demande, etc.). C'est un domaine en forte croissance sur lequel les attentes sont de plus en plus conséquentes et que la filière souhaite soutenir en y apportant une offre structurée. L'offre technologique permettra à la fois de renforcer les capacités d'action des forces régaliennes ou de sécurité privée, en nombre limité face à un évènement de cette ampleur, et d'autre

part, de faire face à des menaces nouvelles qui nécessitent une réponse technique renforcée (cyber, drones…).

Objectif :

Le projet a le triple objectif d'assurer la sécurité des Jeux, de soutenir la modernisation des forces de sécurité en cohérence avec le Livre blanc, et de structurer et développer la filière des industries de sécurité via un événement majeur et mobilisateur. Ces objectifs s'inscrivent dans une démarche de dialogue étroit entre les utilisateurs et l'industrie, afin que l'offre soit pleinement adaptée aux besoins des utilisateurs, en conciliant innovation, performance, compétitivité et capitalisation au-delà des Jeux.

En effet, la filière dispose de fortes compétences et de solutions innovantes permettant d'apporter, aujourd'hui et à l'avenir, une réponse évolutive, efficiente et de très haut niveau aux besoins de sécurité des grands évènements. Le projet permettra, en s'appuyant en particulier sur les JOP, de valoriser la filière française, structurer son offre en matière de sécurité des grands évènements, mettre en avant sa capacité à mettre en œuvre des innovations marquantes et faire progresser les usages et cadres d'emploi des technologies, tout ceci en liaison avec la filière sport et tourisme.

Le projet de sécurisation des JOP 2024 par son temps contraint, représente un accélérateur majeur pour la mise en œuvre d'une politique industrielle de sécurité coordonnée et structurée pour la France.

L'offre ainsi structurée a bénéficié de l'important travail public-privé engagé dès 2017 par le CoFIS, qui a conduit notamment à une analyse (2018) des risques, menaces et besoins, à la consultation de la filière par des AMI (appels à manifestation d'intérêt - 2019) permettant d'identifier des solutions innovantes, et qui s'est poursuivie par des échanges denses en 2019. Cette offre pourra bénéficier à l'État pour les JOP 2024 mais aussi pour les grands évènements qui seront organisés dans les prochaines années. Ce projet regroupant l'ensemble des acteurs (grands groupes, PME, PMI, Startups) permettra aussi de doter la France d'une offre compétitive au niveau international.

L'industrie vise à développer une offre attractive qui d'une part maximise la valeur ajoutée et le retour pour l'État et les utilisateurs et d'autre part, s'agissant d'évènements festifs, assure une expérience de grande qualité à travers les « parcours » visiteur, athlète, acteurs de sécurité.

Cet objectif sera poursuivi à travers les actions structurantes suivantes :

- Constitution d'une équipe industrielle capable de fédérer la filière et de satisfaire les intérêts essentiels de l'État
- Élaboration d'une proposition industrielle initiale, notamment d'une architecture système, puis de propositions détaillées
- Définition collaborative et par itération entre l'État, les utilisateurs et l'industrie des capacités à mettre en place
- Activité de R&D
- Développement, mise en place et opération des solutions et capacités ainsi définies
- Promotion d'une offre « grands événements » et d'une offre export dérivée de l'offre des JOP 2024

Le projet s'attachera aussi à développer l'héritage des JOP en choisissant des solutions pérennes et à offrir des opportunités pour le développement des territoires.

Bien que les activités de sécurité privée, ne fassent pas partie de la filière des industries de sécurité, un dialogue avec ces acteurs est nécessaire, et l'offre de la filière sera construite en suivant une approche capacitaire globale. Les optimisations proposées prendront en compte l'ensemble hommes / technologies / organisations et les interactions correspondantes.

Pilotage et participants :

Le projet a vocation à rassembler l'ensemble des acteurs nécessaires au succès de la démarche : les industriels, l'État, les utilisateurs (État, Paris 2024, Solideo, collectivités territoriales, opérateurs d'importance vitale, sécurité privée, opérateurs d'infrastructure et de sites, acteurs du tourisme, etc.)

Le projet sera doté d'un comité de pilotage industriel (entreprises et groupements industriels en soutien) présidé par un directeur de projet qui s'appuie sur d'autres instances :

- l'équipe industrielle réunie autour d'une offre globale : les entreprises présentes au comité de pilotage, entreprises intégrées ultérieurement à l'offre (grands groupes, ETI, PME, startups).
- le groupe mixte État– Industrie, qui permet le dialogue entre les parties sur le projet et en valide les principes. L'État désignera un ministère coordinateur. Ce groupe mixte accueillera les autres parties prenantes notamment les utilisateurs et des représentants des pôles de compétitivité.

Le projet développera des liens avec l'ensemble des opérateurs en responsabilité : ministère de l'intérieur (CNSJ, PP, PN, GN, …), ministère de l'économie, ministère des sports, ministère du travail, ministère de la transition écologique, autres ministères impliqués, Paris 2024, Solideo, collectivités locales, opérateurs d'importance vitale et opérateurs de sites, acteurs de la sécurité privée, fédérations, etc.

Livrables attendus et calendrier prévisionnel :

Le projet a vocation à durer jusqu'à la fin des JOP en 2024. Les étapes clés du projet, engagé dès 2018 par anticipation, sont les suivantes :

- Structurations de l'industrie (2018-2019)
- Mise en place d'une équipe de marque étatique (début 2020)
- Première contractualisation dès 2020 des travaux dans le cadre du projet, notamment pour ce qui concerne les études et expérimentations technologiques
- Compléments d'études et expérimentations / déploiement / (2021 – 2023)
- Formation, utilisation opérationnelle et retex (2023 – 2024).

Le projet donnera lieu aux livrables principaux suivants (des livrables ont été produits en 2019 par anticipation).

Année	Livrables
2019	- Constitution du consortium équipe de France / Industrie - Proposition globale de sécurité (remise le 26 juillet 2019 à la CNSJ) - Compléments remis au ministre de l'Intérieur en novembre 2019 lors de Milipol : Addendum / concept d'architecture ; technologies et programme de R&D ; programme d'accompagnement, études et expérimentation
2020	- Remise d'une première proposition d'études et d'expérimentations par le consortium industriel - Définition du cadre de travail État-Industrie - Premier Contrat d'études et expérimentations technologiques - Réalisation des travaux d'innovation / ANR et SGDSN - Constitution de l'offre générique de la filière - Plan de communication et de soutien à l'export
2021-2022	- Études détaillées et expérimentations complémentaires - Résultats des travaux d'innovation ANR et SGDSN - Déploiement de pilotes - Validations /certifications
Début 2023 jusqu'en sept. 2024	- Déploiement des technologies de sécurité à l'occasion de la Coupe du Monde de Rugby 2023 puis des JOP 2024

Automne 2024	- Retex suite aux opérations

Engagements réciproques :
Pour atteindre les objectifs, l'État et l'industrie prennent les engagements réciproques suivants.

1. **Engagements de l'industrie :**
   - Fédérer l'industrie française de la sécurité autour d'un consortium le plus à même de porter une offre de sécurité globale pour assurer la sécurisation des grands événements et en particulier les JOP 2024, tout en répondant aux impératifs de souveraineté.
   - Définir et construire une offre cohérente et structurée dans une démarche collaborative avec les utilisateurs.
   - Intégrer les meilleures solutions et offres technologiques innovantes d'origine française pour les incorporer dans une approche cohérente et structurée entre les grands groupes de la filière, les PME, et les start-ups innovantes. L 'offre finale incorpora donc une part importante de PME et startups.
   - Construire une offre robuste de l'industrie française embrassant toute la chaîne de valeur et répondant aux besoins identifiés à travers une architecture modulaire et évolutive. Il s'agit de doter la France d'une offre complète de solutions de sécurité qui sera mise en valeur lors des JOP et pourra être proposée lors d'évènements futurs en France et à l'étranger.
   - Coordonner activement et soutenir la collaboration de recherche et développement des acteurs français pour non seulement consolider mais aussi construire une offre technologique de sécurité à l'état de l'art. L'industrie conduira des démonstrations, expérimentations et pilotes sur la période 2020-2023.
   - Mettre en place les formations avec les parties prenantes afin d'assurer l'appropriation des solutions.
   - Mobiliser tout au long du projet ses meilleures compétences et savoir-faire pour assurer le bon fonctionnement des solutions mises en place dans le cadre de la filière, pour la sécurité des grands évènements et des JO 2024.
   - Appliquer pour les grands évènements une politique de R&I cohérente et complémentaire entre les industriels de l'Équipe France (pour éviter les doublons et assurer l'efficacité d'ensemble).
   - Maintenir l'équipe France dans la durée afin de constituer une offre générique permettant d'adresser le marché de la sécurité des grands évènements en général, en particulier à l'export
   - Mener des actions de promotions avant, pendant et après les JOP 2024 avec l'appui notamment des groupements exports comme le GICAT.

2. **Engagements de l'État**
   - Constituer en 2020 et animer une Équipe de Marque interministérielle en capacité d'exprimer les besoins précis du Ministère de l'intérieur en termes de technologies de sécurité. Cette équipe de marque étudiera ces technologies de sécurité, en lien avec le consortium industriel et en parfaite cohérence avec les propositions du Livre blanc de la sécurité intérieure.
   - Solliciter un budget "*sécurité des JOP 2024 et des grands évènements sportifs internationaux*" piloté par le Ministère de l'intérieur, en vue de financer l'expérimentation des technologies de sécurité choisies et leur déploiement opérationnel.

   Et dans le cadre décrit ci-dessus :

   - Participer au groupe mixte État-industrie et favoriser la participation des parties prenantes (pilotage CNSJ)
   - Assurer la coordination de l'ensemble de ses représentants, dans toutes les phases du projet.

Synthèse des engagements clés	
L'industrie s'engage à :	- **Fédérer la meilleure équipe France à même de répondre aux impératifs de souveraineté et de sensibilité et associant les PME et les start-up de la filière** - **Construire dans une démarche collaborative avec l'État une offre globale robuste assurant sur le terrain en 2024 la meilleure sécurité des JO** - **Coordonner, soutenir et co-financer la collaboration de R&D pour assurer le meilleur niveau technologique des solutions mise en œuvre**
L'État s'engage à :	- **Constituer en 2020 et animer une Équipe de Marque interministérielle en capacité d'exprimer les besoins précis du Ministère de l'intérieur en termes de technologies de sécurité Cette équipe de marque étudiera ces technologies de sécurité, en lien avec le consortium industriel et en parfaite cohérence avec les propositions du Livre blanc de la sécurité intérieure.** - **Solliciter un budget "*sécurité des JOP 2024 et des grands évènements sportifs internationaux*" piloté par le Ministère de l'intérieur, en vue de financer l'expérimentation des technologies de sécurité choisies et leur déploiement opérationnel.**

<u>Modalités d'évaluation du projet</u> :
Le projet sera considéré comme ayant atteint ses objectifs selon plusieurs critères cumulatifs :

- Formation d'un consortium industriel porteur de l'offre France pour la sécurité, sûreté et cybersécurité des grands événements,
- Existence d'un (de) contrat(s) structurants entre le consortium représentant l'industrie et les bénéficiaires pour la sécurisation des grands événements
- Contractualisation dès 2020 de prestations d'études et d'expérimentations technologiques
- Part significative de l'industrie française (produits et services technologiques) dans la sécurité des JO (hors part de la sécurité humaine)
- Part en valeur de l'offre attribuée au PME et start-up supérieure à *30 %*
- Nombre de nouveaux usages majeurs mis en œuvre
- Utilisation des solutions de la filière dans les événements autres que les JO et notamment la Coupe du Monde de Rugby 2023, ou à l'étranger
- Robustesse de la sécurité mise en œuvre démontrée suite au Retex
- Existence d'une offre France constituée pour l'export

PROJET STRUCTURANT N°2 : CYBERSECURITE ET SECURITE DE L'IOT

La France a un potentiel exceptionnel en matière de cybersécurité. La filière a l'ambition de relever le défi de réaliser ce potentiel en alignant et mobilisant les acteurs sur des politiques :

- **d'éducation et de formation (4000 formations en 3 ans),**
- **d'actions territoriales dynamisant les initiatives régionales,**
- **de mise en œuvre des synergies dans le cadre d'un Forum État-Industrie-Utilisateurs,**
- **d'innovation et de développements technologiques, en particulier pour les besoins souverains,**
- **de mise en place d'investissements ambitieux ciblant plus particulièrement les PME en croissance.**

Ce projet s'appuiera notamment sur les travaux collaboratifs menés au sein du futur Campus cyber.

Contexte et périmètre :

La cybersécurité est un secteur industriel stratégique sur les plans sécuritaire, économique et sociétal.

L'autonomie stratégique et technologique ainsi que la certitude d'une indépendance suffisante vis-à-vis des acteurs étrangers sont seules à même d'assurer notre souveraineté. Renforcer ou acquérir cette indépendance nécessite l'émergence d'une industrie nationale de taille mondiale capable notamment de rentabiliser ses investissements par des ventes à l'export. Le développement et la pérennisation des acteurs de cette filière doivent donc être considérés à la fois comme un impératif de souveraineté numérique nationale et comme un vecteur d'autonomie stratégique européenne.

Par ailleurs, la France dispose d'atouts considérables grâce à un écosystème diversifié et performant (entreprises de toutes tailles, recherche dynamique, excellence technique reconnue…). Capitaliser sur ce tissu industriel et faire de la France un champion de la cybersécurité est donc également un levier fort de développement économique et de création d'emplois pour notre pays et pour l'Europe.

L'Etat dresse ce constat dans la revue stratégique de cyberdéfense, publiée le 12 février 2018 par le Secrétariat général à la Défense et à la Sécurité Nationale (SGDSN). Il est donc nécessaire que l'État et les industriels travaillent de concert dans l'atteinte de ces objectifs communs.

La confiance numérique, secteur dans lequel s'inscrit la cybersécurité, est en outre caractérisée par un contexte réglementaire en pleine évolution (directive NIS, RGPD, Cyber Act européen, création du centre cyber européen, Cloud Act américain, etc.) susceptibles de faire émerger de nouveaux besoins auxquels l'industrie doit se préparer.

La confiance numérique est actuellement portée par la transformation numérique des entreprises et de la société, l'internet des objets et la 5G. Du point de vue économique, les produits et services de cybersécurité représentent 6,6 milliards d'euros de chiffre d'affaires en France en 2018, 3,7 milliards d'euros de valeur ajoutée, près de 35000 emplois, et une croissance annuelle de l'ordre de 11,9%. Le secteur est marqué par une forte innovation, avec des positions françaises d'excellence dans des domaines tels que l'IA et la cryptographie. Enfin, il est clé parce qu'il est au carrefour de plusieurs autres secteurs (services et équipements IT, télécoms, défense et aérospatial), et qu'il imprègne l'ensemble de l'industrie.

Cependant, l'offre demeure très fragmentée (63% des entreprises de la confiance numérique font moins de 2 millions d'euros de chiffre d'affaires) et une forte exposition à la concurrence mondiale (le poids des acteurs étrangers est estimé à 30% à 40% du marché français si on inclut les services) dont les acteurs dominants sont concentrés dans quelques pays (États-Unis, Israël).

Face à cette situation, l'industrie française s'est jusqu'à présent développée de façon relativement autonome et a donné naissance à quelques grands groupes mondiaux ainsi que plusieurs centaines de PME innovantes avec un potentiel mondial.

Néanmoins, un certain nombre de constats peuvent être faits :

- L'absence de solutions nationales et/ou européennes dans certains domaines sensibles de la cybersécurité soulève à terme des questions d'autonomie stratégique voire de souveraineté ;
- si la France et l'Europe ont fait des efforts significatifs pour soutenir leur industrie, les volumes investis sont sans commune mesure avec ceux investis par d'autres États, en particulier les États-Unis, en termes de R&D mais également d'achat direct de produits et de services de cybersécurité par les agences nationales ;
- le retour des utilisateurs démontre que la fragmentation de l'offre française rend nécessaire une démarche de mise en cohérence des offres.

Pour répondre à ces défis, le projet « cybersécurité et sécurité de l'IOT » s'articulera autour de cinq axes, couvrant chacun une dimension essentielle de la problématique abordée : la dimension humaine, la dimension géographique, le dialogue des acteurs, et le développement de l'offre :

- L'axe 1, « Faire de la France une terre de cybersécurité », consiste à mettre en place les dispositifs destinés à rendre le grand public plus averti des risques cyber, renforcer l'attractivité des métiers de la cybersécurité et de la France, et assurer des capacités d'enseignement et de formation nécessaires à tous les niveaux.

- L'axe 2, « Mobiliser les territoires », vise à dynamiser les énergies et les intelligences disponibles sur l'ensemble de nos territoires pour coordonner les initiatives locales, et contribuer à leur mise en cohérence en réponse aux besoins de cybersécurité de la filière, et des bassins industriels français.

- L'axe 3, « Forum État Industrie Utilisateurs », projette de créer un outil de dialogue et d'actions coordonnées entre l'Etat, l'industrie et les utilisateurs afin d'échanger sur les besoins, le cadre réglementaire, les contraintes et les opportunités générées par l'environnement international dans le secteur de la cybersécurité.

- L'axe 4, « Doter la France d'une offre de rang mondial », consiste à développer en bonne collaboration des démonstrateurs, prototypes et projets susceptibles de hisser l'industrie de cybersécurité française aux premiers rangs de l'offre mondiale.

- L'axe 5, « Déployer des actions structurantes pour l'écosystème dans le cadre du campus cyber », fait le lien entre le CSF et le campus cyber à venir. Le campus cyber aura une vocation très opérationnelle, à la différence du forum qui sera une instance stratégique. Le campus pourra mettre en place des actions du contrat de filière.

Ce projet a été écrit après recueil par l'ACN et Hexatrust des idées émises par un panel d'industriels et d'utilisateurs au terme de plusieurs réunions dont un barcamp. 84 organisations ont participé, dont notamment le CESIN, le CIGREF, le CLUSIF, le pôle Systematic, Bretagne Developpement Innovation, les ministères des Armées, de l'Intérieur, de la Transition Ecologique et Solidaire, et de l'Économie ainsi que des représentants de nombreux industriels et des écoles ayant des cursus en cybersécurité. Il porte donc les idées de l'ensemble de la filière.

AXE 1 : FAIRE DE LA FRANCE UNE TERRE DE CYBERSECURITE

La cybersécurité constitue une filière dynamique et en croissance. Mais la pénurie constatée des talents en matière de cybersécurité risque de s'intensifier dans les prochaines années, mettant en dangers la cyber résilience de nos organisations publiques et privées ainsi que notre compétitivité sur le terrain du numérique.

L'objectif de la filière est de maximiser le potentiel humain de la France en matière de cyber. A cette fin, pour renforcer la culture cyber et les compétences disponibles, la filière vise à : 1) rendre le grand public plus averti des risques cyber ; 2) renforcer l'attractivité des métiers de la cybersécurité et 3) assurer des capacités d'enseignement et de formation nécessaires à tous les niveaux (scolaire, formations post bac courtes et longues, reconversion).

1.1. Renforcer la résilience de la population

Une démarche de compréhension de l'informatique et aux risques IT est nécessaire dès l'entrée au collège : d'une part pour sensibiliser les enfants aux risques auxquels ils sont exposés sur internet et d'autre part pour créer un enthousiasme technologique paritaire (chez les garçons et les filles) nécessaire au bon développement de futures générations de métiers.

Aujourd'hui, les usages du numérique sont traités au collège dans le cadre du programme d'enseignement moral et civique (EMC) et de l'éducation aux médias et à l'information (EMI), ainsi qu'en mathématiques et technologie. Au lycée, la cybersécurité figure explicitement dans le programme d'EMC. L'enseignement de « Sciences numériques et technologie » fait d'ores et déjà partie du tronc commun en seconde, où les questions de sécurité et de confidentialité sont traitées. En première et en terminale générale, la spécialité « Numérique et des sciences informatiques » (NSI) vise l'appropriation des fondements de l'informatique pour préparer les élèves à une poursuite d'études dans l'enseignement supérieur. En outre, le cadre de référence des compétences numériques et la certification délivrée en fin de cycle 4 (collège) et de cycle terminal (lycée) comprend plusieurs domaines parmi lesquels « Protection et sécurité ».

La filière et l'Éducation nationale travailleront ensemble avec les territoires en vue de la mise en place des ressources de formation adaptées. Parallèlement pour sensibiliser les adultes aux risques en matière de cybersécurité, un message national de sensibilisation sera diffusé au grand public analogue aux messages nationaux dans le domaine de la santé publique. Le but est d'élever le niveau général d'hygiène informatique pour réduire l'impact potentiel d'une attaque sur la population.

Pilotes :

- Etat : Ministère de l'Éducation Nationale et de la Jeunesse
- Industrie : ACN/HT et/ou Cigref

1.2. Créer de nouvelles formations courtes

La filière arrive aujourd'hui plus ou moins à trouver les ingénieurs pointus dont elle a besoin et le nombre de places en master semble maintenant suffisant. En revanche, elle présente un déficit de formation aux niveaux Bac et Bac +2. A titre de comparaison, l'État d'Israël forme plus de 5000 nouveaux lycéens par an à la cybersécurité[2]. Le but est de faire de la cybersécurité une opportunité de développement non seulement économique (et d'emploi) mais aussi sociale (parité H/F et cadres/agents de maitrise/employés).

La rénovation récente du BTS « Services informatiques aux organisations », dont la première rentrée aura lieu en 2020 et la première session d'examen en 2022, est un premier signal positif pour la

[2] Il s'agit du programme Masgshimim qui vise les lycéens de la seconde à la terminale et a été lancé en 2013.

formation de technicien en cybersécurité, celle-ci constituant l'un des blocs de compétences à valider pour le diplôme.

Concrètement les actions prévues sont les suivantes :

- Etudier avec les professionnels la création de nouvelles formations courtes en cybersécurité (de niveaux 3, 4, 5 / BTS ou DUT Cyber, …) ou l'approfondissement, voire l'adaptation des formations existantes (ex : BTS « Services informatiques aux organisations », ou autres diplômes), dans la logique de les adapter aux besoins des utilisateurs. L'objectif est de former 4000 opérateurs cyber en 3 ans sur les outils des éditeurs nationaux. Ces derniers s'engagent à fournir les licences et les tutoriels nécessaires.
- Développement de cursus modulaires de formation cybersécurité pour la reconversion des demandeurs d'emploi et la montée en compétences des salariés et de formations de courte durée adaptées à cet objectif de reconversion.
- Mise en œuvre d'une campagne massive de publicité sur les métiers de la cybersécurité telle que par exemple « Devenir Expert en Cybersécurité ». Le but : faire connaître aux jeunes les métiers de la cybersécurité grâce à une communication forte et attractive (en termes d'image, de valeurs, de style de vie, d'emploi). Les canaux de diffusion doivent être : un site internet dédié, les réseaux sociaux (Instagram, Facebook, LinkedIn) ainsi que l'affichage publicitaire massif (panneaux des transports bus et métro ; spot télévisuel).
- Participation d'industriels et d'utilisateurs à la définition des contenus des formation.

Pilotes :

- État : Ministère de l'Éducation nationale et de la Jeunesse, Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, ministère du Travail (DGEFP)
- Industrie : Hexatrust/Cigref/Cesin/ Syntec numérique

<u>Engagements réciproque de l'axe 1</u> :

Industrie :

- Fournir les outils et les experts nécessaires pour les formations
- Accueillir des stagiaires en formation dans l'industrie et chez les utilisateurs
- Financer et réaliser la campagne sur les métiers

État :

- Mettre en place les conditions permettant de viser des formations approfondies en cybersécurité
- Favoriser le développement de la spécialité « Numérique et des sciences informatiques » (NSI) au lycée général et technologique
- Financer et réaliser la campagne nationale de sensibilisation citoyenne

AXE 2 : MOBILISER LES TERRITOIRES

La cybersécurité concernant tous les Français, toutes les industries, il est indispensable de mobiliser le plus de territoires possibles pour éviter l'apparition de « fractures cyber » et accompagner leur transformation numérique.

La filière souhaite associer et renforcer les pôles territoriaux, à la fois utilisateurs et écosystèmes de cyber, et qu'ils soient renforcés comme clés du succès de son développement. A cette fin elle vise à les mobiliser, à renforcer leur rôle de sensibilisation, à développer la coordination et la synergie entre les projets et initiatives régionales au plus proche des bassins industriels français et de leurs besoins, tout en incitant les régions à mettre en place les outils et les politiques d'achats au profit des entreprises locales de cybersécurité.

2.1 - Mobiliser des organisations économiques territoriales

Les spécificités des territoires permettent d'imaginer le développement d'axes métiers de la cybersécurité différents les uns des autres en ligne avec les besoins des secteurs des utilisateurs implantés sur le territoire. Il convient alors de développer des métiers cyber adaptés à chacun, en coordonnant les initiatives pour limiter la déperdition d'énergie et capitaliser sur les dynamiques locales.

Les actions prévues sont les suivantes :

- Établir une cartographie des projets, initiatives et forces RH en France et dans toutes les régions.
- Mobiliser les organisations économiques territoriales (Développement économique, CCI, Pôles, Cluster, etc..) autour de l'enjeu cyber en s'appuyant sur les axes de développement locaux, participer aux projets structurants et décliner localement les actions de formation et d'attractivité de la filière. [3]
- Organiser le dialogue entre les différentes initiatives territoriales dont l'éventuel futur campus cyber pour éviter toute dispersion et optimiser l'efficacité globale.

Pilote :

- Forum État Industrie décrit à l'axe 3

2.2 - Mise en place d'infrastructures d'accueil dans les territoires

Le but de cette action est de fournir des espaces physiques d'échange et de développement pour les entreprises du secteur et en particulier les start-ups. Ces espaces auront quatre missions :

- Favoriser le partage et la mutualisation d'outils, de compétences et de données entre les acteurs locaux de l'écosystème
- Accompagner l'innovation publique et privée pour concourir au développement local de la filière de cybersécurité
- Inciter les collectivités locales à s'équiper localement
- Servir de point focal au dialogue entre les différentes initiatives territoriales identifiées au paragraphe précédent.

Le CSF sollicitera les régions pour fournir un hôtel d'entreprises pour la cyber et organiser un guichet unique pour le soutien et le financement. Ces hôtels d'entreprise devraient idéalement comporter des espaces locaux d'idéation et de démonstration (showrooms) ainsi que des campus pour accueillir les écosystèmes locaux.

[3] On pourrait par exemple demander aux pôles mer de prendre en charge les aspects cyber de la Marine et des grands navires marchands et de croisière.

Cybersécurité et sécurité de l'IoT

Pilotes :

- État : Ministère de la Cohésion des Territoires et Régions volontaires (via les pôles), la Mission FrenchTech
- Industrie : Un industriel local chef de file par région volontaire

Engagements réciproques pour l'axe 2 :

Industrie

- Mobiliser les organisations industrielles régionales autour de projets structurants
- Soutenir la mise en place des moyens et des projets dans les régions intéressées.
- Co-réaliser la cartographie

Etat

- Inciter les régions à s'intégrer dans le dispositif (influence, moyens…)
- Aider à la coordination des différentes initiatives locales et nationales en matière de sensibilisation au risque cyber
- Co-réaliser la cartographie
- Étudier et mettre en œuvre les moyens d'inciter les collectivités locales à s'équiper localement.

AXE 3 : CREER UN FORUM ÉTAT-INDUSTRIES-UTILISATEURS CYBERSECURITE

L'objectif est de développer une instance de pilotage et de dialogue public-privé efficace pour fédérer et développer la filière de cybersécurité. Le forum rassemblera tous les acteurs de la filière (administration, associations d'industriels et d'utilisateurs, clusters, pôles, …), conduira un dialogue stratégique et mènera des chantiers essentiels au développement de la filière. Ce forum visera notamment à mobiliser la réglementation, mettre en place une base d'informations partagées, promouvoir l'émergence d'un marché domestique européen, coordonner les actions françaises en Europe et à l'international (notamment la certification), soutenir le grand export, mener des réflexions sur la mise en place d'une éventuelle réserve civile cyber.

Ce forum sera le canal privilégié de coopération et de communication des plans d'action issus de la revue stratégique de cyberdéfense

Il sera institué sous la forme d'un organisme piloté par des représentants de l'État et des organisations industrielles. Il pourra établir des sous instances et des groupes projets en charge des différents domaines de compétences ci-dessus. Il s'appuiera sur une Délégation Générale composée de permanents. Au vu des enjeux, la taille idéale semble être une dizaine de permanents pour les différentes missions du forum : représentation à Bruxelles, stratégie et veille, attractivité, soutien à l'export…

Le budget objectif est de l'ordre de 1M€+ par an assuré par l'industrie (tour de table à préciser).

Le forum a vocation à être le pilote de l'ensemble des actions décrites dans le contrat de CSF.

3.1 - Mobiliser la réglementation pour le développement de la filière

Il s'agit de mettre en cohérence les politiques, les commandes publiques et les priorités de R&D et d'innovation, au regard de la doctrine de cyber sécurité, en particulier :

- Travailler conjointement à ce que les obligations des grands opérateurs soumis aux règles de la commande publique et celles des acteurs liés par des instruments de protection spécifiques (OIV et OSE à travers la LPM et NIS par exemple) soient renforcées et mises en œuvre à travers des schémas de qualification et de certification efficaces et auxquels l'Industrie française ou européenne sache répondre.
- Renforcer le lien entre la filière industrielle, la recherche et l'État.
- Amplifier ces priorités par une action concertée au niveau européen.
- Éviter que l'industrie se retrouve de facto en concurrence avec l'État
- Le forum sera mis à contribution pour la création et la révision des schémas de qualification et de certification des produits et des services pour les rendre plus performants tant d'un point de vue technique (prise en compte des nouveaux environnements notamment « as a service » ou encore IoT), que d'un point de vue industriel (time-to-market).

Il convient enfin de veiller à ce que les obligations réglementaires soient appliquées correctement. Pour cela, il faut inciter tous les secteurs à s'approprier l'approche globale de cyber sécurité :

- Mettre en place une structure d'échanges périodiques État/Industrie/Utilisateurs pour remonter les problèmes identifiés.
- Inciter les autres CSF à participer à un groupe tripartite (filière cyber / secteur utilisateur / ANSSI) pour définir des schémas de certification de cyber sécurité adaptés aux besoins du secteur, en vue de les porter de manière coordonnée au niveau européen.
- Produire des documentations métiers et des méthodologies adaptées aux différents secteurs et aux filières industrielles utilisateurs ;
- Mettre en place des incitants pour accompagner les secteurs utilisateurs dans leur nécessaire cyber sécurisation.

3.2 - Mise en place d'une base d'information partagée

Cette action vise à la mise à disposition et la gestion d'un ensemble de données (data set) partagé entre les acteurs de la filière à l'image de ce qui existe ailleurs (notamment au Canada) ou dans d'autres filières (Boost Aerospace par exemple dans l'aéronautique). Un tel ensemble de données permet de constituer des benchmarks standards des outils du marché. Il constitue également une excellente base d'apprentissage pour différentes nouvelles technologies qui en ont besoin notamment l'apprentissage automatique et l'intelligence artificielle. Il permet à tous de partager une base commune utilisable pour les entreprises, associations, particuliers et donc enrichissable par chacun, de développer des formations et, plus généralement, de rendre disponible, au plus grand nombre, des informations auparavant inaccessibles (université, entreprises ; etc.). Il pourrait (entre autres) contenir les données suivantes :

- Vulnérabilités
- Signatures
- Jeux de tests
- Marches à suivre
- Faux positifs
- Best practices

3.3 - Coordination Europe et international (dont certification)

L'établissement d'un plan d'action dans ce domaine repose sur la parfaite connaissance des mécanismes français et européens, sur une vision précise de l'action des différents acteurs ainsi que sur une parfaite coordination des informations et actions liées dans des groupes de suivi spécifiques rassemblant tous les acteurs publics et privés de l'écosystème autour d'un sujet d'intérêt commun (à l'image de l'Équipe de France du cPPP Cyber / ECSO).

Cette vision doit couvrir, aux niveaux français et européens, les aspects législatifs et réglementaires, mais aussi les domaines de la certification et la normalisation. Ces éléments sont déterminants car ils structurent le marché de la cybersécurité des années à venir. Ils doivent donc faire l'objet d'une veille permanente. L'action sur les textes européens (Centre de compétences cyber européen et Cyber Act), sur la mise en œuvre des textes existants (NIS, RGPD, e-IDAS, etc.) et dans les instances européennes (ENISA) doit être renforcée et coordonnée. Les actions prévues sont :

- Porter au niveau européen l'idée que l'autonomie en matière cyber est une nécessité
- Promouvoir et soutenir de façon plus active les actions de l'industrie française en Europe y compris dans l'innovation
- Créer un outil collaboratif de veille réglementaire et de cartographie dynamique et partagée des différents lieux d'intérêt / groupes d'experts / calendriers de prise de décisions / territoires actifs, sur les thèmes de normalisation / certification / réglementation. Cet outil doit permettre, sur un sujet donné, de faire le point sur l'état de la réglementation, les évolutions en cours (calendriers législatifs, etc.), la hiérarchie des normes, les acteurs impliqués dans les travaux afférents, les échéances à venir, etc.
- Favoriser des points de coordination autour de nos positions vis-à-vis de l'Europe et de ses instances. Formaliser ce que la France souhaite mettre en avant en matière d'évolution du cadre règlementaire européen : promotion d'un observatoire de la transposition de la directive NIS et élaboration d'axes pour une directive « NIS 2 », suivi du projet de règlement European Competence Centers, du European Cybersecurity Act, etc…

3.4 - Participer à l'émergence d'un marché domestique Européen

L'émergence et le développement d'un marché domestique européen est un levier important pour permettre aux entreprises de la confiance numérique de lutter à armes égales avec leurs compétiteurs mondiaux, qui disposent d'ores et déjà de marchés domestiques beaucoup plus étendus.

C'est pourquoi toutes les actions visant à homogénéiser le marché européen et à réduire les barrières entre États membres de sorte à créer un marché le plus accessible possible aux acteurs européens sont essentielles.

De nombreuses initiatives sont menées par l'Union européenne en ce sens et notamment l'ensemble de l'édifice réglementaire visant à élaborer un Marché Unique du Numérique. Ces initiatives doivent être promues, consolidées et amplifiées.

C'est notamment le cas pour le règlement European Cyber Act qui vient d'être adopté et qui instaure un cadre pour l'élaboration de schémas de certifications communs en matière de cybersécurité sous l'égide de l'ENISA. Ce règlement permettra à terme d'avoir des schémas de cybersécurité opposables directement dans l'ensemble des Etats membres, ce qui est un objectif poursuivi de longue date par notre industrie. Il est urgent que l'ensemble de l'écosystème de la confiance numérique s'approprie ces nouveaux outils et mécanismes et soit en mesure de proposer des schémas de cybersécurité dans tous les domaines (horizontaux ou verticaux) associant étroitement à leur élaboration les offreurs de solutions de cybersécurité, les utilisateurs et l'ANSSI. La filière doit également participer aux travaux et arbitrages sur ces schémas à travers les différents groupes d'experts mis en place par le European Cybersecurity Act. L'appui coordonné des autorités publiques françaises actives à Bruxelles sur ces sujets est un élément clé pour optimiser l'influence de notre écosystème dans ces processus.

Parallèlement, il est également important de mieux faire connaître l'offre française au sein de l'Union européenne, notamment en initiant des actions (cyber road trips, par exemple) dans les autres pays européens. Le résultat de telles actions sera d'autant plus optimisé qu'elles seront collectives et synergétiques, entre les grands groupes, les ETI, les PME, les startups ainsi qu'avec les autres acteurs de l'écosystème de la cybersécurité (recherche, laboratoires d'évaluation, etc.).

Enfin, une connaissance approfondie et une veille exhaustive sur l'ensemble des acteurs européens liés au secteur sera un atout majeur afin de bien prioriser les actions et établir une stratégie efficace. Cette montée en compétence des acteurs français pourra se faire grâce à des outils ad hoc (cf. propositions du § 3.3) de monitoring et de veille sur de nombreux sujets dont notamment le suivi des appels d'offres en matière de cybersécurité dans les différents États membres.

3.5 - Soutien au grand export

Le marché national est trop étroit pour que puisse émerger une filière industrielle des technologies cyber capable de faire jeu égal avec les USA, la Chine, Israël et la Russie. La conquête de marchés export est nécessaire. Pour cela, la filière a besoin du soutien de l'État, comparable à celui mis en œuvre dans d'autres filières (aéronautique, défense…) et que les pays concurrents n'hésitent pas à faire jouer dans la cyber (Israël et les USA notamment). Ce soutien général passe par une mobilisation de l'ensemble des acteurs du soutien à l'export (MAE, Business France, Bpifrance, DG Trésor, DGA/DI, MININT/DCI…) autour des dossiers cyber.

Deux actions ponctuelles sont par ailleurs prévues :

- La première est la création de deux centres de soutien mutualisés, un sur la plaque Asie et l'autre sur la plaque Amériques pour permettre à nos entreprises d'assurer un soutien en « follow the sun » à moindres frais. Business France et les CCI seront sollicités pour porter ces projets qui seront autofinancés à terme.
- La seconde est de capitaliser sur l'existant pour doter la filière cybersécurité d'un salon de taille mondiale, c'est-à-dire un salon de 2000 exposants de plus de 50 pays avec 100 000 visiteurs.

Engagements réciproques pour l'axe 3 :

Industrie :

- Mettre en place le forum, en définir les statuts et les modalités pratiques (hébergement, recrutement, etc..) en liaison avec l'État. Monter le tour de table du coté industrie avec des engagements sur cinq ans.
- Mettre en place un outil de veille sur les sujets économiques, normatifs et réglementaires
- Alimenter la base de données partagée
- Renforcer la présence française dans les organismes internationaux de normalisation / standardisation
- Installer deux centres de soutien « follow the sun »

État :

- Soutenir le forum
- Alimenter la base de données partagée de type Boost Aerospace Cyber
- Porter les positions coordonnées au sein du forum vers l'Europe et les organisations internationales
- Renforcer la présence française dans les organismes internationaux de normalisation / standardisation
- Mobiliser Business France et les CCI internationales autour de la cybersécurité
- Mettre en place les moyens nécessaires au soutien étatique en vue de l'émergence d'un salon de taille mondiale (Ministère de l'intérieur)

AXE 4 : DOTER LA FRANCE D'UNE OFFRE DE RANG MONDIAL

Afin de poursuivre le développement technologique et commercial de l'offre française et de la hisser au rang mondial, des actions seront lancées pour développer les briques et solutions, promouvoir l'offre française, la faire connaître auprès de toutes les filières utilisatrices et assurer l'accès des entreprises au financement nécessaire à leur développement.

4.1 - Amélioration et promotion du « made in France »

En matière de cybersécurité, l'image de marque est double : elle dépend de l'éditeur et de la nationalité. A titre d'exemple, une solution américaine ou israélienne est réputée de qualité en cybersécurité. De la même manière, l'objectif est de faire de la France une marque forte, ce dont elle est capable, à l'instar des secteurs du luxe ou de l'aéronautique.

Deux points laissent penser que l'objectif est atteignable. D'abord, la France est reconnue dans le domaine des mathématiques et de l'informatique. En attestent le fait que plusieurs éditeurs et intégrateurs majeurs sont issus du pays (Dassault Systèmes, Cap Gemini, Atos…), ou encore que les Français sont très représentés dans les équipes de la Silicon Valley. La France est en outre reconnue dans le domaine de la sécurité. Soumis à une menace forte et persistante, le pays résiste depuis de nombreuses années avec succès. Étendre cette reconnaissance à la cyber sécurité semble être un objectif raisonnable.

L'objectif de développer cette marque France est triple

- Inciter les grands groupes français et européens à acheter français à l'échelle de leurs opérations mondiales
- Positionner la France en leader du marché cyber européen
- Positionner la marque France au grand export.

Promotion et renforcement du label France Cybersécutity :

La capacité à distinguer et à valoriser les offres françaises constitue un atout essentiel. Le label existant France Cybersecurity, animé conjointement par un collège d'industriels, d'utilisateurs et étatiques est un outil sur lequel il convient de capitaliser. Issu d'une action filière dans le cadre du plan 33, il vise à attester de l'origine française d'un produit ou d'une solution de cybersécurité et s'inscrit en pleine complémentarité des certifications/qualifications délivrées par l'ANSSI qui attestent quant à elles de la robustesse des produits. Ce label doit donc être systématiquement promu, notamment par les acteurs publics, à travers l'ensemble des initiatives et actions liées à l'export. Par ailleurs, ce label pourrait être complété par une appréciation de critères fonctionnels et métiers telle que l'ergonomie. Dans la même logique, toutes les actions visant à mettre en lumière, caractériser et assurer la promotion de la filière de la confiance numérique doivent être amplifiées.

Évolution du mécanisme de certification :

Concernant la qualification, la revue stratégique de cyberdéfense préconise une évolution du mécanisme comme suit : « *La qualification constitue un mécanisme éprouvé et bien adapté à la validation des exigences de sécurité de l'État pour des produits de sécurité classiques. La France pâtit cependant d'un catalogue de produits qualifiés insuffisant, tant en termes de diversité des fournisseurs que de couverture de certains besoins des administrations ou OIV, notamment dans des domaines émergents comme celui des sondes de détection. Par ailleurs, le mécanisme actuel de qualification, centré sur l'évaluation de sécurité, ne prend pas en compte les attentes fonctionnelles au sens large (richesse des fonctionnalités, performances, ergonomie) du client, et souffre de ce fait d'une image négative (les produits qualifiés sont souvent perçus comme inférieurs sur le plan fonctionnel). Le travail précurseur de modernisation d'ores-et-déjà engagé pour la qualification des sondes de détection*

pourrait servir de modèle, sur la base d'un retour d'expérience, pour la qualification d'exigences fonctionnelles. »[4]

Faire de l'État un acheteur important et exigeant des produits de la filière

Enfin, l'État doit se comporter en acheteur important et exigeant de solutions pour assurer la sécurité de ses administrations, en privilégiant celles qui sauvegardent notre autonomie stratégique, via les Visas ad hoc, garantissant ainsi un premier niveau de retour sur investissement pour les acteurs qui ont fait l'effort d'obtenir ces visas. Il doit également faire la promotion de ses acquisitions, pour inciter les grands acteurs industriels français et européens à s'équiper avec ces mêmes offres et soutenir ainsi la filière à l'export.

Un Observatoire, adossé aux initiatives existantes et compilant des indicateurs utiles à la compréhension et à l'analyse du secteur, serait un instrument nécessaire pour atteindre ces objectifs. En effet, la connaissance la plus précise possible de la filière, mais aussi des acteurs qui la composent et de leurs évolutions est essentielle pour permettre à l'État d'accompagner la montée en puissance de sa base industrielle. Le critère de réussite sera l'apparition d'au moins trois licornes françaises dans le domaine comme nous avons su le faire il y a quelques années dans d'autres technologies clefs de l'informatique.

Pilote :

- Le Forum État-Industrie-Utilisateurs

4.2 Contribution aux autres projets structurants de la filière

Plusieurs projets décrits au sein des sections territoires de confiance, identité numérique et numérique de confiance nécessiteront des composantes cyber fortes. L'axe prévoit donc de contribuer à ces projets en y apportant les compétences cyber nécessaires. Les modalités précises de collaboration du projet cyber à ces autres projets structurants de la filière seront finalisées avec ceux-ci ultérieurement.

Concrètement les actions seront les suivantes :

- Collaborer à la conduite des projets en question
- Identifier les besoins en cyber et l'adéquation avec les briques disponibles
- Mener les développements nécessaires éventuels dans le cadre de projets collaboratifs
- Assurer la bonne implémentation des briques dans les projets

4.3 Développement de briques permettant d'assurer la cyber sécurité des infrastructures

Le Forum Etat/Industrie recueillera les besoins de l'État et des utilisateurs dans les différentes filières. Il définira alors collectivement les actions d'accompagnement requises et les briques technologiques nécessaires pour monter une offre adaptée. Celle-ci devra assurer la sécurité de bout en bout des infrastructures numériques en conformité avec les préconisations de la LPM, de la directive NIS notamment pour les Opérateurs d'Importance Vitale (OIV), et du RGPD. L'offre de Cloud à sécuriser est, elle, du ressort du projet structurant « Numérique de Confiance » qui puisera dans ces briques technologiques de confiance pour assurer la conformité.

L'identification des besoins pourra donner lieu à des propositions en matière de développements collaboratifs de projets d'innovation ou de plate-forme au niveau territorial, national et européen.

Il est aussi l'opportunité d'une coopération étroite entre les industriels petits et grands et l'Etat. En effet, la revue stratégique de cyberdéfense recommande, entre autres, de mettre en place une action qui consiste à analyser et faire émerger les technologies clés essentielles à la sauvegarde de

[4] Extrait de la revue stratégique de cyberdéfense, 12 février 2018

l'autonomie de la France dans le numérique. Ces technologies ont donc vocation à protéger les systèmes d'information sensibles, à savoir ceux des administrations et des opérateurs d'importance vitale.

De son côté, l'État formule des besoins, détaille les briques technologiques qui les sous-tendent et dresse une cartographie de l'existant. Les industriels complètent la cartographie des offres existantes. L'objectif final à court et moyen terme consiste à faire émerger une offre de confiance qui répond aux besoins essentiels sur propositions des industriels du secteur.

Plusieurs projets techniques et un projet de gouvernance cybersécurité ont d'ores et déjà été identifiés comme pertinents et sont susceptibles de faire l'objet d'appels à projets :

Agent de confiance

L'industrie souhaite faire émerger un EDR (Endpoint Detection and Response) souverain. Un EDR est complémentaire à l'approche par sondes souveraines et très lié à la cyber threat intelligence. Le besoin est urgent et le marché des EDR est considérable : porté par la baisse des performances des antivirus traditionnels face aux nouvelles menaces, le marché mondial des EDR est estimé à 1,3 milliards de dollars (source Marketsandmarkets). On peut donc extrapoler une taille de marché des EDR de plus de 300 millions de dollars pour l'Europe et de près de 50 millions pour la France (par application du ratio Gartner France / marché mondial). Le but est de développer un outil de détection performant, intégrable (SOAR/SIEM) et scalable, en capitalisant sur des initiatives Open Source (comme le préconise l'ANSSI).

Cyber Threat Intelligence

Le deuxième projet consiste à doter le pays et nos entreprises de capacité de détection de très bonne qualité en créant une communauté de confiance d'échange de données standardisées.

Leurrage

Le troisième projet est lié au précédent et concerne le leurrage. Le leurrage permet de renforcer les dispositifs de détection des attaques, d'étudier les comportements des attaquants et de leur faire perdre du temps. Complémentaire à la Threat Intel, il permettra d'ajouter une « longueur d'avance » aux SOC afin de pouvoir réagir rapidement. Couplés aux sondes, les dispositifs de leurrage se révèlent particulièrement efficaces.

Données de test

Le quatrième projet est la mise à disposition d'un ensemble de données (data set) public, pour constituer des benchmarks standards des outils du marché et constituer une base d'apprentissage pour différentes nouvelles technologies qui en ont besoin notamment le Machine Learning et l'Intelligence Artificielle.

Intégration et Interaction

Le projet de gouvernance consiste en la constitution de l'Initiative d'Intégration & d'Interaction Inter Produits « 4I », qui permet aux produits cyber français de fonctionner ensemble au travers de canaux de communication standardisés (API). Afin de favoriser cette initiative, il semble opportun de créer une enveloppe budgétaire progressive dédiée à l'émergence de projets communs, de faire vivre un catalogue et de faire émerger des offres intégrées.

Pilote : le Forum État-Industrie-Utilisateurs

4.4 Développement de solutions en surcouche applicative permettant d'assurer la souveraineté sur les données sur des infrastructures non contrôlées

L'accélération de l'adoption des cloud publics et privés associée à l'explosion de la génération des données par les systèmes industriels et les objets connectés génèrent de nouveaux risques et challenges pour les organisations soucieuses de la protection de leurs données : Perte de maitrise des

environnements les hébergeant, nouveaux modèles organisationnels, nouveaux modèles de business, interopérabilité, conformité réglementaire et exposition à des lois extraterritoriale…

Il devient impérieux de protéger nos systèmes face à de tels risques, en développant des technologies et solution de confiance permettant de protéger efficacement les données dans ce nouveau contexte.

Adresser ces enjeux repose sur trois axes prioritaires et complémentaires. Dans le cadre du contrat de filière, il est proposé de mettre en place des plateformes sur chacun de des 3 axes:

- Fournir une solution de protection des données de bout en bout en surcouche applicative supportant les environnements de cloud hybride tout en gardant la maitrise de la gestion des identités et du chiffrement en s'appuyant sur des technologies de confiance
- Développer une solution permettant le « transcodage » des données chiffrées et facilitant le passage d'un environnement sécurisé à un autre dans le respect de leurs niveaux de classification afin d'adresser les challenges technologiques du post-quantique et de l'interopérabilité des systèmes de chiffrement
- Adresser le challenge de la protection, de l'intégrité et de la traçabilité des accès aux données dans les environnements Big Data sur lesquelles s'appuient les systèmes IoT et les environnements industriels, grands générateurs de données.

Pilotes :

- État : ANSSI
- Industrie : Hexatrust

4.5 Cybersécurité des IOT au service de filières industrielles choisies

La diffusion de la cybersécurité dans l'ensemble des secteurs utilisateurs est un enjeu majeur pour permettre d'élever le niveau de protection global de notre pays. L'internet des objets qui est vecteur commun à de nombreux secteurs utilisateurs s'accompagne de nouvelles menaces mais représente également une opportunité de diffuser une culture et des solutions de cybersécurité adaptés à chacune des filières concernées.

La filière mènera des actions de sensibilisation auprès des autres filières pour que les aspects cyber soient pris en compte le plus en amont possible et fassent autant que possible appel à des solutions issues de son sein. Des contacts préliminaires ont été pris avec les filières mer, énergie, santé et infrastructures numériques

Le CNI et la DGE veilleront à ce que les autres filières fassent appel à la filière sécurité en tant que de besoin et l'intègre dans leurs projets le nécessitant. La filière s'engage à participer à tous les projets ainsi identifiés.

Pilotes :

- État : DGE
- Industrie : CICS

4.6 Investissements

Le développement d'une industrie puissante nécessite l'accès des entreprises au financement. Cet accès est souvent l'occasion pour des intérêts non souhaités de s'inviter dans les fleurons de notre industrie. Pour éviter que des entreprises stratégiques se retrouvent ainsi sous influence, il est nécessaire que l'Etat joue un rôle actif en tant qu'investisseur, en particulier lors de la phase de Capital Développement ou les tickets sont souvent relativement importants.

Concrètement, ce soutien prendra la forme d'un fonds souverain stratégique doté suffisamment pour pouvoir assurer en fonds propres ou quasi fonds propres la phase capital développement d'une dizaine de grosses PME ou d'ETI et les accompagner jusqu'à la sortie (industrielle ou en bourse). Ce fond pourra accueillir en son sein des investisseurs financiers (LP) amis pour augmenter son efficacité. Il aura a priori vocation à investir en tant que majoritaire ou au sein d'un bloc de contrôle majoritaire.

- État : DGE et BPI
- Industrie : Hexatrust

4.7 Fonds assurantiel

Par ailleurs le déploiement du numérique dans tous nos usages essentiels et vitaux s'accompagne de nouveaux risques face auxquels tous les utilisateurs ne sont pas également armés/ protégés. A titre d'illustration, 80% des PME ayant subi une attaque informatique et mal protégées risquent la disparition dans les deux ans qui suivent.

Les grandes entreprises et l'État ont des moyens et des ressources ce qui n'est pas le cas des 4 millions de TPE, PME et d'organisations qui sont soumises aux mêmes devoirs liés aux réglementations NIS et RGPD.

L'idée consiste à créer une couverture assurantielle du Risque IT pour tous, qui viendrait financer les dommages et la remédiation en cas d'incident. Pour explorer cette piste, l'État pourrait réunir les assureurs pour réfléchir à la création d'un tel fonds.

Engagements réciproques pour l'axe 4 :

Industrie :

- Renforcer, structurer et promouvoir le label France Cybersecurity
- Participer aux travaux des autres projets des autres axes de la filière
- Monter et cofinancer les projets fédérant l'industrie sur les briques identifiées
- Collaborer avec l'État pour l'analyse les besoins clefs identifiés dans le cadre de la revue stratégique de cyberdéfense
- Monter et cofinancer le projet de surcouche applicative
- Sensibiliser les autres filières industrielles au sujets cyber
- Identifier leurs besoins et y répondre
- Apporter la méthodologie et le support et les mettre en œuvre auprès des autres filières
- Participation capitalistique au fond d'investissement pour des scale ups à vocation européenne et mondial

État

- Soutenir le label France Cybersecurity
- Cofinancer les projets fédérant l'industrie sur les briques identifiées
- Faire du CSF le canal de diffusion des résultats et plans d'actions de la revue stratégique de cyberdéfense.
- Cofinancer le projet de surcouche applicative
- Soutenir la démarche vers les autres filières au niveau du CNI et réglementaire
- Inciter à un renforcement des dispositifs de financement de la cybersécurité :
    - En incitant les actionnaires du fonds deep tech issu du rapport Tibi à faire de la cybersécurité un secteur prioritaire du fonds
    - En étudiant la création d'un fonds sectoriel dédié.

AXE 5 : DEPLOYER DES ACTIONS STRUCTURANTES POUR L'ECOSYSTEME DANS LE CADRE DU CAMPUS CYBER

A l'heure où les cyberattaques sont susceptibles de porter atteinte aux intérêts vitaux de la Nation et de remettre en cause la soutenabilité des usages numériques, il est nécessaire d'organiser la montée en puissance des acteurs du numérique et de l'innovation sur les enjeux de cybersécurité.

D'autres pays ont fait le choix de politiques ambitieuses pour fédérer leurs écosystèmes nationaux dans le domaine de la cybersécurité. Israël, en particulier, le CyberSpark à Beer-Sheva, se distingue sur le plan international et constitue de ce point de vue un exemple inspirant.

Dans ce contexte, le Président de la République a souhaité qu'une dynamique soit engagée pour mettre en place un « campus cyber », porté par les acteurs industriels et fédérant l'écosystème français de cybersécurité. Dédié à la mise en œuvre de synergies, un tel projet devrait étroitement associer le monde académique et le secteur public.

Le Premier Ministre a ainsi adressé le 16 juillet 2019 une lettre de mission à Michel Van Den Berghe lui demandant d'étudier l'opportunité, la faisabilité, le périmètre souhaitable et les conditions de réussite de ce projet, notamment s'agissant de sa viabilité économique, sa gouvernance et de son financement.

L'initiative portée par le président de la République d'un campus dédié à la cybersécurité s'inscrit naturellement dans la filière. Une coordination étroite sera établie entre le campus et le CSF. Le CSF sera l'une des parties prenantes à la gouvernance du campus. Le campus, à vocation opérationnelle, pourra héberger les actions du CSF cohérentes avec les missions et objectifs qui auront été validées par le Premier ministre.

A titre d'illustration, le campus cyber pourrait être le socle d'actions du CSF, par exemple : héberger le forum État-industrie-utilisateurs, dispenser des formations pour former des opérateurs cyber, héberger un ensemble de données (data set) partagé entre les acteurs (type Boost Aerospace dans l'aéronautique) pour constituer une base d'apprentissage pour de nouvelles technologies...

Engagements réciproques pour l'axe 5 :

Industrie :

- Proposer des actions du contrat de filière pouvant être mises en œuvre au sein du campus cyber

État :

- Évaluer la pertinence et la faisabilité d'un campus cyber
- Assurer, le cas échéant, une étroite coordination entre le projet de campus cyber et le CSF

Projet structurant Cybersécurité et sécurité de l'IoT

Synthèse des engagements clés

Les industriels s'engagent à :

- **Mobiliser les organisations industrielles régionales autour de projets structurants**
- **Mettre en place un Forum État-Industries-Utilisateurs fédérant et pilotant la filière**
- **Installer deux centres de soutien « follow the sun »**
- **Renforcer, structurer et promouvoir le label France Cybersecurity**
- **Monter et cofinancer les projets fédérant l'industrie sur les briques identifiées**
- **A une participation capitalistique au fonds d'investissement pour des scale ups à vocation européenne et mondiale**

L'État s'engage à :

- **Mettre en place les conditions permettant de développer des formations courtes en cybersécurité**
- **Soutenir le Forum État-Industries-Utilisateurs et porter les positions coordonnées au sein du Forum vers l'Europe et les organisations internationales**
- **Soutenir le label France Cybersecurity**
- **Cofinancer les projets fédérant l'industrie sur les briques identifiées**
- **Soutenir le développement d'un salon de taille mondiale**
- **Inciter à un renforcement des dispositifs de financement de la cybersécurité**
    - **En incitant les actionnaires du fonds deep tech issu du rapport Tibi à faire de la cybersécurité un secteur prioritaire du fonds**
    - **En étudiant la création d'un fonds sectoriel dédié**

PROJET STRUCTURANT N°3 : IDENTITE NUMÉRIQUE

Clef de voute de l'économie numérique et de la protection des données personnelles, l'identité numérique constitue un formidable moteur de développement et de souveraineté. Le projet Identité numérique a l'ambition de répondre pleinement et durablement à ces enjeux et d'asseoir le leadership de l'industrie française en développant une offre de solutions innovantes, s'appuyant sur le déploiement rapide de la carte nationale d'identité électronique et portée par un écosystème national dynamique.

Contexte / thème :

1. Apporter une identité numérique de confiance, un enjeu clé

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 de l'ensemble des acteurs industriels de la filière identité numérique 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. Cette ambition doit être au service de l'inclusion, de l'accès aux droits, de la démocratie locale, et des usages actuels ou à venir liés au développement du numérique.

2. Développer un écosystème français de l'identité numérique

Le succès du déploiement de l'identité numérique à des fins publiques comme privées, de niveaux substantiels et élevés, adossée aux titres d'identité garantis et délivrés par l'État, dépend du développement d'un écosystème équilibré où la place et le rôle tant des acteurs privés que de l'État sont clairement définis. Notamment en vue de lever les freins du développement d'une offre de services la plus large et la plus innovante possible vers l'ensemble des utilisateurs (citoyens, résidents…).

Acteurs

Les catégories d'acteurs de l'identité numérique sont les suivantes

- Utilisateurs : personnes physique ou morales, caractérisées par des attributs d'identité univoques.
- Fournisseurs d'identité (FI) : entité publique ou privée mettant à disposition des utilisateurs un moyen d'identification électronique.
- Fournisseurs de services (FS) : entité publique ou privée, responsable d'un service en ligne dont l'accès nécessite une identification électronique de l'utilisateur
- Fédérateurs d'identité : entité publique ou privée capable de mettre à disposition de FS (publics et privés) une offre de plusieurs FI (publics et privés), et de plusieurs niveaux d'identité eIDAS et ceci en garantissant un point d'entrée unique à ces acteurs
- Fournisseurs de données (FD) : entité publique ou privée mettant à disposition des FS des données fiables sur la base des données pivots de l'utilisateur, et avec son consentement explicite

Usages

Le succès dépendra de la capacité à se focaliser sur les usages permettant un effet d'entrainement vis à vis du reste des acteurs. L'approche sectorielle pourrait être efficace, car plus à même de cerner le contexte dans lequel s'intègre l'identité numérique et de propager les bonnes pratiques au sein des fournisseurs de services du secteur. Parmi eux, ceux à traiter en priorité, se classent facilement en fonction de leurs obligations règlementaires (par exemple le domaine financier obligé de suivre les

directives AML4 ou DSP2), le volume de transactions potentielles, la récurrence d'usages, le besoin en sécurité et la valeur « ressentie » par l'utilisateur final. A titre d'exemples, les secteurs suivants sont particulièrement concernés : la finance, la santé, les assurances, les courriers recommandés électroniques, l'économie collaborative, les jeux en ligne.

Modèles économiques
Le modèle économique se doit d'être simple, équitable afin d'assurer les mêmes chances de succès entre tous les acteurs. En effet l'identification et le développement des usages et le recrutement des fournisseurs de services les mettant en œuvre ne suffiront peut-être pas à assurer le succès du déploiement de l'identité numérique.

Les travaux du CSF permettront d'alimenter les réflexions de l'État en vue de définir les conditions pour rendre cet écosystème viable, compréhensible et profitable pour tous les acteurs, en particulier :

- La coexistence des fournisseurs publics et privés d'identité numérique sans distorsion de concurrence, en particulier leur périmètre d'usage et les règles de tarification appliquées
- Le mécanisme de fixation des prix dans un contexte de coopération/compétition potentielle public-privé.
- Le rôle du fédérateur d'identité FranceConnect pour développer les usages, garantir l'interopérabilité des identités et promouvoir les offres d'identités substantielles et élevées et les évolutions qui pourraient être apportées au modèle actuel où FranceConnect assure le rôle d'interface utilisateur, vérificateur d'identités, fédérateur et connecteur des fournisseurs d'identité, ainsi que de l'authentification pour les services partenaires.
- Le choix entre trois modèles :
    - un modèle où le ou les fédérateurs d'identités ou une plateforme complémentaire se charge de réguler les prix, et les contrats,
    - un modèle où le ou les fédérateurs d'identités ou une plateforme complémentaire se charge de réguler les prix, les contrats, et les flux financiers entre FI et FS.
    - un modèle où le ou les fédérateurs d'identités fournissent les volumétries de transactions aux FI et FS mais ne régule pas les prix et ne gère pas les flux financiers entre FI et FS.

Il existe également un besoin avéré en termes de fourniture et d'échange d'attributs, autour de la notion du « dites-le nous une fois ». La combinaison de données d'origine diverse permettrait de simplifier et sécuriser les parcours (moyennant consentement explicite des clients-citoyens, naturellement). Le modèle économique associé à ces services sera précisé.

Encore faut-il que la mécanique sous-jacente permette à une offre de cette nature de se développer facilement et notamment donne aux FS la possibilité de trouver facilement les données dont ils ont besoin auprès des FD. Ce qui s'apparenterait à un mécanisme de « place de marché » des données.

D'autres moyens ou eServices tels que la signature qualifiée, l'horodatage, l'archivage ou le séquestre pourraient venir compléter l'offre de services des fournisseurs d'identité ou fournisseurs de données et enrichir les cas d'usages des fournisseurs de services.

Enfin, l'accompagnement et le conseil des citoyens dans l'utilisation de leur identité numérique est aussi un élément différenciant potentiel pour les FI : des offres diversifiées adaptées à chaque public pourraient laisser plus de place à l'innovation et à la création de valeur. Le secteur privé apparait le mieux armé pour s'adapter à la dynamique du marché et l'émergence de nouvelles technologies et supports numériques.

Pour toutes ces raisons, le développement rapide de l'offre des FI et FS privés sera clé afin de garantir une offre de services la plus large et la plus innovante possible vers les utilisateurs ; la stimulation de la demande par l'offre, et la sensibilisation des citoyens à la nécessité d'utiliser des services sécurisés, accélèrera l'innovation technologique et favorisera le développement de nouvelles solutions.

Objectifs :

Face à la menace de solutions d'identité numérique hégémoniques fournies par les grands acteurs mondiaux de l'internet, l'industrie veut, en concertation avec l'État, développer une offre française de l'identité numérique (briques technologiques, services d'identité numérique, relations avec les fournisseurs de services), qui s'appuie sur la dérivation de l'identité régalienne et se différencie des grands acteurs mondiaux par un haut niveau de protection des données personnelles. Cet objectif

sous-tend d'une part la croissance et l'emploi du segment, et d'autre part la souveraineté de l'économie numérique et le soutien de toute la filière de la sécurité du numérique.

Le projet structurant « Identité Numérique » a pour ambition de créer les conditions d'un développement rapide du déploiement et de l'utilisation de l'identité numérique en France, en développant les solutions technologiques, en facilitant les usages, en participant aux travaux sur l'environnement réglementaire, permettant d'apporter des solutions sécurisées et ergonomiques aux citoyens et de créer, consolider et faire rayonner des leaders industriels Français dans le domaine.

Pour assurer cet objectif, l'industrie vise essentiellement à :

- Aider l'État à déployer de la meilleure façon la carte nationale d'identité électronique, et les infrastructures associées. Pour cela, la filière contribue à l'élaboration des spécifications requises (contenu, interfaces, enrôlement, service de comparaison biométrique, gestion du cycle de vie ...).
- Aider l'État à proposer un parcours utilisateur simple en vue de développer les usages des identités numériques publiques et privées, en particulier assurer une bonne articulation avec FranceConnect et les éventuels autres fédérateurs qui pourront exercer leur activité sur des périmètres complémentaires à celui de FranceConnect.
- Développer et promouvoir des solutions d'identité numérique privée de niveau substantiel et/ou élevé et favoriser le dynamisme de l'écosystème associé.
- Définir, et soumettre à validation de l'ANSSI, les standards techniques (par exemple, des profils de protection) permettant de garantir que les solutions françaises auront un niveau de sécurité qui soit à la hauteur des enjeux.
- Assurer le développement international en garantissant l'interopérabilité des solutions entre elles et avec les solutions internationales, et en définissant ou adoptant des standards permettant de donner aux fournisseurs d'identité et de technologies de sécurité français une avance commerciale forte et un avantage concurrentiel sur le plan international.
- Soutenir l'innovation et ouvrir de nouveaux services et usages associés à l'identité numérique.

Ces objectifs seront atteints par la mise en œuvre d'un plan d'actions comportant des actions sectorielles et la mise en place des conditions de succès. **L'élément clé du projet est sa capacité à mettre d'accord les industriels autour d'une spécification technique, qui constitue d'ores et déjà un succès du CSF.**

Plan d'action :

Le plan d'actions s'articule autour des éléments suivants :

1. Actions techniques
    - Spécifications : participer à la conception de la CNIe comme un moyen permettant de prouver de manière sécurisée son identité en face à face, mais aussi via un réseau de communications électroniques. En particulier, cette confiance devra reposer sur la mise en œuvre d'un système d'information permettant d'assurer que les données d'identité figurant sur le titre (alphanumériques et biométriques) n'ont pas été altérées ou modifiées et qu'elles sont mises en œuvre par leur légitime détenteur.
    - Qualification technique et mise à disposition au meilleur prix des composants nécessaires à l'utilisation de l'identité numérique par les citoyens : par exemple lecteur de carte à puce, intergiciel ou extension de navigateur internet (pour ordinateur), application (pour téléphone mobile). Dans ce but,
        - Un catalogue d'offre capacitaire pour chacun de ces composants sera mis à disposition de l'État.
    - L'État et l'industrie viseront à adopter un seul intergiciel.
    - Lancer des pilotes de solutions d'identité numérique

- Favoriser le développement et l'offre par le secteur privé de solutions d'identités dérivées de la CNIe.

2. Actions pour développer les usages et le modèle économique : définir des secteurs d'activités pour l'usage de l'identité numérique
   - Animer des groupes de travail multisectoriels dans l'optique notamment de promouvoir et de valoriser l'identité numérique et ses services associés.
   - Par secteur d'activité, sur la base du dialogue avec les acteurs sectoriels :
     - Mesurer les attentes, comprendre leurs priorités, évaluer les aménagements règlementaires éventuels, identifier les cas d'usages moteurs et usuels, recenser les perspectives de transformation des usages et des bénéfices potentiels, évaluer les besoins en niveau de sécurité…, évaluer les gains et la valeur du / des services, identifier les éléments pouvant faciliter l'adhésion, ainsi que les freins et les mesures pour les contourner.
   - Tester, raffiner, finaliser les scénarios financiers possibles, avec les fournisseurs de services et d'identités, d'attributs, et de signatures.
   - Participer aux réflexions autour de la précision du modèle économique cible
   - Le CSF pourra contribuer à clarifier les besoins de niveau d'assurance d'identité numérique en fonction des usages en liaison avec l'État et l'ANSSI en particulier. Cette clarification pourrait permettre d'assurer une homogénéité des niveaux de confiance et de sécurité parmi tous les fournisseurs de service.
   - Développer des actions de communication conjointes État/Industriels importantes vis-à-vis des citoyens et des utilisateurs afin de favoriser une adoption rapide.

3. Actions pour le développement international de la filière et la promotion des normes et valeurs du schéma d'identification numérique français et européen
   - Participer aux instances de normalisation européenne et internationale
   - Construire des solutions enrichies de fonctionnalités, d'attributs, permettant de donner un avantage concurrentiel à la filière.

4. Actions pour accélérer l'innovation
   - Favoriser le développement et l'offre de solutions d'identité numérique permettant des fonctionnalités de pseudonymisation, de services innovants associés à l'identité numérique, de parcours utilisateurs fluides et simples, d'infrastructures et de techniques facilitant la délivrance, l'activation et l'usage de l'identité numérique
   - Explorer le potentiel de la blockchain.
   - Accompagner une stratégie de compagnon numérique des documents sur mobile, en complément des documents physiques
   - Explorer activement l'extension aux objets connectés

Livrables / calendrier (État – Industrie) :

- Spécifications de l'OS de la CNIE : 2019 (travaux engagés par anticipation)
- Cadre normatif : début 2020
- Première CNIE : mi 2021
- Pilote et premiers services d'identité numérique dérivés de la CNIe opérationnels : 2021
- Campagne de communication en soutien de la croissance vis à vis des utilisateurs et des fournisseurs de service : 2021
- Lancement de projets d'innovation : 2021

Pilotage :

Un comité de pilotage du projet de la filière est mis en place pour assurer son avancement et prendre les mesures correctives nécessaires si besoin.

Il sera également mis en place une instance partenariale public-privé de l'écosystème de l'identité numérique. Cette instance associera l'État et les acteurs privés, les fournisseurs de service (FS), les fournisseurs d'identité (FI) et le ou les fédérateurs d'identités publics et privés, des associations d'utilisateurs et les fournisseurs de technologies. Cette structure échangera sur les règles de gouvernance et les conditions de structuration et d'évolution de l'écosystème de l'identité numérique (règlementation, référentiels techniques…). Un groupe « Expérience Utilisateurs » pourra être mis en place en vue de l'amélioration continue des services et d'un développement d'offres nouvelles.

Participants :
Les acteurs suivants sont impliqués dans le projet : les industriels et acteurs associatifs de la filière, les fournisseurs d'identité, des représentants des fournisseurs de service, les autorités de certification, les représentants de l'État.

Engagements réciproques entre l'État et la filière :

1. **Engagements de l'industrie**
   - Participer à l'élaboration des spécifications de l'OS de la CNIe et de son intergiciel, et fédérer l'ensemble des acteurs, en accord avec les grands industriels
   - Conduire des études sectorielles en animant des groupes de travail avec les acteurs majeurs pour développer les usages et les conditions de succès
   - Contribuer à la clarification en liaison avec l'État et les fournisseurs de services des besoins de niveaux d'assurance d'identité numérique en fonction des usages
   - Mettre à disposition du plus grand nombre des solutions d'identité numérique de niveau élevé assurant un haut niveau d'ergonomie, de facilité d'utilisation et d'intégration.
   - Suivre les évolutions technologiques et favoriser le dialogue entre fournisseurs de services, opérateurs et industriels pour anticiper la R/D et co-construire l'offre technologique,
   - Conduire le changement auprès des décideurs publics et privés et des utilisateurs par la communication et la promotion
   - Favoriser le dialogue entre fournisseurs de services et industriels pour anticiper la R&D et co-construire l'offre
   - Développer des solutions et services enrichis permettant d'étendre les bénéfices et l'attractivité pour les utilisateurs d'une identité numérique substantielle ou élevée (attributs complémentaire, coffre-fort électronique, etc.)
   - Participer aux instances de normalisation pour soutenir les approches françaises
   - Construire rapidement des solutions permettant de viser directement le développement d'usages opérationnels à grande échelle et les mettre en service
   - Définir n (à préciser) pilotes et les lancer en concertation avec les acteurs publics nationaux et territoriaux
   - Développer des actions de sensibilisation et de communication
   - Définir et monter les projets d'innovation (pseudonymisation, blockchain, IoT, …)

2. **Engagements de l'État**
   - Déployer à partir de l'été 2021 une carte nationale d'identité électronique, dont les spécifications de l'OS seront définies en lien avec l'industrie ;
   - Poursuivre le déploiement de FranceConnect ;
   - Mettre en œuvre le nœud eIDAS FranceConnect (aux niveaux substantiel et élevé), afin de garantir l'interopérabilité des identités françaises vers les autres pays européens (et inversement).
   - Mettre en place les dispositifs permettant d'impliquer les entreprises dans la gouvernance de l'identité numérique ;

- Poursuivre les travaux normatifs liés à l'identification électronique sécurisée
- Promouvoir et soutenir la mise en place de premiers pilotes et d'expériences innovantes
- Contribuer au développement d'un écosystème de l'identité numérique de confiance :
    - En développant les usages publics requérant une identité numérique adaptée à l'évolution des risques et menaces
    - En garantissant pour l'usager la gratuité d'utilisation de l'identité numérique adossée à la CNIe
    - En permettant l'accès à la partie identité numérique de la CNIe aux fournisseurs d'identité privés afin qu'ils dérivent facilement leur identité
- Développer des actions de communication et de sensibilisation vis-à-vis des citoyens et des utilisateurs, en liaison avec l'ensemble des relais territoriaux et de médiation numérique (services déconcentrés de l'État, collectivités territoriales, associations, maisons France Service…), afin de favoriser une adoption rapide et inclusive de l'identité numérique.

Synthèse des engagements clés

Les industriels s'engagent à

- **définir une spécification unique de l'OS de la future CNIe,**
- **construire rapidement des solutions et services enrichis permettant de viser directement le développement d'usages opérationnels à grande échelle et les mettre en service**
- **développer des actions de sensibilisation et de communication vers les acteurs du secteur privé**

L'État s'engage à :

- **déployer la CNIE dès 2021**
- **poursuivre en 2020 les travaux normatifs assurant les conditions de succès de l'identité numérique publique et privée**
- **poursuivre le déploiement du fédérateur d'identité FranceConnect**

Modalités d'évaluation du projet :

Le succès du projet sera évalué en fonction des critères suivants :

- Volume de CNIe déployées en 2022
- Volume d'utilisateurs de FranceConnect
- Volume d'usages aux niveaux eIDAS substantiel et élevé
- Volume d'identités dérivées aux niveaux eIDAS substantiel et élevé
- Nombre de fournisseurs de services contribuant à cet écosystème

PROJET STRUCTURANT N°4 : TERRITOIRES DE CONFIANCE

La sécurité des personnes, des biens et maintenant des données, est un besoin au cœur des territoires de plus en plus intelligents, connectés et en pleine mutation. Le projet Territoires de confiance a pour ambition d'assurer un leadership français au travers de solutions globales pour les collectivités et les sites s'appuyant notamment sur :

- **le développement d'une offre de plateforme de services de confiance à destination des collectivités de toutes tailles,**
- **le déploiement de nouveaux usages adossés à des technologies de rupture.**

Le projet vise l'exemplarité en matière de traitement des données personnelles en établissant une charte éthique liant l'Industrie, l'État et les utilisateurs des technologies de sécurité.

Contexte & périmètre

La notion de territoires de confiance se comprend comme les moyens déployés pour assurer la sécurité de la ville intelligente (smart city), mais aussi des territoires intelligents, jusqu'aux aires portuaires et maritimes en particulier, y compris l'outremer. Les termes « territoires smart & safe », ou « territoires intelligents et sûrs » sont également utilisés dans le texte avec le même sens.

C'est un sujet clé aujourd'hui qui fédère tout le périmètre de la filière. En effet, il requiert le concours d'acteurs de la cybersécurité, de l'identité numérique ou encore des spécialistes de la biométrie, mais également de la sécurité physique ou électronique, puisqu'il est question de sécuriser toute une ville, bâtie entre autres sur les technologies du numérique. Un périmètre aussi large représente un marché potentiel très important.

Les territoires connaissent des mutations profondes induites par de nouvelles approches conceptuelles (smart city, résilience) et par la transformation numérique. Une économie nouvelle se développe rapidement autour des données et des nouveaux usages. A une demande de services plus globaux s'ajoutent des enjeux de compétitivité et de souveraineté. Dans ce contexte, la sécurité des villes et des territoires intelligents, s'inscrit comme un élément essentiel à maîtriser pour garantir la tranquillité, la résilience et l'attractivité des territoires. La protection de l'ensemble des données et leur utilisation pertinente ne peuvent se faire qu'en appliquant les principes de sécurité dès la conception des produits et services. C'est la notion de privacy and security by design.

Par ailleurs, le potentiel des technologies de sécurité évolue très rapidement et l'objectif est donc de développer des solutions globales, flexibles et innovantes en matière de sécurité des territoires intelligents, qui exploitent ce fort potentiel et qui hisseront l'industrie française au rang de leader mondial du domaine d'ici 2025. A cette fin, l'association du numérique et de l'humain dans les solutions proposées apparaît comme un élément de différenciation à cultiver.

Le projet associe des collectivités partenaires qui ont déjà officialisé leur concours : région Grand Est, ville de Nice et métropole Nice Côte d'Azur, métropole de Rennes, métropole de Lyon, métropole de Lille, métropole de Chartres, Syndicat d'électrification de la Loire et est bien sûr ouvert aux collectivités se joignant à la démarche ultérieurement. Il invitera les porteurs d'initiatives concourantes, tels que Security System Valley et le pôle d'excellence européen pour sécurité globale (PESG). Le GICAT apporte un soutien opérationnel à l'ensemble du projet.

AXE 1 : DESSINER LA TRANSITION VERS LES TERRITOIRES INTELLIGENTS ET SECURISES

Faire émerger les besoins et les usages soutenant la transformation des territoires intelligents et sécurisés

Contexte : Les perspectives de développements portées par les métropoles et les territoires embrassant les concepts de smart et safe city sont extrêmement larges. Les métropoles et les industriels français, voire européens, de la sécurité doivent donc nouer un dialogue étroit afin de s'entendre sur une vision partagée tournée vers un développement économique compétitif. Le périmètre envisagé comprend la sécurité de façon générale, y compris les infrastructures et la cybersécurité, en synergie avec les autres capacités de la smart city (mobilité, gestion de l'énergie, etc.) pour offrir une palette de services sécurisés valorisant l'ensemble des données. Ce dialogue doit également s'étendre aux opérateurs privés devant sécuriser leurs activités sur les territoires.

Objectifs : Définir avec les collectivités et les opérateurs du territoire une vision partagée de la ville et des territoires intelligents et sécurisés (vision multi-sectorielle, multi-acteurs – incluant les citoyens et favorisant la security & privacy by design, prise en compte du rapport Thourot-Fauvergue). Cet objectif se décline comme suit :

- Identifier les drivers en termes d'usages et de besoins qui permettent de définir un socle de capacités et de principes pouvant être promu comme modèle ou standard[5]
- Identifier les concepts et capacités à expérimenter en priorité.

Actions prévues

- Monter et animer un groupe de travail en partenariat entre la filière et des collectivités et acteurs représentatifs, notamment les ministères concernés et la ville de Nice (pilote du 13ème partenariat sur la sécurité dans le cadre de l'agenda urbain de l'UE). Associer aux travaux de ce groupe les citoyens, les associations, les acteurs de l'enseignement et de la recherche, etc.
- Animer un groupe spécifique cyber et mobilité (constitué autour de la métropole de Rennes),
- Suivre et valoriser le démonstrateur « Safe city Projet » en cours à La Défense et à Nice,
- Suivre les projets de coordination de la sécurisation des territoires portuaires (Le Havre, Marseille, Toulon, Dunkerque, etc.) ou d'espaces (en liaison avec le projet fédérateur de la Smart offshore industry de la filière des industriels de la mer).

Livrables et calendrier :

- Constitution du groupe public-privé en partenariat avec les métropoles partenaires (2020)
- Vision documentée d'un socle de capacités et d'usages clés des territoires smart & safe (2021)
- Définition public-privé et pluridisciplinaire des capacités prioritaires et d'un programme d'expérimentation (2021)
- Programme de valorisation des résultats finaux du démonstrateur Safe city (pilote Thales)
- Identification de nouveaux projets de sécurisation de territoires
- Spécification d'un centre de coordination Cyber des ports maritimes (2020) (pilote : GICAN)

Participants et pilotage :

- Pilote : Thales, co-pilote AN2V
- Participants : panel d'industriels de la filière, collectivités partenaires (métropoles, villes, départements, ports, etc.), SGDSN, ministères (Intérieur, MTES, économie/DGE), pôles de compétitivité, groupements, ainsi que des acteurs innovants du secteur de la sécurité et de la cybersécurité.

[5] Les thèmes d'échanges pourraient être tels que les suivants :

- Témoignage de villes sur l'apport des technologies en terme de gain opérationnel (Dijon : retour poste de commandement unique: police, vidéosurveillance, sécurité, circulation et neige, Rennes avec le City Information Modeling , notamment sur les algorithmes prédictifs , Nice sur la reconnaissance faciale et le Piave Safe city, Marseille et sa plateforme LIVIN …)
- « En quoi les objets connectés (IoT) , le développement de la 5G et les plateformes de sécurité sont des opportunités pour une politique de territoire de confiance»
- « Le citoyen acteur de sa sécurité grâce demain au edge computing»
- « L'imbrication entre sécurité locale et sécurité nationale »

Engagements réciproques :

1. **Engagements de l'industrie**
   - Monter et animer un groupe de travail en partenariat entre la filière et des collectivités
   - Doter la filière d'une charte éthique partagée entre industrie et utilisateurs (pilote CICS)
   - Soutenir l'interopérabilité de projets globaux et en coordonner le développement
   - Documenter les actions menées

2. **Engagements de l'État et des collectivités**
   - Afficher la volonté de l'État et sensibiliser les territoires sur l'importance de la sécurité et la souveraineté des territoires intelligents (DGE)
   - Contribution à l'analyse du besoin via la mobilisation d'acteurs publics : ministère de la Cohésion des territoires et des Relations avec les collectivités, ministère de l'intérieur, SGDSN, SGMer, associations d'élus, etc.
   - Engagement de plusieurs collectivités phares dans l'action (notamment Nice, Lille, Lyon, Rennes, Chartres, SEL42)
   - Concours de l'État et des collectivités pour communiquer sur l'action et ses enjeux, dans un cadre national et européen

AXE 2 : DEVELOPPER UNE OFFRE DE SERVICES DE CONFIANCE POUR LES TERRITOIRES INTELLIGENTS

Développer les architectures et modèles de plates formes de services en mode agile avec des collectivités ou des territoires.

Cet axe sera mis en œuvre en coordination et synergie avec le projet « Construire les Smart Territoires » de la filière Infrastructures du numérique et avec le projet « Cybersécurité et sécurité de l'IoT ».

Thème : « La France, les villes et collectivités, incubateurs des territoires de confiance de demain ».
Pour répondre au besoin des collectivités en recherche de services numériques de confiance dans le cadre d'une démarche « Smart & Safe » et d'outils et services évolutifs et adaptés à l'architecture et aux besoins de la ville et du territoire de demain et de leurs citoyens (communication, mobilité, IA, IoT, doubles numériques), les partenaires visent le développement expérimental d'une approche globale, standardisée et interopérable, sur un ou plusieurs territoires représentatifs.

Objectifs :

1) Proposer aux collectivités un cadre facilitant la maitrise de leurs données et services, leur assurant « security & privacy by design » et garantissant les données et services des territoires smart & safe. Développer une offre globale de sécurisation des données et de services résilients[6] s'appuyant sur des plateformes distribuées de services de confiance tirant parti de toutes les données disponibles et assurant la sécurité de ces dernières. Ces plateformes de confiance permettront d'offrir des capacités multiservices et multiutilisateurs intégrant la gouvernance des données.

2) Développer et expérimenter les modèles d'architecture, les briques fonctionnelles, les produits et services mettant en œuvre l'approche ci-dessus. Les services développés et expérimentés s'adresseront aux acteurs et opérateurs locaux publics et privés mais également aux citoyens. A cet effet, une bibliothèque d'applications / de services de confiance sera mise en place. L'approche implémentée devra permettre de mutualiser des capacités entre des villes et/ou territoires.

[6] Par exemple : vidéo protection intelligente, services IoT de confiance, services de supervision / hypervision, services collaboratifs multimédia de confiance, applications citoyennes, etc.)

3) Monter un projet de démonstration ou de déploiement de plateformes et services sur au moins 2 bassins représentatifs (ville, métropole ou territoire) pour assurer la généricité de la démarche.
4) Développer des partenariats public-privés autours des technologies de l'IOT et de la mise en œuvre de solutions interopérables et de services innovants entre les communautés territoriales et les opérateurs privés (en particulier les OIV) dans le cadre de la protection des personnes, des infrastructures ou du patrimoine (mutualisation de réseaux de capteurs, services de surveillance communs.).

Ces objectifs seront poursuivis à travers : a) l'exploitation des travaux de l'axe 1 et des projets en cours (villes et territoires ruraux), b) l'élaboration de schémas directeurs dans des collectivités pilotes en co-design avec la filière, c) des projets d'expérimentation et de déploiement, d) de la communication. L'utilité d'un label sera explorée. Les travaux seront conduits en prenant en compte les perspectives des marchés européens et export.

Participants et pilotage :

- Pilotes : Airbus + Thales
- Participants : industriels de la filière, collectivités partenaires, ministères (Intérieur, MTES, économie/DGE, SGDSN …), ARF (à confirmer)

Un comité de pilotage assurera la gouvernance de l'approche de plateforme, incluant l'interaction entre usages et contenu. Ce comité de pilotage s'assurera qu'une collaboration est mise en place avec d'autres projets de la filière (Cybersécurité et sécurité de l'IoT, Numérique de confiance) et avec le projet « Construire les Smart Territoires » de la filière Infrastructures du numérique.

Livrables et calendrier :

- Proposition de modèles d'architecture et de plateforme de services : 2021
- Montage, développement d'un projet 2021-2022
    - Déploiement et expérimentation sur un première collectivité (début 2022)
    - Déploiement et expérimentation sur un deuxième collectivité (fin 2022)
- Mise à disposition d'une offre de plateforme de services validée par les expérimentations (2023)

Engagements réciproques :

1. **Engagements de l'industrie**
    - Fédérer les acteurs industriels français (grands groupes, PME, start-ups) pour proposer les principes d'une offre globale, la développer et la démontrer
    - Travailler étroitement et de manière « agile » avec les territoires partenaires pour assurer l'adéquation de la proposition avec les besoins
    - Identifier et monter des projets d'innovation si nécessaire
    - Mobiliser des ressources pour la réalisation des points précédents

2. **Engagements de l'État et des collectivités**
    - Mobiliser des financements et des ressources l'État et des collectivités (régions, métropoles, villes, etc.) pour lancer un ou plusieurs projets coopératifs de ce type
    - Mettre le territoire, ses données, ses expertises métier à disposition pour expérimenter les solutions
    - Déployer les solutions si elles répondent au besoin ou schéma directeur du territoire et sont éligible vis à vis du droit
    - Contribuer au rayonnement des solutions validées (éventuellement labellisées), notamment en ouvrant une tribune à la filière dans le cadre d'événements organisés par les territoires
    - Aider à explorer la levée des freins légaux et réglementaires

AXE 3 : ACCELERER L'EMERGENCE ET L'EXPERIMENTATION DE NOUVEAUX USAGES GRACE AUX RUPTURES TECHNOLOGIQUES

Développer les architectures et modèles de plates formes de services en mode agile avec des collectivités ou des territoires.

Contexte : De nombreuses collectivités ont déjà mis en place ou prévoient de mettre en place des programmes d'innovation et d'expérimentation autour de nouveaux usages permis, entre autres, par la mobilité, la connectivité, l'IA, l'internet des objets / 5G, les applications pour les citoyens.

Objectifs :

Aider ces collectivités à accélérer, sur la base de leurs besoins, l'émergence de projets de co-innovation entre l'Industrie et les territoires pour expérimenter et développer ensemble des usages innovants à un horizon de déploiement de 3 à 5 ans. Des exemples de tels usages peuvent être le partage instantané de video avec un PC pour guider les agents, le développement d'interactions entre policier et objets connectés.

Une démarche de co-innovation s'appuie sur des engagements réciproques de l'Industrie et des collectivités par :

- la mise en commun de moyens et ressources,
- la définition de cadres d'expérimentation,
- la mise en place de moyens technologiques,
- La participation d'un écosystème de partenaires.

Cet axe de travail s'appuiera entre autres sur les actions conduites dans le cadre du démonstrateur Safe city (2018-2021). Il comporte les étapes principales suivantes :

- Définition conjointe entre l'Industrie et des représentants des territoires d'un cadre de co-innovation applicables pour tous les acteurs intéressés par la démarche,
- Proposition par les acteurs des territoires de sujets d'expérimentations permettant de répondre à un usage précis et susceptible de pouvoir être répliqué dans plusieurs collectivités,
- Sélection par l'Industrie et les territoires des premiers sujets retenus pour ces démarches de co-innovation,
- Association à chaque démarche de partenaires territoriaux, d'acteurs de la recherche et de l'enseignement, de collèges de citoyens, d'associations,
- Adossement à des hubs existants et/ou création d'un ou plusieurs hubs,
- Échanges, communication et promotion des résultats.

Livrables :

- Cadre de co-innovation et d'expérimentation entre l'Industrie et les territoires
- Identification des premiers sujets retenus sur la base de propositions émanant des territoires
- Communication sur au moins trois nouveaux usages majeurs expérimentés et validés issus de ces programmes de co-innovation

Calendrier :

- Mars 2020 : Mise en place d'une gouvernance commune Industrie/Territoires et définition du cadre de co-innovation
- Septembre 2020 : Sélection des sujets retenus pour les premières démarches de co-innovation (3 minimum) et mise en place du cadre de co-innovation
- Mars 2021 : Démarrage des projets
- Jusqu'en septembre 2023 : Réalisation des projets dont la mise en œuvre sur les territoires
- Septembre 2023 : Bilan, communication,
- Suite : décision de lancer une deuxième vague de sujets

Participants et pilotage :

- Pilotes : Orange, Thales
- Participants : industriels de la filière et collectivités partenaires, *ARF (à confirmer)*

En lien avec le groupe cyber de la filière, la dimension cybersécurité, appliquée aux spécificités des projets menés avec les collectivités, sera prise en compte et décrite.

Engagements réciproques :

1. **Engagements de l'industrie**
   - Assurer la gouvernance et mettre en place les ressources et les moyens pour garantir le succès d'au moins trois projets de co-innovation et d'expérimentation
   - Apporter son expertise méthodologique pour la mise en place du cadre de co-innovation
   - Ouvrir l'accès à ses centres de R&D et à son écosystème de start-ups et partenaires
   - Construire des solutions ayant vocation à être industrialisées si l'expérience terrain est probante.

2. **Engagements de l'État et des collectivités**
   - Identifier des collectivités pilotes participant à la gouvernance de cet axe de travail
   - Apporter les sujets de co-innovation et participer avec la filière à la sélection des premiers projets
   - Mobiliser des moyens au niveau local pour apporter l'expertise « terrain » et le cadre d'expérimentation
   - Mobiliser des financements R&I (État, régions) permettant de contribuer à ces expérimentations, notamment pour rémunérer tout ou partie du travail des PME et Start-Up
   - Promouvoir et communiquer autour des usages émergeants

AXE 4 : PROTEGER LES INFRASTRUCTURES A L'ERE DU NUMÉRIQUE

Thème :

Cet axe concerne la protection des infrastructures et des sites au sens large, qu'il s'agisse d'entités sensibles soumis à des exigeantes accrues, d'établissements recevant du public, etc. Cette protection dépasse la dimension interne et comprend les interfaces avec le territoire.

Contexte :

Dans l'ensemble des secteurs d'activité, les infrastructures et les sites font non seulement face à des malveillances et des menaces physiques de plus en plus importantes, mais leur vulnérabilité est également accrue par les failles véhiculées par le numérique et ses usages. Ces infrastructures (sensibles ou non) utilisent, en effet, de plus en plus des solutions denses et évolutives reposant sur les technologies issues du numérique (IA, IoT, cloud, services, géolocalisation, etc.). De plus, les contraintes d'exploitation des sites et la diversité des activités qui y sont exercées peuvent poser des difficultés aigües.

Objectifs :

L'objectif est de développer pour l'ensemble des secteurs d'activités une offre globale en réponse à des situations complexes et hétérogènes, souvent le fruit d'actions malveillantes combinées physiques & cyber. Dans ce cadre, une expérimentation va se dérouler avec le secteur de la santé, dont les résultats devront pouvoir bénéficier à l'ensemble des secteurs d'activités. Cet objectif initial est fixé en partenariat avec le SGDSN et le ministère des solidarités et de la santé, au titre de sa politique de protection des établissements de santé et de sa volonté de donner de la visibilité à la filière et de contribuer à sa promotion.

L'objectif est poursuivi en suivant deux lignes clés développées particulièrement pour la protection des établissements de santé :

- **Contribuer à l'analyse des besoins sécuritaires des utilisateurs et à l'identification des réponses appropriées** :
    - Conduire un dialogue entre l'industrie, l'État et les opérateurs notamment du milieu santé pour diffuser les informations et mieux développer les réponses et méthodologies appropriées (définition des bonnes pratiques, approches cyber-physique, réponses globales, security by design, approches combinées sécurité-sureté, interopérabilité et standardisation, traitement des menaces hybrides, simulations, exercices…)
    - Faire la promotion des bonnes pratiques et des solutions techniques qui pourraient y être associées pour les établissements de santé comme pour les autres secteurs d'activités (y compris le domaine portuaire en fédérant l'action des acteurs territoriaux).
    - S'appuyer sur les recommandations du projet européen H2020 - SAFECARE, qui propose d'uniformiser le modèle de sécurité des services de santé pour mieux protéger les patients et les personnels face aux attaques physiques ou cyber (membres français du consortium : AP-HM, Airbus Cybersecurity, OBS/Enovacom, Santé Publique France, MININT).
- **Développer et expérimenter des solutions innovantes et adaptées aux établissements de santé, pouvant ensuite être déclinées dans les structures d'autres secteurs d'activités.** Cette action s'appuiera sur le potentiel de travailler à la protection de projets de nouveaux établissements de santé et comprendra :
    - Le lancement d'un projet d'envergure pour la protection d'un (nouvel) établissement de santé visant à assurer une approche globale, capable de passage à l'échelle, interopérable et réplicable, répondant aux bonnes pratiques. Ce projet permettra si possible (véhicule contractuel approprié) de couvrir à la fois le développement et l'acquisition ;
    - L'identification en parallèle de sujets pour des projets innovants ciblés (supervision/hypervision avancée, analyse prédictive, etc.).

Livrables et calendrier :

- Constitution du groupe Industrie-État-Utilisateurs (2020) / documents donnant les résultats des travaux (2020 à 2022)
- Guide(s) sectoriel(s), guide des bonnes pratiques et catalogue(s) décrivant l'offre en matière de protection :
    - Guide et catalogue pour les établissements de santé (2020),
    - Une solution concrète dans chaque fonction concourant à la sûreté, étude ou réalisation, selon ce qui est disponible,
    - Référentiel permettant de déterminer un « niveau de performance de sécurité » standardisé pour chaque site
- Définition et lancement d'un projet de développement de la protection d'un (nouvel) établissement de santé majeur (2020 ou 2021)

Participants et pilotage :

Pilotes : Airbus[7] + Bertin

[7] Leader industriel de l'étude H2020 SafeCare.

Participants : industriels de la filière, acteurs du bâtiment, SDGSN, SGMER, ministères (MSS, MTES), utilisateurs (opérateurs de santé*).*

Engagements réciproques :

1. **Engagements de l'industrie**
   - Animer un dialogue stratégique au sein du groupe projet
   - Structurer et décrire l'offre au regard des solutions techniques associées aux besoins de sécurité (sur le modèle de l'action conduite par le CICS pour la protection des sites SEVESO de 2016 à 2018)
   - Réaliser les études, monter, cofinancer et conduire le projet de développement et d'expérimentation
   - Projet de protection d'un établissement de santé majeur : faire les études préliminaires et réaliser le projet en coopération avec l'opérateur

2. **Engagements de l'État et des collectivités**
   - S'investir dans le dialogue, faciliter le dialogue entre industrie et opérateurs
   - Soutenir un projet de développement et d'expérimentation de la protection d'un nouvel établissement de santé
   - Soutenir la démarche de projet de protection d'un (nouvel) établissement de santé majeur (retenir le(s) sites)
   - Faciliter la communication sur l'offre capacitaire auprès des établissements de santé, en tenant compte du caractère innovant et évolutif des différentes technologies
   - Proposer des sites pilotes pour les études et les expérimentations éventuelles, en lien avec les projets
   - Promotion des bonnes pratiques et solutions vers d'autres secteurs d'importance vitale ou sensibles (SGDSN)

AXE 5 : FACILITER LE DEPLOIEMENT DES TERRITOIRES INTELLIGENTS ET SURS

Contexte :

Le marché des territoires intelligents et sécurisés est en émergence et fait face à de nombreux **freins** ou écueils. Il manque en même temps de d'ambition et de réalisme pour l'ensemble des **accélérateurs** envisageables.

Objectifs :

Comprendre, orienter et faciliter l'offre (les industriels) et la demande (les territoires) et déployer des actions pour adresser efficacement tous les projets. Cet objectif sera poursuivi à travers un travail sur les freins et accélérateurs selon 3 aspects :

1. Volets capacitaires : stratégique, organisationnel, technique, juridique et réglementaire, financier, éthique (6 volets)
2. Besoins : étude & segmentation des besoins pour a) ville / hypercentre, b) métropoles dont les banlieues, c) ruralité en s'inspirant de l'exemple l'initiative des blocs communaux, et aussi des territoires ruraux via les départements (ADF) : Yvelines, Oise, Var, Alpes Maritimes (3 segments)
3. Acteurs (3 types d'acteurs) :
   a) L'offre : les industriels (besoin de vision à 15 ans, de continuité au-delà des mandats électifs)
   b) La demande : les territoires (avec les cycles des élections, de la compétitivité territoriale)

c) Les administrations (Ministères : intérieur, écologie, transport, éducation…, CNIL, forces de l'ordre, syndicats…)

Livrables et calendrier :

- Rapport d'analyse croisant les 3 aspects ci-dessus : échelonné de 2020 à 2022
- Livrables dérivés
  - Cahier de propositions argumentées d'évolutions légales et réglementaires : 2021
  - Kit pour les collectivités (guide, livre blanc, outils, programme de sensibilisation, formation des élus, ROI, etc.) : 2022
  - Définition de scénarios et « use case » envisageables pour les 10 prochaines années : 2021
- Étude de marché dont cartographie des acteurs et des solutions en regard des dimensions d'innovation et de souveraineté Française et Européenne : 2021

Participants et pilotage :

- Pilotes : AN2V, Luceor
- Participants : panel d'industriels de la filière, collectivités partenaires, ministères (Intérieur, MCT, …), ARF (à confirmer)

Engagements réciproques :

1. **Engagements de l'industrie**
   - Fournir un rapport d'analyse des freins et accélérateurs du marché (2020 à 2022)
   - Fournir un cahier de propositions argumentées d'évolutions légales et réglementaires : 2021
   - Réaliser une étude de marché dont cartographie des acteurs et des solutions

2. **Engagements de l'État et des collectivités**
   - Étudier l'allocation d'un fonds additionnel de type FIPD pour aider des capacités liées au projet
   - Soutenir le label créé par la filière
   - Soutenir les évolutions législatives et réglementaires proposées
   - Communiquer et sensibiliser, comme en particulier dans le cadre de la European Cyber Week.

Synthèse des engagements clés	
L'industrie s'engage à :	- **Établir une charte éthique sur l'utilisation des technologies de sécurité** - **Fédérer les acteurs industriels pour proposer les principes d'une offre globale pour les données et services de sécurité des territoires, la développer et la démontrer** - **Expérimenter et valider au moins trois nouveaux usages clés en co-innovation avec les territoires** - **Lancer un projet de protection de nouvel établissement de sante en collaboration avec le ministère de la santé**
L'État s'engage à :	- **Sensibiliser les territoires sur l'importance de la sécurité et la souveraineté des territoires intelligents** - **Soutenir le lancement de deux projets de démonstration (territoire urbain et site de santé)** - **Contribuer au rayonnement et à l'adoption des solutions résultant du projet** - **Soutenir les évolutions législatives et réglementaires identifiées par le projet pour faciliter le déploiement des territoires intelligents et sûrs**

PROJET STRUCTURANT N°5 : NUMERIQUE DE CONFIANCE

Le numérique de confiance vise à structurer des offres industrielles de confiance compétitives pour répondre aux besoins des entreprises et de la puissance publique dans le numérique. Le cloud est le premier besoin identifié. Pour le satisfaire, la filière a tracé une feuille de route :

- **Définir une stratégie d'utilisation du cloud suivant la sensibilité des données**
- **Proposer des offres compétitives qualifiées cloud de confiance**
- **Mettre en place des dispositions renforçant la réversibilité, la portabilité et la transparence dans le cloud.**

Le numérique est devenu central dans la vie sociale et économique. Le pouvoir donné par la maitrise du numérique est significatif et la dépendance qu'il peut induire très profonde. Il est donc essentiel que la France et l'Europe déterminent les domaines où la dépendance à des savoirs ou des capacités étrangères est critique et mette en place les actions pour renforcer d'une part, la compétitivité de nos entreprises et, d'autre part l'autonomie stratégique de la France et de l'Europe. Tel est l'objectif du projet structurant « Numérique de confiance » : structurer des offres industrielles de confiance compétitives pour répondre aux besoins des entreprises et de la puissance publique dans le numérique.

Le premier objectif de ce projet est de définir entre la filière et l'État les axes sur lesquels des objectifs de souveraineté nationale ou européenne liant numérique et sécurité doivent être fixés. Le projet vise donc d'une part, à définir ces axes, à expliciter quelle nature de maîtrise ou de confiance est recherchée et, d'autre part, à conduire les actions correspondant aux objectifs fixés tout en répondant aux besoins de compétitivité des entreprises et de la puissance publique.

Un premier axe concernant le cloud de confiance a été retenu. Le projet a vocation à être complété par d'autres axes par la suite.

AXE 1 : STRUCTURER UNE OFFRE FRANÇAISE ET EUROPÉENNE COMPÉTITIVE DE CLOUD DE CONFIANCE

Contexte :
Le cloud peut être défini comme un modèle de gestion informatique permettant l'accès via un réseau à des ressources informatiques partagées et configurables. Les prestataires de services cloud fournissent différents services habituellement classés en trois types d'activité : infrastructure en tant que service (IaaS), plateforme en tant que service (PaaS) et logiciel en tant que service (SaaS).

La numérisation des entreprises a entrainé depuis quelques années un recours massif aux offres cloud. En permettant l'accès instantané à des infrastructures ou à des services numériques, de plus en plus complexes, le cloud permet des gains importants d'efficacité à la fois par une diminution des coûts, par une plus grande agilité dans l'utilisation des ressources informatiques et par une capacité accrue de développement de nouveaux services innovants.

Le cloud est aujourd'hui un vecteur d'efficacité, de compétitivité et d'innovation aussi bien pour l'action publique que pour les entreprises. Cependant, une entreprise utilisatrice de services de cloud accepte, parfois sans en être consciente, d'être en partie dépendante techniquement du fournisseur de service (notamment de ses capacités en matière de sécurité). Il est donc important de créer un cadre permettant une adoption du cloud par les utilisateurs dans un cadre de confiance.

Le marché mondial cloud et des services associés représente 440 milliards d'euros en 2018 et fait l'objet d'investissements importants de la part de toutes les grandes puissances mondiales, chacune

ayant compris son intérêt pour le développement de son économie numérique. La maîtrise technologique européenne du cloud relève donc d'un enjeu d'autonomie stratégique mais également de compétitivité internationale des entreprises européennes. Il convient donc de proposer les moyens concrets permettant de répondre aux besoins fonctionnels et de sécurité des entreprises pour le stockage et le traitement de leurs données sensibles.

Il y donc un équilibre à trouver entre les besoins de sécurité (technique et juridique) des entreprises et les solutions cloud existantes qui doit ainsi permettre aux entreprises utilisatrices mais aussi aux entités publiques de tirer pleinement profit des technologies cloud dans un marché de confiance.

La première condition de notre souveraineté numérique et de cette protection, c'est de disposer d'une capacité suffisante d'hébergement et de traitement de données pour lesquels les besoins s'accroissent avec la révolution numérique en cours. La seconde condition, c'est de sécuriser techniquement et juridiquement ces données, dans un cadre maîtrisé.

Objectifs :
Forte de ce constat, la filière nationale doit contribuer à favoriser la confiance dans le cloud qui permettra de contribuer plus largement à la numérisation des entreprises et leur compétitivité dans un cadre maitrisé. Au-delà de la confiance de cette offre, la filière française se doit également de proposer des offres cloud compétitives répondant aux besoins des entreprises et de la puissance publique.

L'objectif général est de permettre à une offre de cloud de confiance compétitive de se déployer et de mettre à la portée des entreprises des solutions qui répondent à des besoins particuliers de protection de leurs données sensibles. Cette offre contribuera à l'autonomie numérique française et européenne et à la maitrise du cloud suivant la sensibilité des données.

Les actions :

Priorité 1 – Définir une stratégie d'utilisation du cloud suivant la sensibilité des données

La filière participera activement aux réflexions engagées par l'État dans la définition des données sensibles. Ces réflexions permettront d'aboutir à une doctrine claire sur la valeur des données et sur la nécessité de favoriser le recours à des offres cloud de confiance en fonction de la sensibilité de celles-ci. Des actions de communication conjointes entre l'État et la filière seront menées pour sensibiliser les utilisateurs aux avantages du cloud, ainsi qu'aux enjeux de sécurité liés son usage, notamment concernant les risques sur les données.

Priorité 2 – Développement de la confiance dans le cloud

Le développement de la confiance dans le cloud passe notamment par l'application d'un certain nombre d'exigences techniques et juridiques sur les offres de fournisseurs cloud. Celles-ci seront basées sur les travaux menés par l'ANSSI, l'autorité nationale en matière de sécurité et de défense des systèmes d'information. La filière aura pour objectifs de proposer suffisamment d'offres cloud répondant aux exigences définies et répondant aux besoins des entreprises et de la puissance publique.

Priorité 3 - Structurer et renforcer l'offre cloud de confiance française

Au-delà de la confiance qu'apportera cette offre cloud de confiance française, il est primordial qu'elle soit compétitive et réponde à l'ensemble des besoins des entreprises et des acteurs publics. La filière, avec le soutien de l'État, devra concentrer ses efforts notamment sur les couches plateformes et applicatives. Des partenariats pourraient être aussi développés entre acteurs pour couvrir l'ensemble des fonctionnalités nécessaires aux entreprises.

Priorité 4 – Limiter les effets de verrouillage et renforcer la réversibilité, la portabilité et la transparence dans le cloud

L'ouverture est un élément essentiel pour les utilisateurs des solutions cloud. L'État et la filière collaboreront pour veiller à ce qu'elle soit prioritaire dans les développements des offres. La filière

mettra en place les solutions techniques pour faciliter la migration vers un cloud de confiance, avec des services cloud de confiance comparables aux services en cloud public. La filière participera activement aux réflexions engagées par la Commission Européenne dans la perspective du futur programme Horizon Europe où la portabilité dans le cloud constitue un chantier complexe mais un objectif de la stratégie pour un marché unique numérique. La filière s'engagera également au niveau européen et international pour définir, influencer et promouvoir les standards d'interopérabilité nécessaires pour accompagner et accélérer l'adoption du cloud. Enfin, la filière favorisera la réversibilité dans le cloud pour permettre aux utilisateurs de récupérer leurs données et applications dans le cloud. L'État veillera en parallèle à ce qu'ils disposent de plus de lisibilité concernant les offres cloud qu'ils utilisent, et favorisera les solutions technologiques démontrant cette réversibilité dans le cadre de ses marchés.

Engagements réciproques :

1. **Engagements de l'industrie**
   - La filière contribue aux travaux de l'État concernant la définition des données sensibles en s'appuyant sur différents relais de l'écosystème.
   - La filière s'engage à proposer suffisamment d'offres qualifiées pour répondre aux besoins des utilisateurs. Ces offres permettront de développer la confiance dans le cloud et accroitre son adoption par les entreprises et les acteurs publics.
   - La filière s'engage à proposer un hébergement ainsi que des offres IaaS, PaaS et SaaS de confiance compétitives. Ces offres permettront de répondre aux besoins des entreprises et des acteurs publics concernés.
   - La filière s'engage à limiter les effets de verrouillage et renforcer la réversibilité, la portabilité et la transparence dans le cloud, incluant notamment une présence renforcée dans les organes de standardisation tout comme ceux de la Commission européenne.

2. **Engagements de l'État et des collectivités**
   - L'État s'engager à définir, en lien avec la filière, une doctrine claire sur la notion de données sensibles et sur la nécessité de privilégier des offres cloud de confiance pour les données sensibles et apportant une certaine transparence pour les utilisateurs.
   - L'État s'engage à soutenir le développement de la filière pour proposer des offres cloud de compétitives que ce soit sur l'hébergement, l'IaaS, le PaaS ou le SaaS.
   - L'État s'engage à accompagner les actions de la filière auprès de la Commission européenne et des partenaires concernant la limitation des effets de verrouillage et le renforcement de la réversibilité, de la portabilité et de la transparence dans le cloud.
   - L'État s'engage à favoriser les solutions réversibles dans le cadre de ses marchés publics.
   - L'État s'engage à poursuivre les travaux liés à la protection des données sensibles tant au niveau national qu'au niveau européen (notamment les négociations par la Commission européenne avec les États-Unis d'un accord bilatéral Union européenne – États-Unis équilibré pour parer aux risques combinés liés au numérique et à l'extraterritorialité).

FEUILLE DE ROUTE N°1 : INTERNATIONAL

DES INITIATIVES VISANT UNE CROISSANCE GRADUELLE DES EXPORTATIONS

Contexte :

Enjeux forts pour une industrie de souveraineté

La filière s'est forgé une image d'industrie d'excellence qui est aujourd'hui reconnue non seulement sur le territoire national mais également en Europe et dans le monde. Le volume d'exportation, de l'ordre de 50 % du chiffre d'affaires global de la filière, soit 13 Md€, atteste cette reconnaissance au-delà des frontières nationales.

Le développement des exportations est à la fois une nécessité et une opportunité pour les industriels de la filière :

- **Nécessité** car il ne saurait exister de développement pérenne d'une industrie dans un marché globalisé sans croissance à l'exportation. En particulier, les efforts d'investissements sont tels qu'ils ne peuvent s'appuyer économiquement que sur des volumes d'affaires importants que la seule réponse aux besoins nationaux ne peut satisfaire et ce, de surcroît, dans un contexte budgétaire national toujours plus tendu. La filière regroupant de nombreuses technologies de souveraineté, il est vital de consolider les acteurs du secteur en développant les exportations.
- **Opportunité** car les besoins pour plus de sécurité connaissent une croissance soutenue, à fort niveau de résilience au plan mondial, et les ruptures technologiques annoncées (IA, 5G/IOT, etc.) apparaissent comme autant de leviers pour se positionner sur les projets y faisant appel.

Une internationalisation déjà forte mais variable

La filière s'appuie sur un écosystème d'entreprises extrêmement large qui présente un paysage varié en matière d'activité export et de besoins en soutien associés : on y trouve ainsi des grands groupes positionnés comme leaders mondiaux dans leur secteur (déjà fortement internationalisés), certaines ETI très présentes à l'export et d'autres beaucoup moins et enfin de multiples PME et start-up dont la majorité est peu présente sur les marchés export.

Des propositions pragmatiques pour une croissance graduelle des exportations

La feuille de route « export » de la filière détaille un ensemble d'initiatives visant à développer les exportations de la filière selon **trois axes : connaître, se faire connaître et soutenir directement la filière en matière d'exportation.**

Ces différentes initiatives s'appuient essentiellement sur et complètent les travaux menés dans chacun des 5 projets structurants de la filière.

Les actions :

1) Connaître (les marchés et les dispositifs de soutien)

La connaissance des marchés et appels d'offres locaux est essentielle au développement d'une activité « export ». De même, le non-recours aux divers dispositifs de soutien est souvent le fait d'une méconnaissance de ces dispositifs, auparavant portés par des acteurs différents.

La filière lancera deux initiatives capitalisant sur les outils déjà existants et les démarches en cours :

- **La promotion auprès des groupements des plateformes régionales de la « team France export »** (https://www.teamfrance-export.fr/) qui regroupent les solutions publiques proposées par les Régions, les services de l'État, Business France, les Chambres de Commerce et d'Industrie et BPI France pour faire gagner les entreprises françaises à l'international (en particulier, la base de données ProAO de Business France, d'appels d'offres publics internationaux et locaux) ;

- **Méthode/Porteurs :** newsletters, réunions avec les adhérents -> en présence des administrateurs de la plateforme (Business France) et sous l'impulsion de la filière.
- **Calendrier :** 2020 et N+1 ; N+ 2**.**
- **Indicateur : r**elevé statistique annuel du recours à ces outils.

- **Le « mapping » d'un nombre limité de pays considérés comme prioritaires** par projet structurant (une quinzaine maximum), en coordination avec Business France et le ciblage d'actions visant à faire connaître les entreprises, identifiées par un appel à manifestation d'intérêt.
  - **T2 2020** : appel à manifestation d'intérêt auprès des entreprises de la filière, en vue du ciblage des actions visant à se faire connaître (cf. infra) – partage de la liste d'entreprises intéressées avec les référents Business France, les ASI et autres personnels concernés des représentations françaises à l'étranger ;
  - **Méthode/Porteurs de projets :** interroger les porteurs des 5 projets structurants, selon une logique ascendante à savoir en partant des besoins des industriels.
  - **Indicateur :** liste des pays prioritaires (3 à 4 pays, ne pas démultiplier les pays cibles).

2) Se faire connaître

L'axe « **se faire connaître** » doit permettre de **promouvoir les savoir-faire** des industriels de la filière à la fois en France et à l'étranger.

La priorité pour la filière Industries de sécurité est de structurer une offre française de rang mondial, en particulier dans les **segments clefs de la cybersécurité, de l'identité numérique, du « cloud de confiance » et des offres de sécurité innovantes pour les territoires et les sites.** C'est l'objet de la structuration de la filière en cinq grands projets dont les feuilles de route respectives visent précisément à développer des offres françaises de haut niveau, tant en termes de qualité technique que de respect de certaines grandes libertés (protection de la vie privée, etc.).

La filière engage 5 actions clés pour développer sa visibilité à l'export :

- **La mise en place de labels** de type « made in France », « utilisé en France » (lors des JO, par tel ministère, etc.) et **d'une charte éthique** pour l'ensemble de la filière.

  A titre d'exemple, **le label « France Cybersecurity »**, animé conjointement par un collège industriel, d'utilisateurs et étatique est un outil sur lequel il convient de capitaliser. Ce label mis en place en 2015 vise à attester l'origine française d'un produit ou d'une solution de cybersécurité et s'inscrit donc en pleine complémentarité des certifications/qualifications délivrées par l'ANSSI qui attestent quant à elle la robustesse des produits.

  Objectifs :
  - **T4 2020 :** définir un(des) label(s) analogue à « France Cybersecurity » sur l'ensemble du périmètre de la filière : « Label France Sécurité » ;
  - **T4 2020 :** finaliser la charte éthique du CSF d'ici la fin 2020.
  - **Méthode/Porteur :** développement d'une marque/bannière, en marge des projets structurants. A réaliser par la filière.
  - **Indicateur** : nombre d'entreprises labélisées 2021 et 2022, 2023, *etc.*
- **Le partenariat avec d'autres filières exportatrices** pour favoriser la chasse en meute en incitant les entreprises remportant de grands projets à l'export (BTP, sport et évènementiel, smart city, etc. ...) qui comprennent en général un volet sécurité et cybersécurité à utiliser en priorité des solutions nationales. Ce **marketing « indirect »**, sera conduit avec **le support actif du CNI International,** en ciblant les autres filières stratégiques avec l'objectif de faire connaître

les capacités de la filière et développer des approches et offres coordonnées sur les marchés export.

- **Calendrier** : réunion des RI 1er T 2020, à défaut une réunion inter-filières en format restreint : rapprochement pertinent avec la filière construction.
- **Méthode/Porteur :** via le CNI International.
- **Indicateur** : nombre de rencontres tenues.

- **Le développement du potentiel des salons et grands évènements internationaux** pour la promotion de la filière en particulier le soutien étatique (invitation de délégations). Les groupements de la filière participent d'ores et déjà à de nombreux salons et en facilitent l'accès aux PME (Pavillon France) :
  - **La filière cybersécurité** a pour objectif se doter d'un salon de taille mondiale, c'est-à-dire un salon de 2000 exposants de plus de 50 pays avec 100 000 visiteurs ;
  - **Méthode/Porteurs :** Capitaliser sur un salon existant (à Lille) et le renforcer. Plusieurs salons existants, à mettre en cohérence pour obtenir une masse critique (visibilité internationale).
  - **Calendrier** : dès 2020 et N+1, N+2, etc.
  - **Indicateur** : nombre de participants à ces salons
- **Par ailleurs, les déplacements officiels à l'étranger des autorités nationales en charge des questions de sécurité seront davantage mis à profit.** Il s'agit ici de structurer et d'animer un mécanisme simple d'information des adhérents sur ces visites, de partage des éléments de promotion de la filière et, au cas par cas, de constitution d'une équipe d'accompagnants industriels.
  - **Méthode/Porteurs** : réunion avec le ministère de l'intérieur pour définir un *modus operandi* afin d'être alerté sur les déplacements internationaux des autorités et la possibilité d'associer des entreprises. A moyen terme, envisager un élargissement à d'autres ministères. Diffusion de l'information sur la base des pays prioritaires (mapping).
  - **Calendrier :** T2 2020 à savoir la mise en place du mécanisme visé avec l'administration et en particulier le ministère de l'intérieur.
  - **Indicateur** : nombre d'entreprises accompagnées lors déplacements internationaux des autorités.
- **La participation à des opérations ciblées organisées chaque année par Business France** sur la base du « mapping » coordonnée évoqué supra.
  - **Calendrier :** suite au « mapping », à partir de fin 2020 et sur la programmation 2021 de Business France (recensement des intérêts à l'été 2020).
  - **Méthode/Porteurs :** Co-construction entre la filière et Business France
  - **Indicateur :** nombre d'opérations réalisées au profit de la filière, et succès de ces opérations (volume de chiffre d'affaires contracté, nombre de PME françaises impliquées, etc.).

3) Soutenir la filière

Enfin, l'axe « **soutenir directement la filière en matière d'exportation** » apparaît comme totalement déterminant au développement plus avant de la filière à l'export. Une raison à cette situation est le **déséquilibre qui se creuse entre les acteurs nationaux de la filière et leurs compétiteurs étrangers**, en particulier américains et asiatiques. Cette situation n'est pas propre à la filière sécurité.

La filière s'engage dans une action exploratoire pour mieux soutenir les PME à l'export.

Il s'agit de compléter les dispositifs de soutien aux investissements et à l'export destinés aux PME (recensés sur les plateformes régionales de la « team France export ») par la complémentarité grand groupe / PME pour les appels d'offres internationaux. Celle-ci est parfois limitée par l'obligation pour le lauréat du marché de recourir à des partenaires locaux ou par la plus faible compétitivité-coûts des PME françaises. L'idée est **d'étudier la faisabilité d'un mécanisme incitatif pour les grands groupes qui favorise l'investissement dans une PME innovante dans le cadre d'un marché d'export.**

- **Étudier avec le ministère de l'économie et des finances la pertinence et la faisabilité d'un mécanisme fiscal favorisant le « chasser en meute ».**
    - **Échéance : T2/3 2020.**

FEUILLE DE ROUTE N°2 : EUROPE

FAVORISER LA MISE EN PLACE D'UNE POLITQUE INDUSTRIELLE DE SÉCURITÉ À L'ÉCHELLE DE L'UE

Contexte :

Afin de contribuer au développement de capacités au plan communautaire répondant d'une part aux politiques de sécurité nationale (y compris en matière de souveraineté) et, d'autre part, aux intérêts et capacités du tissu industriel national, la filière a mis en place en 2013 un groupe de travail, co-présidé par le SGDSN et par le conseil des industries de confiance et de sécurité (CICS), qui a, notamment :

- élaboré une position française et directement contribué au document de politique industrielle européenne de la Commission de juillet 2012 ;
- alimenté les positions françaises pour la création d'ECSO en 2016 ;
- contribué au document de l'agenda stratégique de la commission 2021-2027 en 2019
- élaboré depuis fin 2017 une position française pour quatre priorités stratégiques européennes en matière de politique industrielle de sécurité, allant de la recherche à la proposition de programmes d'investissements : la sécurisation des frontières de l'Espace Schengen ; la transformation numérique et l'interopérabilité des forces de sécurité ; la protection des infrastructures critiques de transport et d'énergie ; la sécurisation de la ville intelligente.

Ces travaux se sont inscrits également dans le cadre de l'action n°31 du ***Plan d'action contre le terrorisme*** **(PACT)** « Faire de l'industrie européenne un acteur de la sécurité de l'Union », sous double pilotage du SGDSN et du SGAE.

Le CSF assure la poursuite de cette action, dont l'impact à terme sur la filière est majeur, par un groupe de travail de même nature.

Objectifs :

En coordination avec les projets structurants du CSF, le groupe de travail favorisera l'émergence d'une approche intégrée pour assurer la convergence des intérêts des acteurs, des enjeux de marchés et des politiques de sécurité.

Les objectifs et les actions à mettre en œuvre pour un groupe de travail UE sont directement liés au calendrier pour la nouvelle mandature de la Commission. En matière d'orientation politique, les impulsions données en fin d'année 2019 seront vraisemblablement déterminantes jusqu'à mi- mandat et dans le contexte de finalisation du cadre pluriannuel financier 2021-2027. Ces travaux doivent donc couvrir la période 2020 à 2022 pour être cohérents avec le calendrier européen.

Le principal objectif à poursuive par le groupe de travail Europe du CSF sera la mise en place d'une politique industrielle de sécurité à l'échelle de l'UE, débouchant sur un encadrement législatif (directive) qui renforcerait la souveraineté de l'UE en matière de sécurité et protégerait à cet effet son secteur industriel. Trois sujets et moyens d'actions seront poussés vers les instances UE et nos partenaires États membres notamment :

- Mettre en avant la nécessité de programme d'équipements pour renforcer la sécurité de l'UE : c'est en somme les quatre priorités précédemment exposées, dont il s'agirait d'assurer le « service après-vente » également par les acteurs industriels ;
- Instaurer une préférence UE pour un ensemble de solutions et technologies de sécurité critiques et essentielles pour la souveraineté de l'UE ;
- Favoriser l'émergence du futur écosystème européen de la sécurité en organisant l'accès aux données massives, en fléchant un effort particulier en matière d'IA pour la sécurité et d'impact

du numérique mais aussi des neurosciences, et ce dans le respect du RGPD et des pratiques européennes en matière de protection des libertés civiles.

Un certain nombre d'évènements et de tendances de secteurs adhérents à la sécurité nécessitent de mettre en place une coordination :

- La mise en place du programme de R&D et capacitaire Défense de l'UE avec comme point d'attention, son impact sur la définition d'une souveraineté européenne mais aussi en matière de perception du « dual use » et du continuum sécurité – défense vue par la Commission ;
- L'émergence du débat sur les menaces hybrides dont on ne peut dire à ce jour jusqu'où il viendra impacter le modèle de sécurité globale ;
- La mise en place d'une politique transverse de R&D et de régulation sur l'intelligence artificielle à l'échelle de l'UE dès 2020 ;
- Le changement climatique avec d'ores et déjà des rapprochements opérés au sein de la commission entre gestion des risques et sécurité globale.

Participants :

Les travaux seront conduit par un groupe de travail public-privé piloté par le SGDSN et le CICS.

Livrables :

Le GT produira les livrables suivants :

- Notes des autorités françaises à destination de la commission européenne et de nos partenaires sur les quatre enjeux : 2019
- Élaborer et mettre en œuvre une démarche stratégique conjointe public/privé pour obtenir de la Commission une communication sur la politique industrielle et la préférence communautaire en matière de sécurité. Cette communication devra être suffisamment ambitieuse pour préfigurer une future directive européenne : 2020- 2021
- Faire des propositions concrètes pour peser sur les débats en cours à Bruxelles notamment en matière d'accès aux données et d'utilisation de l'intelligence artificielle au bénéfice des organisations au sein de l'UE en charge de la sécurité : 2020

Engagements :

L'industrie et l'État s'engagent à :

- Reprendre les éléments des positions exprimées par le GT auprès des différents canaux publics et privés, notamment par les représentants et organisations industrielles à Bruxelles.

GOUVERNANCE ET CALENDRIER DU CONTRAT DE FILIERE

- **Tableau récapitulatif du calendrier des projets structurants et des principaux livrables attendus**

Nota : l'avancement des projets structurants sera suivi au niveau du Comex du CNI.

Projet	Pilotes	Résultats attendus	Calendrier
PS1 : Sécurité des grands évènements et des JO Paris 2024	D. Le Coguic (Atos) P. Demigné (Bertin)	- Constitution du consortium Équipe de France	2019
		- Constitution de l'offre générique de la filière	2020
		- Réalisation d'un programme de R&D et d'expérimentation	2022
		- Déploiement des technologies à l'occasion des JO Paris 2024	2024
PS2 : Cybersécurité et sécurité de l'IoT	JN de Galzain (Wallix) Y. Lagoude (Thales)	- Former 4000 opérateurs de cybersécurité dans les 3 ans qui viennent	2021
		- Mise en place du forum État-Industrie-Utilisateurs	2020
		- Mise en place d'une base d'information partagée	2021
		- Mise en place d'actions volontaristes à l'export, dont la création de deux centres de soutien mutualisé (Amériques – Asie)	2022
		- Lancement des projets d'innovation identifiés	2020
		- Inciter à un renforcement des dispositifs de financement de la cybersécurité : o en incitant les actionnaires du fonds deep tech issu du rapport Tibi à faire de la cybersécurité un secteur prioritaire du fonds o en étudiant la création d'un fonds sectoriel dédié pour les scale-up de PME	2020
		- Déployer des actions du projet dans la cadre du Campus Cyber	2020
PS3 : Identité numérique	B. Chappert (IN Group) C. Héritier (Idnomic)	- Première CNIe	mi-2021
		- Pilote et premiers services d'identité numérique dérivés de la CNIe opérationnels	2021
		- Lancement de projets d'innovation	2021
PS4 : Territoires de confiance	L. Denizot (Egidium Technologies) S. Deleville (Spie Batignolles Technologies)	- Adoption d'une charte éthique liant l'Industrie, l'État et les utilisateurs des technologies de sécurité	2020
		- Constitution du groupe public-privé en partenariat avec les métropoles partenaires	2020
		- Feuille de route partagé du développement des territoires smart & safe	2021
		- Mise à disposition d'une offre de plateforme de services à destination des collectivités qui répondra à leurs besoins	2023
		- Sélection des sujets retenus pour les premières démarches de co-innovation	9/2020
		- Déploiement de 3 nouveaux usages issus d'expérimentation de technologies de rupture	03/2021
		- Guide sectoriel pour la protection des établissements de santé	2020
		- Démonstration d'une offre globale de protection sur un établissement de santé majeur à l'ère du numérique	2021
PS5 : Numérique de confiance	M. Paulin (OVH) E. de Rémur (Oodrive)	- Stratégie d'utilisation du cloud suivant la sensibilité des données	2020
		- Proposition d'offres qualifiées cloud de confiance	2021
		- Proposition d'hébergement et d'offres IaaS, PaaS et SaaS de confiance compétitives	2021
		- Dispositions renforçant la réversibilité, la portabilité et la transparence dans le cloud	2022

Les signataires

Contrat Stratégique de la filière Industries de sécurité

Le Ministre de l'Intérieur

Christophe Castaner

Le Secrétaire d'Etat auprès du Ministre de l'Economie et des Finances

Agnès Pannier-Runacher

CSF Industries de Sécurité

Le Président du CSF

Marc Darmon

Organisations Syndicales

CFE-CGC

Philippe Gotti