2019 | 2022

SECURITE NUMERIQUE

POLESCS

MISES A JOUR 2021

AXE STRATEGIQUE **PHASE 4.0**

TABLE DES MATIERES

*La **mise à jour 2021** est stipulée par un filet vertical vert sur le côté des "paragraphes du texte concerné.*

*texte" et de l'annotation **MAJ*** dans le titre*

LE MOT DU PRESIDENT

Chers membres, chers partenaires,

LA PHASE 4.0 des pôles de compétitivité démarre pour la période 2019 à 2022. **SCS** a été sélectionné pour cette PHASE 4.0 et a choisi un positionnement dans la continuité avec quatre axes stratégiques dont la **Sécurité Numérique** avec une feuille de route à construire pour les 4 prochaines années.

Expert du domaine de la **Sécurité Numérique**, **SCS** accompagne les projets innovants, soutient les startups et PME du domaine et structure l'ecosystème via l'animation d'un groupe thématique « **Sécurité Numérique** ».

Les membres **SCS** conçoivent et développent des solutions de **Sécurité Numérique** éprouvées pour de nombreux domaines d'application depuis la protection des données sensibles médicales ou bancaires, en passant par les dernières technologies de cryptographie jusqu'à la protection contre les attaques et intrusion d'un véhicule connecté.

Ces solutions permettent d'accompagner la croissance des marchés en assurant que les enjeux de **Sécurité et de Confiance numérique** seront pris en compte tout au long de la chaîne de valeur.

Dans le contexte des événements sanitaires exceptionnels de l'année 2020 et 2021, **SCS** a souhaité **mettre à jour cette feuille de route** avec l'appui **d'experts** du domaine et dans une **démarche collective**.

Cette contribution « collective » à la mise à jour de la feuille de route est essentielle pour l'ensemble des acteurs de l'écosystème **SCS** mais aussi pour les financeurs de **SCS**. Elle permettra de construire un positionnement robuste et visible au niveau européen, et aussi d'orienter les actions *(notamment les animations)* pour l'écosystème de la **Sécurité Numérique**.

*"Nous remercions les personnes suivantes pour leur contribution à la **mise à jour** de la feuille de route en 2021"*

Romain WACQUEZ
R&D Manager CEA
CEA Tech, équipe commune CEA Tech/MSE

Hervé ROCHE
VP Marketing
TRUSTED OBJECTS

Philippe LALEVÉE
Directeur
Ecole Mines Saint-Etienne

jean Max DUTERTRE
Professeur
Ecole Mines Saint-Etienne

Moussa Belkhiter,

*Président de **SCS***
& Site Manager de NXPSemiconductor Sophia Antipolis

LA PRESENTE FEUILLE DE ROUTE A POUR VOCATION

De décrire le marché et son périmètre

D'identifier les enjeux, les acteurs, les opportunités liés à la Sécurité numérique

De préciser des objectifs et les actions principales sur la période

SYNTHESE DES MISES A JOUR (SUITE COVID-19)

Cette pandémie nous a fait prendre conscience qu'on ne peut tout prévoir et **souligné l'importance accrue d'avoir une stratégie proactive pour le futur.** Les technologies, les solutions et/ou produits devront être agiles et protégés efficacement avec des systèmes de sécurité très élaborés.

Les vulnérabilités aux attaques cyber, l'hyperconnectivité, les déluges de données, la diffusion de technologies de rupture comme le quantique, l'IA, l'émergence de nouveaux usages, l'accélération de certains marchés imposent de **repenser l'innovation et de miser encore plus qu'avant sur les écosystèmes et les compétences.**

Il y a une **volonté politique forte, française et européenne de soutenir la filière numérique** et les aides gouvernementales ont été exceptionnelles.

Cette crise a aussi révélé **l'agilité de nos entreprises et montré la pertinence des coopérations entre start-ups, grands comptes et organismes de recherche.**

Les membres SCS ont saisi ces opportunités avec des premiers résultats très encourageants sur l'innovation générée, les perspectives de développement de certaines entreprises et les futurs investissements locaux contribuant à la souveraineté technologique, recherchée par les pouvoirs publics.

La région Provence-Alpes Côte d'Azur a des atouts indéniables dans le domaine du numérique, et cette pandémie nous démontre la pertinence de la coopération entre le monde académique et les industriels, qui va contribuer au rayonnement international de ces acteurs.

Marchés, tendances et chaîne de valeur

- On constate une **augmentation des attaques** et la nécessité à l'heure d'une digitalisation accélérée par le **COVID-19** de mieux **se protéger** avec des solutions performantes, évolutives *(modulaires)* et adaptées.

- Au niveau national, le Gouvernement a lancé fin 2020 un plan de relance national pour redresser durablement l'économie. Avec **un fond de 136 millions d'euros spécialement dédié à la cybersécurité** et piloté par l'**ANSSI**, le plan **France Relance** prévoit de renforcer le niveau de sécurité des administrations, des collectivités et des organismes au service des citoyens.

- Au niveau régional, la feuille de route Cyber de la Région SUD Provence-Alpes-Côte d'Azur voté fin 2020 souligne le **secteur des objets connectés et des systèmes embarqués sécurisés comme dominant et le plus prometteur en terme de différenciation stratégique.** Elle met en avant également une expertise territoriale pour l'hébergement sécurisé et souverain de données.

- **Des projets structurants sont en cours de développement soutenus par une filière industrielle dynamique :** DIH, Centre de Ressources Cyber, IoTCenter... A titre d'exemple, un **nouveau centre de ressources Cyber régional est prévu à Toulon** et permettra aux PME régionales d'avoir un unique point de contact Cyber pour information ou être orientés vers les acteurs opérationnels référencés.

Verrous technologiques

Les **6 verrous technologiques** de la Feuille de route en 2019 **sont toujours d'actualité.**

Toutefois, le **verrou autour de la cryptographie post quantique** a pris une **grande importance.**

En effet, le domaine quantique a fait l'objet d'une **véritable stratégie gouvernementale** comme **l'Intelligence Artificielle.**

Quelques évènements structurants ont eu lieu en France et à l'international depuis 2019 :

- En Janvier 2020 est publié le **Rapport Forteza** *(Rapport de mission parlementaire)* sur **« QUANTIQUE : LE VIRAGE TECHNOLOGIQUE QUE LA FRANCE NE RATERA PAS »**

Il y est mentionné de **« MAINTENIR UNE INDÉPENDANCE STRATÉGIQUE SUR LES TECHNOLOGIES DE CRYPTOGRAPHIE ».** L'avènement possible de calculateurs quantiques suffisamment puissants *(LSQ)* pour casser les schémas de chiffrement actuels *(e.g. RSA)*, même si cela ne se réalisera qu'à relativement long terme, appelle des actions immédiates en matière de sécurisation des communications sensibles.

- Enfin, le 21 janvier 2021, le **président E. Macron présente le plan quantique avec une enveloppe de 1,3 Millards** sur les technologies quantiques dont « **150 millions d'euros seront consacrés à la cryptographie post-quantique** pour sécuriser les communications avec des protocoles résistant aux méthodes de calcul des futurs ordinateurs quantiques ».

- **A l'international**, le **NIST** est un organisme international travaillant sur la standardisation des solutions de sécurité depuis 2017. Le **NIST** lance régulièrement son célèbre **Concours** pour la standardisation des algorithmes pour la cryptographie post-quantique.

Les propositions reçues sont challengées par les **meilleurs mathématiciens du monde.** Lors du concours l'année dernière, **26 candidatures ont été retenues** *(dont une dizaine sont co-developpées en France).* Et cette année, 7 finalistes et 10 solutions alternatives concourent.

Nouveaux Usages

Avec la pandémie, **les besoins en sécurité explosent :** ceci apparait comme un défi pour les entreprises et les utilisateurs mais aussi comme une opportunité pour les acteurs de la sécurité.

Quelques opportunités sur quelques domaines d'applications transverses apparaissent avec la sécurisation de la chaîne d'approvisionnement & traçabilité, le détournement des objets connectés, la sécurité des réseaux ou encore la sécurité OT.

Une grande tendance apparait avec **les services sécurité dans le cloud ou la notion de « Security-as-a-Service (SaaS) – Platform-as-a-Service (PaaS) ».**

Cette nouvelle « plateforme » de services permettra de délivrer des prestations de " Secure device management" dans le cloud ou encore la gestion sécurisée du cycle de vie de flottes d'objets connectés : *(re-)*provisioning, monitoring sécurisé, mise à jour sécurisée des logiciels, gestion sécurisée de l'identité numérique *(changement de propriétaire)*...

Formations

De nouveaux Masters Spécialisés *(MS)* apparaissent comme le Master **« Cybersecurité des systèmes complexes pour l'industrie et la défense »** délivré par **Centrale Marseille.**

En 2021, un nouveau Master spécialisé **Designer of Secure devices for IoT** sera proposé par l'**Ecole des Mines de St Etienne.**

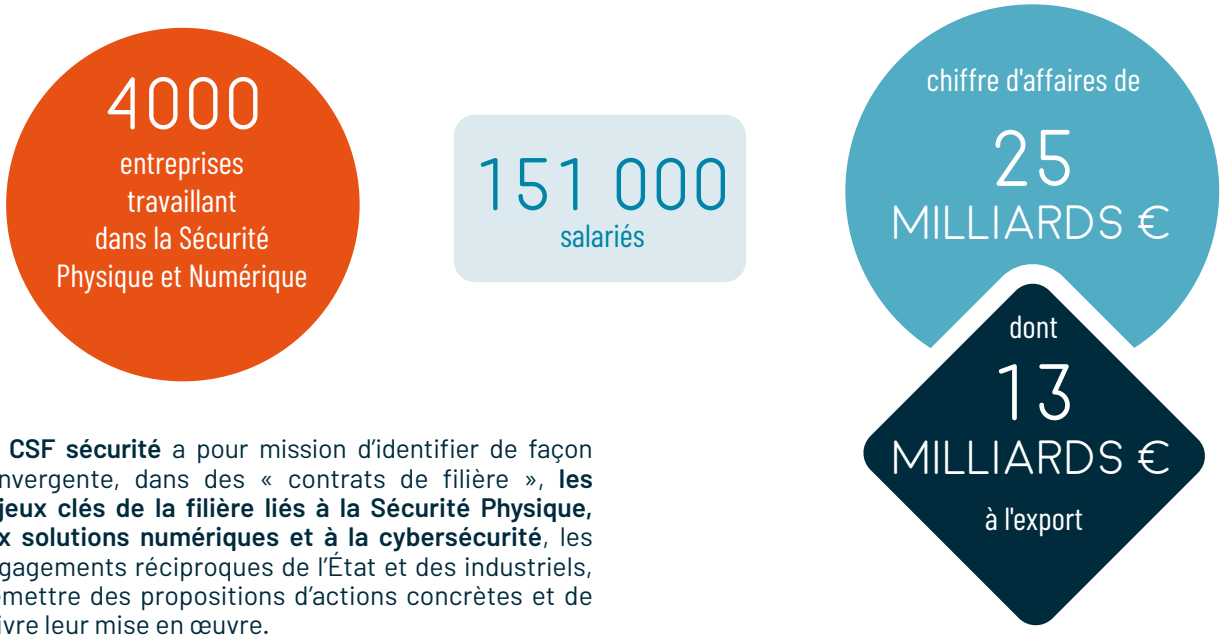
1. Description et périmètre de la Sécurité

1.1 Contexte, définition et périmètre de la Sécurité

La filière de la sécurité est vaste et répond à un besoin fondamental de protection ressenti par tout un chacun, notamment avec les nombreux incidents récents qui ont mis la sécurité des infrastructures, des systèmes, des réseaux et des individus *(et de leurs données personnelles)* à l'ordre du jour des préoccupations prioritaires des citoyens et des pouvoirs publics. Cette filière regroupe en fait la **Sécurité Physique et Numérique**. La sécurité physique ne fait pas l'objet du document présent qui se concentrera sur la sécurité numérique uniquement *(cf chapitre périmètre)*. En revanche on rappelle ici que cette filière comprend, outre le cœur des industries de sécurité, des services privés et surtout un important secteur de services publics de sécurité non marchands *(police et gendarmerie nationales, douanes, polices municipales, sécurité civile dont certaines unités militaires, pompiers, justice, administration pénitentiaire)*.

Au plan national, il est intéressant de noter que **fin 2018** le gouvernement a donné **une place d'envergure à la filière des industries de sécurité** en l'organisant avec la création d'un **Comité stratégique de Filière** *(CSF)*, au sein du Conseil national de l'Industrie.

LA FILIERE DES INDUSTRIES DE SECURITE, JUSQU'A PRESENT STRUCTUREE DANS LE CADRE DU **COMITE DE FILIERE DES INDUSTRIES DE SECURITE** ET AVEC LA PARTICIPATION DU **COMITE DES INDUSTRIES DE CONFIANCE ET DE SECURITE**, REPRESENTE AUJOURD'HUI PLUS DE :



Le CSF sécurité a pour mission d'identifier de façon convergente, dans des « contrats de filière », **les enjeux clés de la filière liés à la Sécurité Physique, aux solutions numériques et à la cybersécurité**, les engagements réciproques de l'État et des industriels, d'émettre des propositions d'actions concrètes et de suivre leur mise en œuvre.

Au plan Européen, **l'Agence Européenne chargée de la sécurité des réseaux et de l'information** *(ENISA)*, créée en **2004**, joue un rôle majeur dans le paysage de la Cyber Sécurité. La directive sur la sécurité des réseaux et des systèmes d'information de **2016** a pour objectif **d'assurer un niveau élevé de sécurité des réseaux et de l'information dans toute l'Union.**

La digitalisation de l'ensemble des secteurs d'activités les rend plus vulnérables aux attaques toujours plus massives et sophistiquées. Cette thématique voit sa criticité augmenter avec le développement d'une pluralité de domaines concernés par les problématiques liées à la protection des données sensibles mais aussi **aux notions de respect de la vie privée et de toutes les questions éthiques qui émergent en environnement connecté :** chez soi, dans son véhicule, au travail, ou en ville.
Parmi ces domaines, nous trouvons avec des degrés de maturité différents : la domotique, l'économie d'énergie avec les compteurs intelligents, le suivi médical personnalisé, la géolocalisation, les réseaux sociaux...
La Sécurité Numérique est donc clé pour notre économie et notre avenir.

1.2 Périmètre de la Sécurité au sein du Pôle SCS

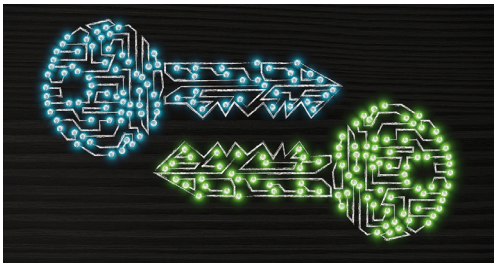
Dans le secteur de la Sécurité Numérique, SCS rassemble un écosystème à la pointe composé d'acteurs industriels et académiques de très haut niveau occupant des positions très fortes et différentiées dans le monde. **Berceau des technologies de la carte à puce la Région PACA**, territoire d'excellence que couvre le Pôle SCS, rassemble des acteurs tels que de **grands industriels de renommée mondiale** *(notamment Gemalto (Thalès company), Thalès, STMicroelectronics, NXP, Schneider Electric...)*, de laboratoires de recherche publics et privés d'excellence *(CEA, EURECOM, EMSE, CNRS...)* et de **nombreuses PMEs et startups dynamiques**.

Cet ensemble représente environ **50 acteurs** pour plus de **5000 emplois** de haut niveau. L'avènement du numérique a un impact majeur sur la filière de la sécurité et les menaces ne sont plus seulement physiques ou matérielles. Ainsi, **le pôle et son écosystème ont un rôle clé à jouer sur le long terme.**

CET **ECOSYSTEME** EST PARTICULIEREMENT **BIEN POSITIONNE** SUR :

- **Les technologies pour la sécurité hardware des puces électroniques**
- **Les cartes à puces et objets sécurisés et autonomes**
- **La cryptographie et ses applications**
- **Les architectures hardware et software sécurisées notamment en environnement contraint**
- **Les méthodes et outils de simulation et de protection contre les attaques sur les puces et les objets**
- **Les expertises et méthodes pour la certification et l'évaluation sécuritaire**

Ce périmètre n'est pas figé et pourra évoluer en fonction du renforcement de certaines expertises ou secteurs technologiques.



2. Références/Liens/Position avec les stratégies régionales et nationales

2.1 Des initiatives engagées au niveau régional, national et européen

La filière sécurité numérique s'inscrit dans plusieurs stratégies et actions aux niveaux **Europe**, **France** et **Région** :

NIVEAU EUROPEEN	**la directive sur la sécurité des réseaux et des systèmes d'information de 2016**	Cible aussi bien les Fournisseurs de services numériques *(DSP)* offrant des services à des personnes au sein de l'Union Européenne que les Opérateurs de services essentiels *(OES)* implantés dans l'Union Européenne. La Directive NIS leur impose entre autres de prévenir les incidents de sécurité, de minimiser leur impact afin d'assurer la continuité du service et de notifier l'autorité compétente pertinente de tout incident de sécurité.
	DIH[1]	
	Agence Européenne chargée de la sécurité des réseaux et de l'information *(ENISA)*[2]	
NIVEAU NATIONAL	**Comité Stratégique Filière Sécurité *(CSF Sécurité)*[3]**	Il va définir la politique industrielle du domaine et reprendre notamment les travaux et mission du COFIS et définir des actions R&D stratégiques.
	Agence Nationale de la Sécurité des Systèmes d'Information[4] *(ANSSI)*, EUROSMART	
	Sécurisation des Jeux Olympiques 2024[5]	
NIVEAU REGIONAL	**OIR *(Opérations d'intérêt régional)* SmarTech et Industrie du futur[6]**	
	Programme de formation professionnelle autour de la Sécurité Numérique de l'IoT	Avec l'UIMM.
	Plateformes mutualisées CIMPACA	Renforcement des moyens en sécurité.

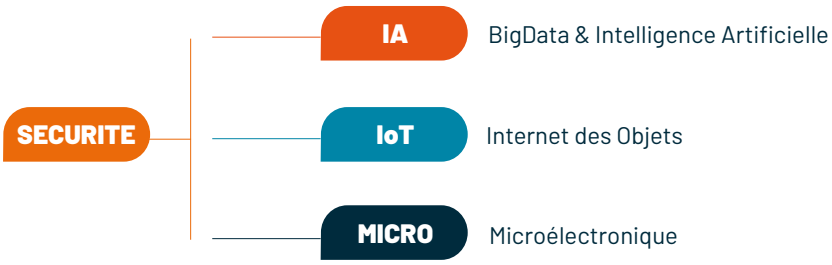
SCS contribuera aux stratégies européennes, nationales et régionales sur la **filière Sécurité** afin de mettre en avant les **atouts et spécificités de son écosystème.**

1 https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs
2 https://europa.eu/european-union/about-eu/agencies/enisa_en
3 https://www.entreprises.gouv.fr/conseil-national-industrie/la-filiere-industries-securite
4 https://www.ssi.gouv.fr/
5 https://jnov.safecluster.com/
6 https://www.maregionsud.fr/economie-emploi/innover-plus-pour-doper-la-croissance-et-la-competitivite/8-operations-dinteret-regional.html

2.2 Synergies entre la Sécurité et les autres axes stratégiques de SCS

Les quatre axes stratégiques identifiés par le Pôle SCS pour **la phase 4** des pôles de compétitivité *(période 2019 – 2022)* sont intimement liés.

Les feuilles de route s'alimentent entre elles, les briques technologiques des unes servant les besoins des autres, parfois même de façon duale. **Indispensables aux solutions communicantes sécurisées**, les enjeux de sécurité et d'identités numériques sont au cœur des technologies Microélectroniques, de l'Internet des Objets en passant par le BigData et l'Intelligence Artificielle :



Avec l'axe stratégique :

MICRO

La maîtrise de l'état de l'art mais aussi des innovations autour des technologies hardware *(microcontrôleurs et mémoire sécurisés…)* existantes ou en évolution afin répondre aux défis de la miniaturisation, de l'intégration et de la Sécurité Numérique sera une composante clé des prochaines décennies. De même, il faudra assurer une excellente maitrise de la digitalisation de la chaîne de valeur et de ses coûts *(productivité et compétitivité)* tout en maintenant les niveaux de sécurité et de protection apportés actuellement par les approches traditionnelles.

IoT

L'adoption du « security and ethic by design » intégrera la sécurité aux objets connectés et aux réseaux dès le stade de la conception. Il faudra pour cela appréhender au bon niveau les menaces et les approches résilientes à mettre en œuvre pour parer les futures attaques qui combineront configurations de masse d'objets connectés, puissance de calcul locale de ces objets et bande passante des réseaux. Par ailleurs, le respect de la vie privée est un autre sujet critique *(« privacy by design »)*. Les objets connectés n'inspirent pas encore totalement confiance. La sécurité des identités et des données sera également cruciale dans le développement de l'Internet des Objets pour la confiance des utilisateurs.

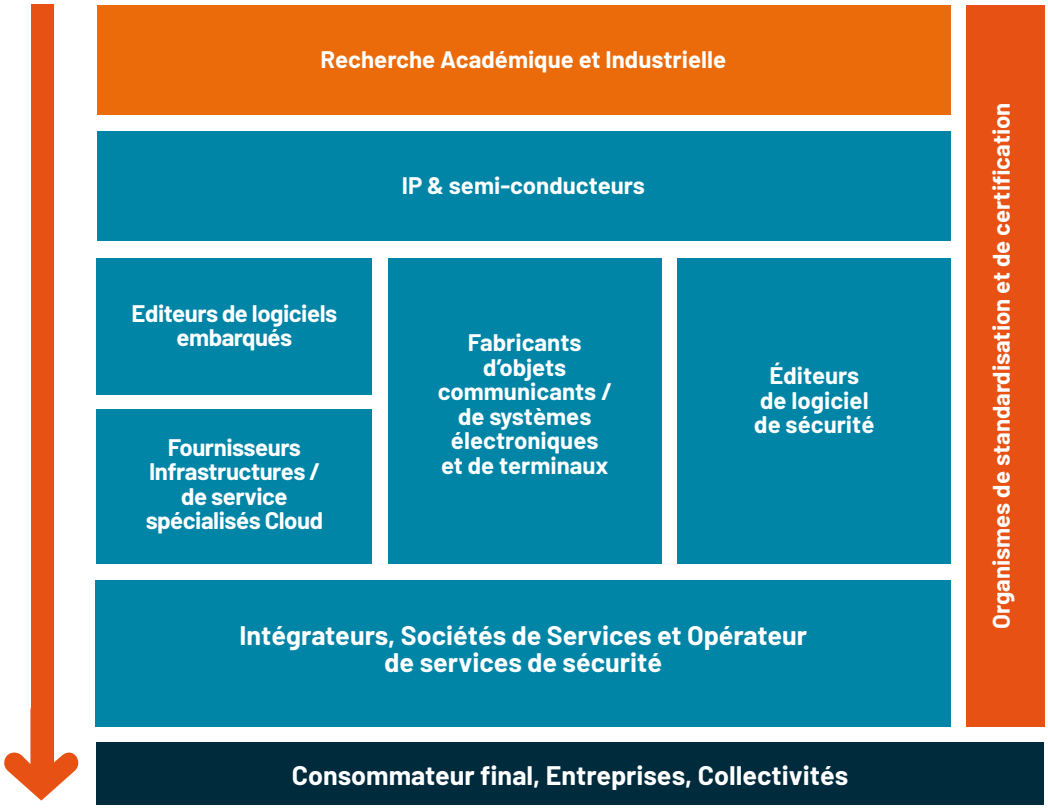
IA

Quelles que soient les applications, les domaines ou les infrastructures, deux familles de technologies sont omniprésentes et entretiennent une relation duale avec le monde de la sécurité. Il s'agit, d'une part, des technologies de l'intelligence artificielle *(IA)*; et, d'autre part, du BigData, alias le traitement de données massives. Ces deux univers technologiques prennent une part de plus en plus importante dans les applications du numérique et aucune n'y échappe. La filière de sécurité doit en maîtriser les arcanes pour en tirer le meilleur parti, à la fois comme outil de sécurisation *(ex: utilisation du deep learning pour les systèmes de détection d'intrusion)* mais aussi comme nouveau marché d'avenir pour lequel il faudra proposer des protections toujours plus complexes contre les **nombreuses attaques connues**: *adversarial examples, data poisoning, model inversion, membership inference,…*

3. Chaîne de valeur & Cartographie des acteurs

La chaîne de valeur permet d'identifier et de positionner les différentes briques technologiques et offres contribuant à la globalité de la chaîne de la Sécurité Numérique.
Elle permet de visualiser graphiquement les éléments clés et les acteurs du domaine. Pour la Sécurité Numérique, la chaîne de valeur s'inspire de travaux passés réalisés dans le Pôle depuis 2013.

Sa déclinaison dans un contexte mondial, puis régional, avec les acteurs du Pôle SCS *(cf la même chaîne de valeur avec les acteurs SCS – en annexe)* permet d'identifier les forces et faiblesses du territoire du Pôle sur chacune des compétences clés du secteur. Ce travail permet de mettre en valeur les leviers d'action potentiels sur la thématique.



Chaîne de valeur de la Sécurité Numérique

4. Marchés et usages cibles

4.1 Marchés prioritaires pour le Pôle SCS

En s'appuyant sur les **expertises de l'écosystème**, les marchés prioritaires dans la stratégie régionale et les axes prioritaires européens, le Pôle SCS a défini **5 marchés prioritaires**, en croissance et impliquant une part importante de son écosystème pour cette **phase 2019-2022 :**

- **Santé**
- **Smart Cities**
- **Industrie 4.0**
- **Transport & Mobilité**
- **Smart Vehicle *(exploratoire)***

Le marché **Smart Vehicle** sera lancé en mode exploratoire en 2019 et sera traité uniquement si des opportunités et des actions concrètes sont identifiées. **Le niveau d'appétence et d'opportunité varie sur ces différents marchés.**

4.2 Dimensionnement des marchés cibles

De nombreux marchés verticaux applicatifs vont pouvoir bénéficier des avancées technologiques **de la Sécurité Numérique**.

Ci-dessous quelques chiffres de taille de marché et de croissance de marché qui vont en bénéficier :

	PRINCIPAUX CHIFFRES
INDUSTRIE 4.0 *(incluant l'agriculture)*	**504 M** d'objets connectés en 2025 dont 80% pour les opérations de supply chain et de logistique – **croissance de 20% / an** *(Idate)* Marché « Smart Logistics », CAGR 2016-2021 32,7% , vers 41,30 Mds$ *(MarketsandMarkets[7])*
SMART CITIES *(incluant SmartBuildings & Retail, Smart Metering Energy, SmartHome)*	**Smart Cities :** Marché estimé à plus de **150Mds€** en 2025 *(Market Research)* – **croissance de 23%/an** **SmartBuildings & Retail : 1,5Mds€** en 2025 - **croissance de 17%/an** *(Frost&Sullivan)* **Smart Metering/Energy : 1 Mds de compteurs communicants** dans le monde en 2020 *(ABI)* **SmartHome :** 224Mu de maisons équipées à court terme pour environ **35Mds€** *(Strategy Analytics)*
SANTE & BIEN-ETRE	**Santé & Bien être :** Plus de **160Mds€** en 2022, **croissance de 20%/an** *(Technavio, Research & Market)* **Wearables** *(incluant les dispositifs portés sur soi comme les « quantified self »)* : **471Mu** en 2021 - **croissance de 100%** sur la période 2016/2021 *(Strategy Analytics)*
TRANSPORT & MOBILITE *(incluant transport intelligent et véhicule autonome)*	**176,5Mds$** en 2021 pour les solutions de smart transport *(Transparency Market Research[8])* **126Mds€** en 2027 pour le marché des véhicules autonomes – **croissance de 40%/an** *(Market research)*

7 https://www.marketsandmarkets.com/Market-Reports/connected-logistics-market-81941108.html
8 https://globenewswire.com/news-release/2016/06/24/851178/0/en/Global-Smart-Transportation-Market-Boosted-by-Growing-Need-for-Smart-Services-to-reach-US-176-5-bn-by-2021-TMR.html

4.3 Usages de la Sécurité pour chacun des marchés prioritaires

4.3.1 Santé

Les objets connectés constitueront donc l'un des principaux relais de croissance du marché du bien-être, de la santé et plus spécifiquement de l'e-santé dans les prochaines années. Le contexte porteur dont bénéficient aujourd'hui ces marchés s'explique notamment par l'explosion des perspectives et des usages sur le marché des **objets connectés** utilisés par le **patient à son domicile**.

En France, si le marché demeure pour le moment relativement faible, les perspectives attendues semblent prometteuses. avec ce qu'il est commun d'appeler e-health, m-health et p-health pour, respectivement, **santé électronique, mobile et personnelle…**

En effet, face aux nouveaux enjeux de **dématérialisation des données**, la **sécurité des données médicales** est un sujet majeur *(au sein même de l'établissement de santé mais aussi de façon déportée chez le patient).* Il faut à la fois assurer l'**échange de données** en toute sécurité, leur intégrité mais aussi leur capacité à être exploitées à tout moment. Ceci pose évidemment de nombreuses questions.

C'est toute la chaîne de valeur de la « eSanté » qui sera concernée par la **sécurisation des données**. En effet, les données envoyées, stockées, utilisées par les objets connectés sont des **données personnelles** à partir desquelles **l'identité** de l'utilisateur peut être retrouvée.

Sont concernés de nombreux acteurs :

- les fabricants de dispositifs médicaux
- les éditeurs de logiciels pour les établissements de santé
- les développeurs d'applications pour smartphone,
- les hébergeurs de données de santé à caractère personnel
- les assureurs
- les organismes publics
- les opérateurs télécoms…

Les technologies **d'identification/authentification**, de **sécurisation de l'IoT** *(HW, SW, hybride..)*, **de protection de la vie privée, et d'anonymisation des données** *(personnelles et sensibles)* sont directement concernées.

4.3.2 Smart Cities

La Smart City ou « **smart territory** » représente un nouvel Eldorado pour tous les fabricants de systèmes sécurisés. Gartner, par exemple, pense que 2,3 milliard d'objets ont été utilisés en 2017 *(+40% par rapport à 2016)* par les Smart Cities. Transports collectifs, éclairages publics, pollution atmosphérique, centrales électriques, hôpitaux, vidéosurveillance… de nombreuses fonctions critiques poursuivent leur **transformation digitale**. Concevoir la ville comme une **plateforme de services d'infrastructure** est un enjeu majeur pour les Métropoles et leurs DSI.

Ce déploiement massif et rapide ouvre de nouveaux espaces de **vulnérabilité**, dont les villes se saisissent peu à peu pour se transformer en **Safe Cities**. L'ensemble des fonctions et des données utilisables par une ville doivent être accessibles, disposer d'éléments de sécurité et de suffisamment de ressources de calcul pour mettre en œuvre de manière optimale une politique de sécurité ad-hoc.

Il y a toutefois quelques facteurs de risque et d'interrogation éthiques *(prédiction des comportements, collectes de données personnelles…)*. Cela appelle donc à une **vigilance non seulement juridique, mais aussi démocratique et citoyenne**.

Dans un rapport, des chercheurs d'IBM présentent les résultats de leurs travaux sur les failles de sécurité de la smart city. Sur un total de 17 failles, huit sont qualifiées de critiques *(ex : détourner les systèmes d'alerte à la population et créer une panique générale)*. C'est la difficile équation que les autorités étatiques doivent résoudre face à la prolifération des outils numériques, mêlant **vidéosurveillance intelligente**, technologies de **big data** et **données biométriques**, déployés par des villes dans le cadre de leur stratégie smart city.

Les organisations — **entreprises, services publics** — doivent tout mettre en œuvre pour identifier toutes les parties prenantes de leur écosystème numérique afin de minimiser leur « **angle mort digital** » qui crée autant de points d'entrée potentiels pour les pirates informatiques.

Dans ce contexte en pleine mutation, des initiatives d'accompagnement des villes voient le jour, à l'image de l'ONG Securing Smart Cities, qui partage ressources et bonnes pratiques.
Certains États adoptent également une stratégie dédiée, à l'instar de la France[9]. De quoi donner lieu à une prise de conscience globale qui mettra la cybersécurité au cœur de la stratégie de résilience des villes de demain.

Les objets connectés installés dans les compteurs d'eau, les bus, les réverbères, poubelles…nécessitent parfois d'avoir des durées de vie de 10 ans.
Les composants microélectroniques intégrés auront donc la nécessité **de consommer très peu malgré la présence de sécurité forte consommatrice en puissance**.

La **conception d'architectures** innovantes permettra d'en augmenter la sécurisation et l'autonomie. L'approche **Blockchain décentralisée** concerne aussi les objets connectés collecteurs de donnée d' énergie et pourrait révolutionner le marché des smartgrids.

4.3.3 Industrie 4.0

L'industrie est dans une phase de mutation majeure avec l'arrivée de l'Internet des Objets dans les usines. **L'IoT apporte dans les process industriels la capacité de placer des capteurs à toutes les étapes d'une chaîne de fabrication**, de manière à être plus réactif et à assurer l'optimisation et la sécurisation des processus de fabrication tout en contrôlant totalement les coûts. On parle alors d'Industrie du futur ou bien d'Industrie 4.0.

A titre d'exemple, tous les composants entrant dans la fabrication de produits **peuvent être localisés en temps réel** et suivis tout au long de la chaîne de production, ce qui permet **d'améliorer significativement la performance de l'outil industriel.**

Parmi ces applications on peut citer :

- **La gestion des approvisionnements en fluides et en matières premières**
- **Le suivi de la performance des équipements**
- **La traçabilité des évènements à toutes les étapes de production**
- **La maintenance prédictive**
- **La réduction des consommations d'énergie**
- **Etc…**

Dans tous les cas, ces applications passent par la collecte de données sur les éléments à suivre, la prise de décision et la mise en œuvre des décisions dans l'environnement de production. Ces éléments sont reliés par des réseaux, auxquels Le développeur d'applications doit apporter la plus grande attention. **En effet, la sécurité est au centre des préoccupations pour l'industrie du futur.**

Une intrusion dans un réseau d'un système de production peut s'avérer particulièrement dommageable tant en termes de **pertes d'actifs** qu'en **risques pour la vie humaine**. En effet, des sites industriels peuvent également être la cible de **cyber attaques.**
En 2014, une usine sidérurgique en Allemagne a été la cible d'une attaque, au cours de laquelle des hackers ont pris le contrôle du système de commande de l'usine, et ont détruit les interfaces homme-machine. Ils ont ensuite pu prendre le contrôle d'un haut-fourneau, l'empêcher de déclencher les alarmes de sécurité et ainsi causer des dommages irréparables.

Il est à noter que ces environnements, regroupés sous le vocable **"OT" pour Operational Technology,** se distinguent du monde **"IT", Information Technology**, qui est celui qui a reçu le plus d'attention des acteurs de la cybersécurité. Les Infrastructures OT, historiquement, étaient isolées du reste du monde et, donc, moins vulnérables, tout du moins aux menaces externes. C'est de moins en moins le cas. Les contraintes spécifiques de ces environnements nécessitent des solutions appropriées, ce qui ne permet pas toujours de bâtir sur l'expertise acquise dans le monde IT.

Pour remédier à ce type d'intrusion dans le monde industriel & professionnel, lorsqu'un parc d'objets

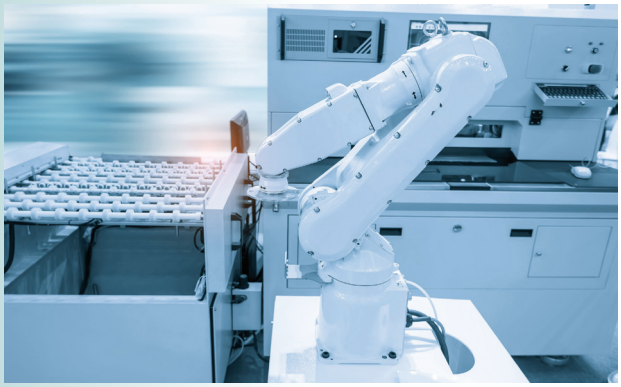
9 Cybermalveillance.gouv.fr

connectés est sur le terrain, **il doit nécessairement être administré de manière à remplir leur fonction et assurer que leur sécurité sera bien gérée** *(on notera que l'analogie est forte avec les domaines de la Santé ou des Smart Cities).*

Des plateformes plus ou moins évoluées sont utilisables pour suivre et mettre à jour les différents objets connectés. Il peut également arriver que certaines applications utilisent des capteurs connectés qui seront très petits, peu chers et qui ne possèdent pas de capacités d'administration.

Dans ce cas, en cas de faille de sécurité, il n'y a pas d'autre solution que de récupérer physiquement les objets pour les reprogrammer, les mettre à jour voire les remplacer, ce qui est contraignant. Les usages font que dans les faits, il n'y aura pas d'administration. Ceci aura donc des conséquences sur le **niveau de sécurité des objets** utilisés dans ces applications puisqu'aucune mise à jour ne sera réellement faite *(cf. notion d'angle mort digital également très fort dans le domaine des smart cities).*

Les concepteurs des outils d'administration des objets connectés doivent prêter une attention particulière **à la sécurité dès la conception de l'ensemble du système** *(Security by design)* et une protection contre toute intrusion ou hacking à distance sur le système de production. **La protection des données collectées, transmises ou stockées** *(dans le cloud)* avec la dynamique de transformation digitale de certaines usines ou machines sera assurée grâce à la **sécurité des composants** et des **protocoles**.



4.3.4 Transport & mobilité

Dans le monde du transport et de la mobilité, **l'IoT révolutionne en premier lieu les transports urbains** *(et en particulier les transports autonomes)* mais aussi tout ce qui touche à **la chaîne d'approvisionnement** *(supply chain)* dans un environnement industriel *(logistique).*

Selon un sondage mené auprès de professionnels de la sécurité informatique, **les transports seraient parmi les infrastructures les plus exposées** *(Government Technology)* **aux cyber-risques** *(avec les systèmes de Wi-Fi publics et les réseaux électriques intelligents).*

Dans le secteur des transports, **des milliers d'alertes seraient déjà recueillies chaque jour dans le monde** *(Smart Cities World).* En effet, le constat est clair : 96% des sociétés de transports et de logistique pensent que l'IoT est l'initiative technologique la plus stratégique que leur organisation adoptera durant cette décennie.

Celle-ci apporte **des solutions tout à la fois innovantes et peu coûteuses** pour l'optimisation de la gestion logistique *(ex : traçabilité des produits, contrôle de la chaîne du froid...).* **La chaîne logistique gagne en souplesse** et permet une adaptation en temps réel de la fourniture à la demande, tout en permettant de gérer la volatilité de la demande, la personnalisation du service client, et une meilleure traçabilité.

L'industrie de la logistique a été pionnière des solutions de traçabilité *(avec Walmart notamment)* : les sociétés de livraison suivent leur colis en quasi-temps réel grâce à une infrastructure faite de code-barres et de lecteurs.

A titre d'exemple, dans le cas du transport de denrées alimentaires, **des capteurs assurent que la chaîne du froid est bien respectée.** Toute interaction frauduleuse avec un tel système remet en cause sa raison d'être. Il convient donc de mettre en place des capteurs de confiance, dont le développement aura pris en compte de manière approfondie le besoin de sécurité : **Security-ByDesign.**

4.3.5 Smart Vehicle

Le déploiement des véhicules connectés ne pourra se faire sans une profonde fiabilisation et sécurisation des réseaux de télécommunications. La sécurité routière exige en effet un échange d'informations hautement réactif et fiable entre véhicules voisins, dans n'importe quelles conditions de densité de circulation. Les données collectées par les véhicules sont considérées comme hautement prioritaires *(disponibilité en temps réel)* car sécuritaires en situations d'urgence, d'événements fortuits ou d'évitement de collision. **Le défi est donc de concevoir des moyens de communications sans fil fiables dans des scénarios présentant de fortes densités.**

Et dans le cadre d'une utilisation générale, il faudra prendre en compte l'hétérogénéité des réseaux de communication : les réseaux cellulaires, les réseaux maillés de faible puissance, le WiFi *(faible consommation)* et la technologie Bluetooth *(faible puissance)* peuvent répondre à différents besoins de communication d'un véhicule connecté. Chacun, cependant, utilise des compromis différents entre la fiabilité, la consommation d'énergie et le débit. Il est donc nécessaire **d'étudier les limites de chaque technologie** et d'élaborer des critères clairs pour sélectionner celles **qui conviennent le mieux à chaque utilisation.**

Pour les véhicules connectés, la question de l'intégrité et de la confidentialité des informations qui circulent sur les réseaux se pose de manière critique. Un des pires scenari que l'on puisse envisager serait, par exemple, la prise de contrôle à distance d'un véhicule connecté. C'est pourquoi **la cybersécurité devient une priorité pour les industriels du transport.** Des moyens de protection existent déjà, mais il faut maintenant les intégrer au processus de développement des véhicules.

Les solutions de cybersécurité devront assurer :

- **la sécurisation des communications internes, des communications entre le véhicule et les systèmes d'information, ou des communications entre les véhicules, par chiffrement et signature**
- **le « durcissement » des calculateurs embarqués : protection des données et des programmes**
- **plus globalement, la sécurisation des systèmes d'information impliqués dans la circulation des véhicules autonomes et connectés**
- **des fonctions de pare-feu *(firewall)* dans les interfaces avec les réseaux extérieurs, la détection des intrusions et la mise en place de protections**
- **L'authentification du conducteur en cas d'accès mains libres à son véhicule et vulnérabilité aux attaques**

4.4 Opportunités marché liées aux évolutions réglementaires et sociétales

Cinq enjeux semblent importants pour les activités de la filière et peuvent constituer des atouts pour les acteurs qui sauront s'en emparer :

CINQ ENJEUX

LA PROTECTION DES DONNEES PERSONNELLES

L'Européanisation du Marché est encadrée et boostée par des règlementations adaptées comme le Règlement Général pour la Protection des Données *(RGPD)* en 2018, la directive ePrivacy. Ces réglementations ont donné un cadre très clair et structurant pour les entités utilisant, traitant et stockant des données personnelles et nécessitent l'utilisation de solutions numériques sécurisées.

Les composants électroniques, les objets structurant les services numériques, l'informatique des entreprises et les réseaux de communication devront intégrer ces fonctions de sécurité. Les **technologies de chiffrement, de contrôle d'accès, la gestion des logs** s'en trouvent impactés et permettront aux applications les utilisant de manipuler les données en toute confiance.

Le RGPD constitue pour les acteurs SCS experts en sécurité une forte opportunité de développement de leur business et contribuer ainsi aux politiques de sécurité et aux formations sécurité devenues une exigence.

CERTIFICATION SECURITAIRE DES OBJETS IoT

De nombreuses attaques récentes ont montré notamment l'étendue de la menace et les dangers d'un IoT sans sécurité. La commission Européenne, appuyée notamment par les travaux de l'ECSO, d'Eurosmart, de l'AIOTI, l'ANSSI en France, a proposé récemment un nouveau règlement concernant la sécurité numérique, CyberSecurity Act visant à proposer des processus et méthodes pour évaluer le niveau de sécurité de produits et notamment ceux de l'IoT en s'inspirant des méthodes qui ont fait le succès de l'industrie de la carte à puce.

Les composants électroniques et notamment les microcontrôleurs utilisés dans les objets et Gateway IoT devront offrir les bons niveaux de sécurité pour que les objets et produits IoT les utilisant puissent obtenir les certifications nécessaires. Ce projet de règlement est une opportunité majeure pour les acteurs français *(dont les membres SCS)* et est une formidable opportunité d'accélération pour le marché des acteurs de l'IoT et de la sécurité numérique.

SECURITE DES RESEAUX ET DES SERVICES

A. Directive de « cybersécurité » NIS : cette directive sur la sécurité des réseaux et des systèmes d'information impose aux fournisseurs de services pour des personnes citoyennes de l'UE de notifier tout incident de sécurité et d'assurer la continuité du service.

B. Le eIDAS : est un règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. La sécurité des infrastructures et des applications doit être conforme.

TRANSITION ECOLOGIQUE ET ENVIRONNEMENTALE

La mesure de la qualité de l'air intérieure *(bâtiments)* et extérieure *(centres urbains, surveillance côtière, détection des incendies)* requiert le développement de nouveaux capteurs/multi-capteurs de gaz *(CO, CO2, ozone, COV, SO2)* à faible consommation et la mise au point de systèmes de capteurs intelligents.

Ces développements seront basés sur les procédés microélectroniques classiques, intégrant de nouveaux matériaux sensibles et nécessitant la mise au point de nouvelles architectures de dispositifs, circuits et systèmes sécurisés.

RASSURER SUR LES USAGES DE LA SECURITE

La montée en puissance de l'utilisation des objets connectés dans le cadre de notre vie de tous les jours *(chez soi, dans la rue ou au travail…)* doit conduire :

- à des actions de communication et de formations vers les utilisateurs dans le contexte de l'IoT « BtoB » puis « BtoC ».
- à des actions de prise en compte de la sécurité dès la conception des produits *(privacy by design).*
- et à des actions de sensibilisation dans le cas du grand public.

Il est également critique que les grands industriels du domaine, et en particuliers du Pôle SCS, maintiennent leur implications dans les grands comités de standardisation et de normalisation *(GS1, Afnor, ETSI…)* où se dessine également le futur cadre éthique *(traçabilité, anonymisation et manipulation des données sensibles …)* qui sera associé à ces futurs usages.

4.5 Opportunités sur quelques domaines d'application transverses MAJ*

Des opportunités marché apparaissent sur des domaines d'application majeurs qui sont pour la plupart présents dans chacun des marchés prioritaires listés ci-dessus. Ces domaines d'application des technologies de sécurité numérique sont détaillés ci-dessous.

• La sécurité comme un service *(SaaS : Security as a Service)*

L'adoption d'une approche "security by design" s'accélère avec la crise COVID-19.

Malgré tout, on observe que la gestion du cycle de vie d'un produit est rarement prise en compte dans le choix des solutions de sécurité.

La gestion du cycle de vie commence au début et se poursuit jusqu'à la mise hors service d'un produit. Il est recommandé pour chaque étape d'aborder l'ensemble des thématiques sécurité pertinentes : sécurité réseau, applicative, matérielle, détection et réaction, gouvernance, maintien en condition de sécurité…

Pour les fabricants de produits, ces solutions de sécurité sur toute la durée de vie peuvent s'avérer difficiles à développer, à installer, à opérer et à maintenir.

Aussi le marché demande des solutions simples, déjà qualifiées, durables et qui assurent un haut niveau de protection.

Des acteurs du marché de la sécurité tentent d'apporter une réponse à cette demande avec des offres de services de sécurité dans le cloud.

Ces services permettraient, à distance et de manière sécurisée :

- de programmer les mises à jour des logiciels, des clés, des certificats ou autres données
- de garantir un démarrage sécurisé du produit
- de réaliser des analyses de sécurité
- de révoquer un produit, etc…

Ces nouveaux services de sécurité s'accompagnent souvent d'un nouveau business model, à savoir un abonnement mensuel ou annuel par produit pour l'accès à tel ou tel service de sécurité.
Ici pour la sécurisation de produits tout au long du cycle de vie, nous ne parlons plus de CAPEX mais d' OPEX ce qui peut présenter un intérêt pour certains fabricants.

Ces services de sécurité commencent à apparaitre mais le parcours est encore long pour avoir une offre de services de sécurité complète, accessible et déployable sur un très grand nombre d'objets ou de matériels.

• Sécurité de la chaîne d'approvisionnement & traçabilité associée

Dans les phases de développement et de fabrication d'objets connectés, les acteurs sont exposés à de réels risques : introduction de fausses données ou de code malveillant, collecte d'informations critiques comme le code de l'application par des tiers ou des certificats de sécurité.

L'écosystème de fabrication moderne et les flux de données/produits entre les parties prenantes y compris celles à l'international, expose les entreprises de l'IoT au vol de propriété intellectuelle, à la contrefaçon, au vol de données de grande valeur *(par exemple des données secrètes injectées à l'étape de fabrication)* ou à l'introduction de logiciels malveillants.

L'objectif serait de construire des infrastructures et des applications « robustes » de la conception au déploiement où des acteurs malveillants seraient limités dans leur capacité à manipuler la chaîne logistique. A tout le moins, toute altération de produit au cours d'une étape de la chaîne doit pouvoir être facilement et systématiquement détectée dans les étapes ultérieures. La création d'une «chaîne d'approvisionnement de confiance » pourrait permettre aux acteurs de l'IoT de relever ces défis.

La gestion de la propriété intellectuelle critique dans le processus de développement, la gestion de clés sécurisées ciblées pour le développement, la fabrication et les applications *(Racine de confiance)*, le chargement sécurisé du firmware avec tous sous-traitants et dans tous pays, ne sont que quelques illustrations.

- **Sécurité du cycle de vie des objets :**

Les objets connectés peuvent être déployés pour une période très longue pouvant aller jusqu'à plus de 20 ans, période pendant laquelle personne ne les surveille.

Durant cette période de vie, le contexte de gestion de ces objets peut être amené à évoluer : changement de propriétaire, changement d'opérateur réseau ou d'opérateur services...

Les objectifs seront :

- une gestion fiable et sécurisée de l'identité numérique de l'objet durant tout son cycle de vie.
- la possibilité de mettre à jour de manière sécurisée le software de l'objet et/ou le protocole de sécurité sur le terrain durant toute la vie de l'objet.
- de protéger la propriété intellectuelle via un cloisonnement de l'IP pendant la durée du cycle de vie du produit.
- de gérer les vulnérabilités.

- **Sécurité des réseaux :**

Les techniques de sécurités traditionnelles se contentent de chercher du code malveillant pour le neutraliser.

Les cyber-assaillants utilisent d'autres techniques, y compris à partir des objets connectés : ils envoient des requêtes, génèrent des interactions inhabituelles entre les machines/objets connectés et les serveurs.

L'IA positionnée au cœur du réseau peut apporter une réponse en détectant ces comportements anormaux, en analysant le trafic et en signalant en temps réel les menaces.

- **Détournement des objets connectés :**

Les cyber-assaillants sont très intéressés par les objets connectés parce que ce sont des appareils pour lesquels il n'existe pas d'antivirus, qui sont peu surveillés mais qui fonctionnent pourtant comme des PC et des serveurs.

Un autre problème important posé par les objets connectés est que personne ne pense à leur appliquer des mises à jour de sécurité.

L'exemple le plus simple est celui de caméras de vidéosurveillance qui ont été hackées parce que personne n'avait songé à changer leur login et mot de passe par défaut *(« root » et « admin »)*.

Le cyber-assaillant s'est infiltré sur le réseau, a détecté la présence de caméras fonctionnant sous Linux et a simplement essayé par force brute des identifiants et des mots de passe. Il s'agissait d'équipements déployés en plusieurs milliers d'exemplaires par certaines entreprises et non protégés par des systèmes de sécurité classiques.

- **Sécurité des capteurs :**

Au-delà de l'authenticité et de l'authentification de l'objet connecté et de la protection des données transmises, la validité du capteur et de la mesure soulèvent des points de sécurité. S'agit-il d'une bonne ou vraie mesure ?

Au niveau d'une plateforme IoT hardware, cela soulève aussi le point de la sécurisation de l'information entre le capteur et le microcontrôleur. L' IA au niveau de l'objet pourrait apporter une réponse.

- **Sécurité OT *(Operational Technology – Devices & Softwares)* :**

OT est l'utilisation de systèmes informatiques pour surveiller ou modifier l'état physique d'un système, tel que le système de contrôle d'une centrale ou le réseau de contrôle d'un système ferroviaire. Comme indiqué plus haut, les priorités, les problèmes et les solutions de sécurisation diffèrent en partie de ce à quoi le monde "IT" *(Information Technology")* est habitué.

Il est notamment fréquent d'être confronté à de fortes contraintes temps réel ainsi qu'à une réticence au déploiement de solutions de sécurité par des opérateurs peu sensibilisés à la problématique sécurité et plus habitués à traiter de fiabilité, disponibilité et sûreté de fonctionnement.

Une simple transposition des solutions existantes pour le monde IT au monde OT n'est donc pas une approche satisfaisante. De nouveaux défis et verrous technologiques sont à considérer. Des solutions et produits ont commencé à apparaître mais un grand chemin reste à faire.

- **Gestion des identités numériques et des données associées :**

Les technologies de base de gestion des identités permettent de gérer les cycles de vie des services numériques d'une organisation. Ces technologies[10] permettent de se protéger des cyber attaques, de l'ursupation d'identité et de toute tentative de fraude autour des données.

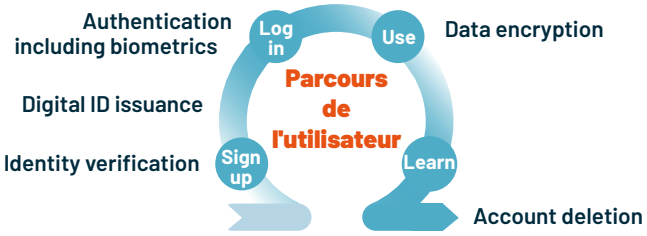
10 Video sur la gestion des identités numériques : https://youtu.be/Aj0954nlvi0

Ci-dessous une image illustrative de la gestion du cycle de vie des services numériques d'une organisation :

Toute organisation en cours de transformation digitale génère de gros volumes de données et des interactions numériques. Cela amène à des cyberattaques de plus en plus nombreuses. Des solutions de confiance numérique tout au long du cycle de vie du service numériques sont nécessaires pour empêcher le vol d'identité et l'usage frauduleux de données.

Confiance numérique exigée

Tout au long du cycle de vie du service numérique



5. Verrous et enjeux technologiques

5.1 Etat des lieux

Le Pôle SCS a déjà lancé plusieurs initiatives et place la sécurité au cœur de sa feuille de route 2019-2022. Il est critique d'un point de vue national et même européen de garantir notre indépendance technologique et l'innovation restera toujours un vecteur permettant de préserver cette souveraineté *(supra)* nationale.

La Stratégie R&D de SCS sera déclinée sur l'axe Sécurité et va permettre ainsi de générer des avancées technologiques dans ce domaine clé. Les projets collaboratifs des acteurs de SCS viseront à lever des verrous technologiques afin de renforcer la compétitivité des acteurs et de faciliter les usages dans les marchés cibles.

Les principaux verrous technologiques identifiés feront l'objet des travaux de R&D pendant cette phase 4.0 et permettront de renforcer et développer les positions des acteurs.

Bon nombre d'entre eux sont liés à la sécurité pour l'internet des objets *(IoT)* : c'est en effet le challenge majeur. Les attaques sont relativement simples *(beaucoup d'objets n'ont pas été conçus de façon sécurisée)*, intrusives *(y compris dans nos vies privées)* et représentent un impact potentiel important en raison de la quantité d'objets connectés disponibles, ce qui augmente la surface d'attaque.

De nombreuses thématiques sont adressées par les équipes de recherche en région. Parmi les axes de recherche *(adressés par l'écosystème SCS et non rangés par priorité ci-dessous)*, nous pouvons citer :

Les verrous prioritaires

1. **Implémentation d'algorithmes cryptographiques légers, contre-mesures et protections à faible impact énergétique.**
2. **Cryptographie post-quantique.**
3. **Développement et concepts d'architectures de sécurité, personnalisables et adaptables.**
4. **Personnalisation des objets IoT, distribution de clés, cycle de vie d'un objet connecté, Mise à jour sécurisée.**
5. **Sécurisation et confiance des systèmes à base d'IA embarquée.**
6. **Mécanisme de démonstration de l'intégrité des différents éléments HW, FW et SW composant le produit fini.**

Les verrous secondaires

1. **Développement de logiciels pour protection et défense des plateformes mobiles.**
2. **Intégration de système IDS à base d'IA dans les passerelles et « en bordure » de réseau.**
3. **Utilisation de protocoles blockchain dans l'IoT.**
4. **Evaluation et validation du niveau de sécurité des nouvelles technologies de fabrication.**
5. **Les calculs à base de données chiffrées.**

5.2 Les verrous prioritaires MAJ*

Seuls les verrous prioritaires font l'objet d'un bref descriptif dans les sous-chapitres **ci-dessous.**

1 Implémentation d'algorithmes cryptographiques légers, contre-mesures et protections à faible impact énergétique.

La forte croissance des objets connectés évoluant dans un environnement énergétique contraint a fait émerger des enjeux liés à à leur alimentation, mais aussi à leur consommation.

La stratégie de sécurité des objets connectés doit donc tenir compte de cette contrainte. Dans ces objets connectés, les algorithmes de sécurité standardisés les

plus communément utilisés *(AES, RSA, etc...)* doivent être remplacés par des algorithmes de chiffrement *(symétriques, asymétriques, hachage)* moins énergivores. Si des solutions ont été proposées, sont soumises à des tests *(concours NIST par exemple)*, l'utilisation de ces algorithmes n'est pas encore généralisée.

En effet la sécurité d'une implémentation, matérielle ou logicielle, sur le composant doit être garantie. Des contremesures associées doivent donc être proposées, elles aussi à faible empreinte énergétique. La prise en compte des spécificités de la cible *(8 bits ou 32 bits, implémentation matérielle ou logicielle, etc...)* guidera vers la spécification d'un couple algorithme/protection dédié.

2 Cryptographie post-quantique.

Les enjeux associés à la cryptographie post-quantique ont évolué depuis 2019 et ont été précisés dans le rapport « Quantique : le virage technologique que la France ne ratera pas » piloté par la député Forteza *(Janvier 2020)*. Ce rapport a préfiguré le plan national quantique dévoilé par le président E. Macron, plan qui prévoit un volet de 150 millions d'euros pour la partie cryptographie.

IBM se lança le premier dans cette course, avec un ordinateur à 2 qbits en 1998. Actuellement, ils sont les premiers à annoncer la commercialisation d'un ordinateur à 20 qbits, et ont démontré avoir su préserver ceux-ci dans un état quantique pendant 90 µSecondes. Intel et Google ne sont pas en reste et annoncent travailler de leur côté à des alternatives...

Nous sommes désormais à l'aube d'une nouvelle ère qui verra l'ordinateur quantique remplacer certains ordinateurs conventionnels en venant résoudre les problèmes que ces derniers ne sont pas en mesure de solutionner en des temps raisonnables.

Il est donc indispensable de travailler dès aujourd'hui sur le sujet de la cryptographie post-quantique sans quoi certains systèmes actuels deviendraient **« hackables »** de manière très simple.

En effet les algorithmes de cryptographie actuels ne résisteront pas à la puissance de calcul des ordinateurs quantiques. Si un certain nombre de solutions sont proposées, elles se heurtent pour le moment aux problématiques d'implémentation sur composants, et leur impact sur les performances.

Les designs des antennes et des puces doivent prendre en compte ces contraintes au sein d'environnement parfois contraints *(miniaturisation, source d'énergie contrainte, fonctionnement en environnement sévère, ...)*

Même si le problème ne sera réel que dans quelques années, il est important de trouver des solutions dès maintenant pour deux raisons :

- **pouvoir déchiffrer :** même dans plusieurs années, certaines données actuelles peut représenter un véritable risque pour certains opérateurs.
- **Dans certains domaines :** les matériels déployés restent en activité durant de très nombreuses années *(ex. satellite)* et il convient d'anticiper le risque post quantique dès maintenant.

3 Développement et concepts d'architectures de sécurité, personnalisables et adaptables.

Si de nombreux progrès ont été faits en termes de conceptions d'architectures de sécurité, à tous niveaux *(systèmes électroniques, réseaux informatiques, contrôle d'accès dans des systèmes fédérés, etc.)*, il n'en reste pas moins vrai que cette activité reste plus un art qu'une science. Les processus de conception, lorsqu'ils existent, sont souvent très spécifiques à un environnement donné et peu amènes à des changements ultérieurs.

La mise en œuvre d'une sécurité facile à utiliser, à personnaliser est un but à poursuivre. La prise en compte d'utilisateurs non experts est impérative, de même que l'utilisation de données qui pourraient s'avérer être erronées, que ce soit de façon accidentelle *(senseur défaillant)* ou intentionnelle *(fake news)*.

Concevoir, pour des non experts et à un coût raisonnable, des systèmes dont l'architecture, par design, permettent d'assurer un haut niveau de sécurité et, ce, dans des conditions changeantes et/ou hostiles à leur fonctionnement est un défi qui nous est posé.

4 Personnalisation des objets IoT, distribution de clés, cycle de vie d'un objet connecté, mise à jour sécurisée des logiciels, protection d'IP logiciel.

La prise en compte de la sécurité dans les spécifications initiales de développement des objets ne cesse de croitre. Néanmoins une sécurisation focalisée sur l'objet et son application expose toujours les acteurs à de réels risques en phase de développement, de fabrication et de personnalisation, de gestion des mises à jour des logiciels de l'objet durant son cycle de vie.

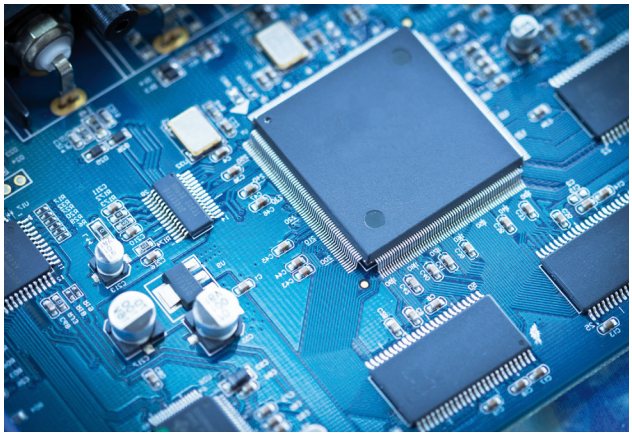
Quelques illustrations de risques auxquels les acteurs sont exposés en fabrication: introduction de fausses données ou de logiciels malveillants, vol d'informations critiques comme le code de l'application par des tiers *(vol de propriété intellectuelle)*, vol de clés secrètes ou de certificats de sécurité, etc...

Notre écosystème demande une prise en compte plus globale de la sécurité avec une approche systémique qui ne soit limitée à la sécurité de l'objet et de son application. L'objectif sera de développer des solutions de sécurité englobant toute la chaîne d'approvisionnement du développement jusqu'au déploiement et englobant aussi une gestion sécurisée de l'objet durant tout son cycle de vie une fois déployé.

Ces solutions passeront entre autres par le déploiement d'infrastructures et d'applications « robustes » dédiées à une chaîne logistique sécurisée.

Nous citerons principalement : la sécurisation de la génération et de l'injection des secrets dans l'objet *(personnalisation/ provisioning)* en usine ou sur le terrain, la programmation sécurisée du logiciel de l'objet en usine ou durant les mises à jour sur le terrain.

De telles solutions répondront aussi à la demande croissante de la protection de la propriété intellectuelle des logiciels dans un écosystème de fabrication moderne avec des partenaires et des sous-traitants multiples et à l'international.



5 Sécurisation et confiance des systèmes à base d'IA embarquée.

L'utilisation de l'intelligence artificielle *(IA)* dans les systèmes numériques se généralise et cette généralisation s'accompagne par un besoin de calculs déportés au plus près du terrain *(edge computing)*. Les composants doivent s'adapter à ces nouveaux besoins. Cependant les algorithmes d'IA, et plus spécifiquement d'apprentissage profond de type réseaux neuronaux, sont sensibles à de nombreuses menaces comme le témoignent un certain nombre de travaux *(Google, Stanford, etc...)*.

Les attaques les plus réputées sont les adversarial examples, en mesure de mettre en défaut un réseau de neurones, pour une application de reconnaissance d'image par exemple, avec une simple modification de la donnée d'entrée qu'une intelligence humaine ne saurait déceler.

D'autres études ont fait état de risque visant la confidentialité des données et des modèles d'apprentissage. Finalement les 3 piliers de la sécurité que sont intégrité, confidentialité et accessibilité sont menacés. Il conviendra donc de trouver des protections efficaces, et en adéquation avec les cibles qui exécutent ces algorithmes d'intelligence artificielle.

6 Mécanisme de démonstration de l'intégrité des différents éléments HW, FW et SW composant le produit fini.

Il est très important de pouvoir vérifier et démontrer en permanence tout au long de la vie de tous les produits communicants sécurisés *(IoT, etc...)* **l'intégrité/authenticité** de chacun des éléments composants le produit - ceci afin de garantir l'absence de chevaux de Troie et de faiblesses aussi bien lors d'interactions et **d'échanges de données** avec le produit que lors de ses mises à jour de parties logicielles *(HW ou SW)* ou suite à des réparations de parties HW.

Pour cela, il faut que chacun des éléments, aussi bien HW que SW, composant le produit puisse stocker des **éléments d'identité/« signature » non falsifiables** et communicables dans un agrégat « produit » conservé à la fois en local et utilisable en réseau, **intégrable** dans des systèmes *(style blockchain par exemple ou autres)*.

Au-delà, de ces preuves d'identité de chacun de ces éléments, il faudra aussi trouver rapidement comment mettre en œuvre au niveau de l'architecture globale du produit des mécanismes de **détection d'ajout d'éléments exogènes non conformes** au design initial et qui pourraient générer des fuites et/ou des **corruptions de données** afin de pouvoir rejeter son intégration dans les réseaux et surtout sa prise en compte dans les analyses IA des big data associées.

6. Formation

6.1 Etat des lieux MAJ*

6.1.1 Introduction

Face à l'explosion des systèmes d'informations et la multiplication des données numériques, les entreprises cherchent à la fois à sensibiliser leurs personnels et à recruter des experts en sécurité.

S'ils visaient auparavant majoritairement des secteurs sensibles, à l'image des banques, les pirates informatiques se tournent aussi vers d'autres domaines, tout aussi cruciaux pour l'économie mondiale. Réseaux ferroviaires, distribution de gaz, systèmes d'approvisionnement en eau sont les nouvelles cibles.

Conscient de l'enjeu, le ministère de la Défense signait, en février 2014, un pacte Défense cyber, faisant de la cybersécurité une priorité nationale. En parallèle de cette volonté politique, les établissements d'enseignement supérieur se structurent pour offrir des formations qui répondent aux besoins du marché. Car plus qu'ailleurs, la recherche de personnel qualifié et formé aux nouvelles spécificités du domaine est devenue une préoccupation majeure.

Face à l'urgence de la situation, bon nombre d'entreprises cherchent à recruter et former rapidement tout leur personnel aux questions de sécurité numérique. Pour cela, elles se tournent notamment vers les établissements ayant mis en place des offres de formation initiale et continue.

Pour répondre à cette demande, l'académie d'Aix-Marseille, en lien avec la Région Provence-Alpes-Côte d'Azur et Industries méditerranée ont obtenu le label d'excellence pour le Campus des Métiers et des Qualifications « Industrie du Futur – Sud » *(CMQ)*, qui comprend la filière industrielle de la microélectronique, ainsi que les filières énergie et aéronautique.

Ce CMQ a pour vocation de mettre en place des formations jusqu'à BAC+8 afin de proposer aux entreprises de trouver les collaborateurs formés dont elles ont besoin, sous la forme d'un catalogue des formations en cours de réalisation.

Ce label permet en particulier de répondre à des appels à projet nationaux. Ainsi, le projet I-NOVMICRO, financé dans le cadre du PIA3, soutenu par SCS, permettra de développer de nouvelles formations sur toute la chaîne de valeur de la microélectronique et de réaliser des investissements pour la mise en œuvre d'un jumeau numérique pour l'apprentissage des procédés de fabrication électronique, et pour l'installation d'une « salle blanche formation » sur le campus de Mines Saint-Etienne à Gardanne.

6.1.2 Formations certifiantes en Région SUD

La région Sud est un territoire historiquement riche sur le sujet de la Sécurité Numérique avec des industriels pionniers dans le domaine. C'est tout naturellement que ecoles et universités ont développé des formations autour de ce sujet central pour les industriels.

Plusieurs formations initiales *(formations universitaires délivrant un grade de Licence ou Master, formations d'ingénieur dont le diplôme est reconnu par la CTI (Commission des Titres d'Ingénieur)* ainsi que les Mastères spécialisés reconnus par la CGE *(Conférence des Grandes Ecoles)*, dans le domaine de la sécurité du numérique répondent à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine.

L'ANSSI a réalisé un référencement *(non exhaustif)* des formations délivrant un titre reconnu par l'Etat de niveau équivalent à Bac+3 jusqu'à Bac+5. L'ANSSI délivre un label SecNumEdu[11] aux formations en cybersécurité de l'enseignement supérieur.

On peut citer en Région SUD entre autres :

Aix*Marseille université	l'université **AMU**[12] à Aix-Marseille qui s'appuie sur les travaux du laboratoire l'IM2NP
CENTRALE MARSEILLE	**Ecole Centrale**[13] à Marseille
MINES Saint-Étienne	**Mines Saint Etienne**[14] ***(MSE)*** à Gardanne qui a créé une Equipe Commune de recherche avec le CEA Leti
EURECOM	L'école d'ingénieurs **EURECOM**[15] à Sophia Antipolis
UNIVERSITÉ CÔTE D'AZUR	**L' UCA**[16] Université de Nice Sophia Antpolis
ISEN ALL IS DIGITAL yncréa	**Yncrea/ISEN**[17] L'Institut Supérieur de l'Electronique et du Numérique à Toulon *(IM2NP également)*
POLYTECH MARSEILLE Aix*Marseille Université	**Polytech**[18] à Marseille

- Mais aussi à proximité, en Occitanie, avec **l'université de Montpellier**[19] *(UM)* et son laboratoire de référence, le LIRMM, qui propose des formations labélisées **SECNUM**[20]

La liste des formations cartographiées en région est fournie dans le tableau **page 24.**

11 https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/
12 https://www.univ-amu.fr/
13 https://www.centrale-marseille.fr/
14 https://www.mines-stetienne.fr/formation/ismin/
15 http://www.eurecom.fr/fr
16 http://www.univ-cotedazur.fr
17 https://www.isen.fr/campus/ecole-ingenieurs-toulon/
18 https://polytech.univ-amu.fr
19 https://www.umontpellier.fr/
20 http://web-pcm.cnfm.fr/secnum/

Cartographie des formations BAC+3 à 5 dispensées dans les établissements d'enseignement supérieur en région SUD, labellisés SecNumEdu pour certains :

NOM DE L'ORGANISME	NOM DE LA FORMATION	TYPE	FORMATION INITIALE	FORMATION CONTINUE	LABEL SECNUM-EDU
Aix-Marseille Université	« Administration et sécurité des réseaux d'entreprises »	Licence pro	X	X	
Aix-Marseille Université	Master Informatique parcours Fiabilité et Sécurité Informatique	Master	X		X
Centrale Marseille	Ingénieur centralien, Option Digital.e	Master Spé CGE	X		
Centrale Marseille	Mastère Spécialisé *(MS)* nommé « Cybersecurite des systèmes complexes pour l'industrie et la défense » Rentrée septembre 2019*	Ingénieur	X		
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	Ingénieur	X	X	X
EURECOM	Master Sécurité Numérique	Master	X		X
Mines Saint-Etienne, cycle ISMIN à Gardanne	Ingénieur Spécialité Microélectronique et Informatique – option Mobilité & Sécurité	Ingénieur	X		X
Mines Saint-Etienne	Master spécialisé, Designer of Secure devices for IoT	Master Spé CGE	X		
Polytech Marseille	Ingénieur Microélectronique et télécommunications	Ingénieur	X		
Polytech Nice	Ingénieur électronique	Ingénieur	X		
UCA Université Nice Sophia Antipolis	Licence Professionnelle Sciences, Technologies, Santé - Mention : Réseaux et télécommunications - Spécialité : Réseaux sans fil et sécurité	Licence pro	X	X	
UCA Université Nice Sophia Antipolis	Ingénieur « Cryptographie, Sécurité, et vie Privée dans les Applications et Réseaux »	Ingénieur	X		
Yncrea/Isen Toulon	Cybersécurité : Protéger et sécuriser les systèmes d'information des entreprises et organisations Réseaux, communications mobiles et objets connectés	Ingénieur	X		

**Rentrée possible en Septembre 2021*

6.1.3 Les nouveaux métiers autour de la sécurité

L'évolution des compétences et des métiers en sécurité nécessitent une adaptation des cursus de formation pour les actuels et futurs professionnels.

Filière particulièrement dynamique, la formation se doit d'être à la pointe des technologies voire moteur de ces transformations par des programmes performants à la fois sur la formation initiale et continue.

Les métiers évoluent et on constate une évolution des compétences existantes et l'émergence de nouveaux métiers :

- **Digital Risk Manager-Officer**
- **Pilotages de prestations extérieures en cybersécurité**
- **Cloud Manager**
- **Expertise sécurité pour PME et TPE**
- **Juriste cybersécurité**
- **Consultants cybersécurité systèmes spécifiques *(industrie, énergie, transport...)***
- **Risk cybersécurité manager**
- **Sécurisation des applications mobiles et objets connectés**

Certains organismes généralistes proposent des formations « courtes » en cybersécurité :

- Des organismes de certification en cybersécurité *(Cloud security Alliance)*
- Des organismes généralistes *(AFNOR par exemple)*

Les règlementations citées dans le chapitre 4 ont un impact sur les marchés mais aussi sur certains métiers de la sécurité :

- **Le RGPD**
  Délégué à la protection des données *(DPD)* - Responsable de la Sécurité des Systèmes d'Information *(RSSI).*
- **La directive de « cybersécurité » NIS**
  Responsable de la Sécurité des Systèmes d'Information *(RSSI),* Analyste CERT.
- **Le eIDAS**
  - Responsable de la Sécurité des Systèmes d'Information *(RSSI)*
  - Développeur sécurité
  - Cryptologue

6.2 Enjeux autour de la formation

Les entreprises font face à plusieurs difficultés :

- difficultés de recrutement car les besoins sont supérieurs aux candidats adéquats disponible.
- difficulté des entreprises à « **retenir** » des salariés « **cryptographe** » ou expert en sécurité « **analogique** ». Ces experts *(ingénieurs ou docteurs)* quittent facilement la région pour rejoindre l'europe du Nord notamment.
- Difficulté d'engager le personnel à se former à la sécurité.

Suite à plusieurs constats et à la lecture d'un rapport sur les formations en cybersécurité[21], les enjeux de formation en sécurité se résument ainsi :

- L'adossement des nouvelles formations avec les plans de formation continue des entreprises locales de la filière Sécurité numérique ou avec un service adéquat *(Gemalto (Thalès company),* STMicroelectronics, HPE, CMA CGM, Airbus Helicopters, Safran, Thalès Alenia Space...
- La mise en capacité de répondre à la demande toujours croissante de montée en compétences des salariés *(ou futurs salariés)* de tout âge et notamment d'alternants de niveaux Bac+2 à Bac +5.
- La possibilité de pourvoir aux offres d'emploi très spécialisées *(Cryptologue,Digital Protection Officer, Digital Risk Officer...).*
- La création de programmes pédagogiques permettant aussi bien de comprendre les méthodes d'attaques et de piratage d'informations que les mesures à adapter concernant les usages numériques *(mail, cloud...)* pour une meilleure sécurité des informations de l'entreprise.
- L'attractivité de la filière Sécurité *(traité en chapitre 8).*

21 CF Rapport Les formations et les compétences en France sur la cybersécurité 2017

7. Soutien & croissance des Startups & PME

7.1 Etat des lieux

Dans le cadre de la nouvelle PHASE 4.0 des Pôles de Compétitivité, SCS renforce son action d'innovation et de soutien aux startups et PME sur la thématique sécurité.

Les TPE/PME/ETI du Pôle SCS doivent dans les 4 années à venir aboutir à une accélération et amplification de leur croissance et création de valeur.

Cette ambition concerne les startups et PME de l'écosystème du Pôle qui ont des profils variés et sont positionnés sur certains maillons de la chaîne de valeur des offreurs de solutions :

- de sécurité matérielle
- de sécurité logicielle embarquée
- de sécurité hybride
- de solutions Blockchain
- d'administration de la sécurité
- de simulation et de protection contre les attaques
- de certification
- .....

On constate que :

- Les PME européennes ont un risque très élevé de perdre leur IP et leurs données de valeur à cause d'un manque de préparation aux attaques et piratages d'informations.
- Face au développement des technologies asiatiques et américaines, le besoin de solutions de sécurité numérique « **Made in Europe** », compétitives et à la pointe de la technologie devient un enjeu majeur de la confiance économique. Les créations de startups et d'essaimage proposant des produits ou service pour la sécurité et confiance numérique en lien avec la croissance de la filière[22] - sont encore trop faibles.
- Une évolution de l'offre des startups et PME existante vers le développement d'offres globales de Sécurité.
- Certains segments tels que la sécurisation des voitures connectées bénéficient d'une croissance de l'ordre de 7% à 10% sur la période 2013-2017.
- Une augmentation des tentatives de piratage de données et une prise de conscience *(tardive)* des PME de la nécessité de sécuriser leurs procédés.

7.2 Enjeux

Les principaux enjeux pour les startups & PME se résument ainsi :

- Augmentation du niveau de protection des PME en région, avec les **solutions de sécurité et confiance numérique appropriées** *(produits, services, infrastructure).*
- **Souveraineté EU :** Accroitre l'autonomie et la souveraineté de l'Union Européenne en sécurité numérique en impliquant les opérateurs européens et les utilisateurs dans l'identifications des besoins et des spécifications à destination des startups & PME offreuses de SCS.
- **Achat public :** Accroitre la demande « intra » européenne et favoriser les politiques publiques d'achat de solutions de sécurité innovantes des PME de SCS.
- **Régulation EU :** L'adoption des nouvelles régulations, comme GDPR et NIS, qui s'appliquent à tous les secteurs d'activité et permettent une meilleure lisibilité et offrent de nouvelles opportunités pour les PME conceptrices de solutions de sécurité *(reporting d'incidents harmonisé avec une même taxonomie, onthologie, template ...quelque soit le secteur).*
- Adéquation des offres des PME avec le marché qui évolue vers le développement d'offres globales de **Security as a Service** *(business model de service versus business model produit).*
- La promotion et le développement des concepts du **Security by Design** et de la **RGPD** pour sécuriser de bout-en-bout des procédés, processus....des entreprises régionales.
- Le positionnement des startups et PME SCS sur certains **marchés en croissance** et certains segments tels que la sécurisation des voitures connectées *(de l'ordre de 7% à 10% sur la période 2013-2017)*, l'Internet des Objets, les smart cities.
- La **fidélisation** et le maintien en région des experts en sécurité numérique, analogique et cryptologues[23] dans les PME régionales malgré l'attrait de meilleures conditions de travail hors région.
- La promotion de l'utilisation de **l' IA pour la sécurité** et la cybersécurité ainsi qu'une base de données partagées pour favoriser le développement de l'IA pour la sécurité et la confiance numérique.

22 9% de croissance moyenne annuelle pour la filière de la Confiance Numérique sur la période 2013-2017- Cette tendance forte devrait se maintenir sur la période 2019-2024 (Observatoire ACN 2019)
23 cf chapitre 6 de ce document « nouveau métier »

8. Visibilité, attractivité & communication

8.1 Etat des lieux

En raison de la diversité des PME françaises en matière de cybersécurité, les entreprises françaises ont des offres souvent moins lisibles et plus difficilement comprises par la clientèle, en particulier en comparaison des offres américaines. **Ce manque de lisibilité provient principalement de l'absence d'une offre française généraliste.**

La Région rassemble des compétences dans de nombreux domaines *(identification & authentification, gestion de l'identité, cryptographie, machine learning, deep learning, sécurisation des IoT et dans une moindre mesure blockchain)* mais elles ne sont pas assez visibles et les offres sont fragmentées et éparpillées.

- La filière Sécurité numérique de SCS, filière d'excellence à même d'attirer des talents français et européens sur une thématique différentiante, n'est pas bien visible et connue des grands donneurs d'ordre en Europe.
- Les formations existantes sont mal connues des entreprises et des étudiants et peu attractives.
- De nouveaux domaines subissent une transformation digitale et deviennent ultra connectés : les communications sécurisées deviennent de plus en plus importants dans ces nouveaux marchés en croissance: voiture connectée, smart home ou smart building, données médicales.
- De nouvelles règles et procédures d'achat de solutions de sécurité numériques pourraient favoriser l'adoption de ce type de solution par les acteurs publics comme privés.
- Les investisseurs et fonds de capital-risque ne sont pas friands des projets orientés sécurité numérique et n'ont pas toujours les compétences pour évaluer et accompagner les entreprises de ces domaines.
- Les propositions des startups et PMEs sont souvent orientées technologies alors que c'est l'intégration de la technologie dans les usages qui apportera la confiance.

8.2 Enjeux

Les enjeux de visibilité de l'ecosystème sécurité numérique et d'attractivité du territoire sont nombreux. On peut citer :

- **Standard et certification :** Les standards, certifications et technologies européennes deviennent globaux et vont s'imposer face aux standards américains. Tenir informé les acteurs SCS des décisions clés des organismes de standardisation et certification est majeur. Gagner en leadership et visibilité sur le domaine de la sécurité numérique est un objectif clé de l'Europe.
- **Attractivité de la filière :** Donner de la visibilité aux salaires attractifs de ces filières auprès des ingénieurs et docteurs jeunes diplômés et aux nombreuses formations existantes dans la région.
- **Vision européenne :** Le partage des roadmap des entreprises offreuses de solution avec d'autres entreprises européennes, pour favoriser les best - practice et la collaboration horizontale ou verticale entre les différents acteurs - notamment à travers les « **clusters Sécurité** » partenaires de SCS ou les « **Cybersecurity valleys** » identifiés par l'EU.
- **Secteur en croissance :** Le partage des nouveaux besoins en sécurité et confiance numérique dans les filières verticales en croissance comme : voiture connectée, smart home ou smart building, données médicales – notamment à travers les pôles et clusters « filière ».
- **Attractivité de l'expertise SCS :** faire bénéficier les grands groupes « **utilisateurs** » de solutions innovantes ou les grands événements à venir en France *(JO2024, Coupe du monde de rugby...)* de l'expertise SCS à travers des expérimentations déployables à grande échelle.
- **La souplesse des règles et procédures d'achat** notamment des gouvernements en europe et des organisateurs d'événements internationaux qui auront lieu sur le territoire français.
- **Le maintien des chercheurs** et freiner leur départ vers les entreprises privées souvent étrangères et maintenir les compétences académiques tout en assurant un transfert de technologie Sécurité numérique vers l'industrie.
- **La lisibilité** et promotion du **positionnement** et des offres des acteurs SCS *(domaine d'expertise).*
- **Les synergies** et les complémentarités **inter-clusters** positionnées sur la sécurité *(Cluster Sécurité)* et les clusters « filière » de la région.
- **L'identification** de solutions de **financement** en fonds propres pour les entreprises de sécurité numérique.

9. Plan d'actions

1

GÉNÉRER, VALORISER ET DÉPLOYER DES INNOVATIONS ET DES AVANCÉES TECHNOLOGIQUES

A Intensifier l'animation et la structuration de l'écosystème d'innovation :

1. Des conférences scientifiques à fort intérêt/participation des acteurs SCS *(ex : PHISIC)*
2. Des journées thématiques et des masterclass pilotées par des experts
3. Promotion des expertises, des ressources et moyens mutualisés

B Développer des projets de R&D innovants technologiques et usages :

1. Animer un groupe de travail pour mettre en avant les compétences technologiques, les plateformes mutualisées et des idées de projets innovants
2. Réunions d'informations sur les différents dispositifs de financement
3. Accompagnement et labellisation des projets R&D remontés par les acteurs SCS
4. Organiser des conférences marchés/usages notamment en partenariat avec d'autres pôles clusters marchés

C Valoriser les projets de R&D et leurs retombées :

1. Collecter et recenser les différents projets des membres SCS
2. Etablir un catalogue des projets et des produits issus des projets
3. Organiser des conférences et animations avec restitution des résultats des projets
4. Promouvoir le passage à l'industrialisation des prototypes et des produits issus des projets en s'appuyant notamment sur les plateformes mutualisées *(IoT center,CIMPaca...)*

2

ACCÈS MARCHÉ

A Accélérer l'accès sur les marchés en croissance :

1. Continuer et renforcer les partenariats avec les réseaux « utilisateurs » *(Pôles filière, IMA, cluster EE, Centre 3IA, Communauté FT, UIMM, Mercatel)* et partenaires *(centre 3IA : health, biotech, smart territories)*
2. Organiser des actions d'open Innovation avec les Grands Groupes et collectivités *(région, membre centre 3IA...)* et sourcing de solutions auprès de PME/startups
3. Organiser des animations & espaces d'échanges entre offreurs & End user d'un marché donné

3

SOUTIEN AUX PMES ET STARTUPS DE LA SÉCURITÉ NUMÉRIQUE

A **Accompagner la croissance & efficacité opérationnelle :**

1. Accompagner la création de startups *(briques technologiques, offres ou services à base de sécurité numérique)* en liaison avec les SATT et les incubateurs
2. Accompagner le renforcement du financement des startups et des PMEs notamment en fonds propres
3. Proposer un catalogue d'outils pour l'efficacité opérationnelle *(marketing, stratégie, pitch, salons, ...)*
4. Proposer des accompagnements pour les PME à des conférences et des salons majeurs nationaux et internationaux sur la sécurité numérique et les marchés associés
5. Mettre en avant des offres et compétences des startups et PMEs dans des catalogues thématiques *(ex : Industrie du Futur, Sécurité de l'IoT..)*

4

FORMATION

A **Accompagner le développement d'une offre complète de formation initiale et continue dans le domaine de la Sécurité numérique en liaison avec les campus des métiers et les besoins des industriels**

5

VISIBILITÉ & ATTRACTIVITÉ

A **Promouvoir l'expertise et les compétences de SCS auprès de la communauté scientifique internationale, des acteurs du marché et des décideurs :**

1. Continuer à communiquer et promouvoir les avancées des acteurs de SCS *(technologies, marché, contrat signé, projet...)*
2. Assurer la visibilité de la filière Sécurité numérique SCS dans les stratégies régionales *(OIR)*, nationale *(CSF industries de la Sécurité)* et Européenne

10. Annexes

10.1 Méthodologie et références

La feuille de route Sécurité du Pôle SCS a été réalisée avec un processus sur 3 mois qui repose sur des réunions physiques du comité restreint du Groupe de Travail et de la Plénière où tous les acteurs SCS ont été invités à participer.

Le comité restreint, composé d'industriels petits et grands et d'organismes de recherche localisés dans la région, a fortement **contribué au contenu** de la feuille de route.

Références

La feuille de route Sécurité s'appuie sur les résultats de différentes études récentes menées dans le domaine par des cabinets de veille, des comités public/privé spécialisés dans le domaine ou encore des centres de recherche mais aussi sur **des études menées par le Pôle SCS entre 2013 et 2018.**

10.2 Présentation du Pôle SCS

Le Pôle de compétitivité Solutions Communicantes Sécurisées *(SCS) (www.pole-scs.org)* est un acteur important et reconnu dans le domaine des technologies du numérique. Il rassemble plus de **300 membres** *(grands groupes, laboratoires de recherche et plus de 200 startups & PME)* en **Région Sud**, représentant **60 000 emplois** dans ce domaine.

Ces acteurs couvrent l'ensemble de la chaîne de valeur des métiers du numérique, du silicium aux usages :

microélectronique, télécommunications et logiciel. SCS se focalise sur **4 grands axes stratégiques** :

- **MICRO** Microélectronique
- **SECURITE** Sécurité numérique
- **IA** BigData & Intelligence Artificielle
- **IoT** Internet des Objets

pour servir des **marchés en croissance tels que la santé**, les smart-cities, le transport & logistique, l'Industrie 4.0, le retail, etc...

LISTE DES ÉTUDES EXTERNES RÉCENTES

- **Livre Blanc INRIA n°02** « Véhicules autonomes et connectés » Janvier 2019
- **Livre Blanc INRIA n°03** « Cybersecurity » Janvier 2019
- **Livre Bleu CoFIS** « Industries de sécurité : anticiper les ruptures technologiques » Septembre 2018
- **Rapport** « Les formations et les compétences en France sur la cybersécurité » en 2017

LISTE DES ÉTUDES MENÉES PAR LE PÔLE SCS ENTRE 2013 ET 2018[24]

- **Etude IA** « Intelligence Artificielle L'écosystème en région PACA » Mai 2018
- **Livre Blanc** « Sécurité & Identités Numériques » Mars 2013
- **Livre Blanc** « La Sécurité de l'Internet des Objets : un enjeu majeur » Septembre 2017
- **Livre Blanc** « Le marché e-santé » en 2015

24 https://www.pole-scs.org/publications/livres-blancs-etudes/

SCS est un acteur de dimension nationale et européenne. Nationale au travers de son réseau de partenaires et notamment **les Pôles Systematic, Minalogic et Images&Réseaux** avec lesquels il a signé une charte de collaboration Européenne grâce à son réseau de partenaires au sein de l'Alliance **« Silicon Europe »** *(www.silicon-europe.eu).*

SCS a reçu en 2013 le Label Gold, délivré par l'ESCA *(European Secretariat for Cluster Analysis)*, pour la qualité de l'animation de son écosystème, de son processus de labellisation et de son management.

10.3 Glossaire

ACN : Alliance pour la Confiance Numérique

AFNOR : Association française de normalisation

AIOTI : The Alliance for the Internet of Things Innovation

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CICS : Conseil des Industrie de la Confiance et de la Sécurité

COFIS : Comité de la Filière industrielle de sécurité

CSF SÉCURITÉ : Comité Stratégique Filière Sécurité

DSP : Digital Service Provider

ECSO : European Cyber Security Organisation

EIDAS : Electronic IDentification, Authentication and trust Services

ENISA : European Union Agency for Network and Information Security

ETSI : European Telecommunications Standards Institute

GS1 : Organisation mondiale de standardisation

IoT : Internet of Things

OES : Operators of Essential Services

RGPD : Règlement General pour la Protection des Données

RSSI : Responsable de la Sécurité des Systèmes d'Information

SIIV : Systèmes d'Information d'Importance Vitale

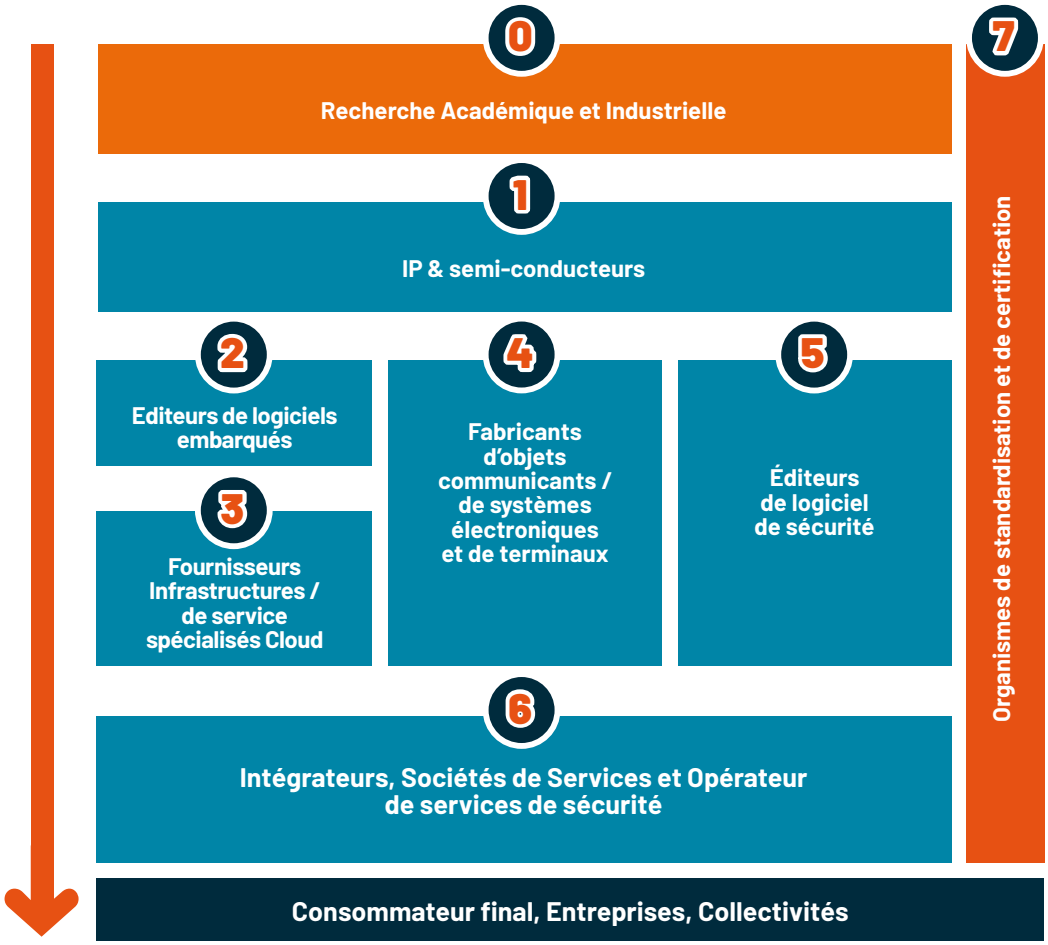
SIS : Systèmes d'Information Sécurisés

SSI : Sécurité des Systèmes d'Information

SSIC : Sécurité des Systèmes d'Information et de Communication

10.4 Chaîne de valeur avec acteurs SCS MAJ*

Ci-dessous est représentée **la chaîne de valeur de la sécurité avec les acteurs SCS** positionnés afin d'identifier les forces de l'écosystème.



Chaîne de valeur de la Sécurité Numérique (acteurs SCS)

0 **Recherche Académique et industrielle :** MINES ST ETIENNE / EURECOM / CEA TECH / YNCREA *(ISEN)* / IM2NP / CENTRALE MARSEILLE

1 **IP & semi-conducteurs :** IDEMIA / INVIA / STMICROELECTRONICS / TEXTPLAINED / PRESTO / NEOTION

2 **Editeurs Logiciels embarqués :** TRUSTED OBJECTS / PROVE&RUN / DOCAPOSTE / IDEMIA / SMARDTV

3 **Fournisseurs d'infrastructures / de services spécialisés Cloud :** ORANGE / HPE / MailnBlack / Docaposte / SmarDTV / GEMALTO *(THALÈS COMPANY)*

4 **Fabricants d'objets communicants / de systèmes électroniques et de terminaux :** NEOWAVE / SPS / PARAGON ID

5 **Editeurs de logiciels de sécurité :** TRUSTED OBJECTS / IDEMIA / GEMALTO *(THALÈS COMPANY)* / EGERIE SOFTWARE

6 **Intégrateurs, Sociétés de Services et Opérateur de services de sécurité :** ORANGE / GEMALTO *(THALÈS COMPANY)*

7 **Organismes de standardisation et de certification :** KEOLABS

10.5 Laboratoires de recherche Sécurité numérique

On peut citer en Région SUD Provence-Alpes-Côte d'Azur entre autres :

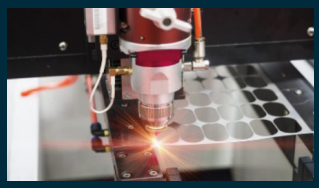
10.6 Exemples de projets collaboratifs SCS liés à la Sécurité numérique

Ci-dessous sont listés quelques exemples de projets collaboratifs innovants labellisés par SCS et issus des actions SCS autour de l'innovation.

CSAFE+

Le projet **CSAFE+** a pour objectif le développement de solutions dédiées à la protection des objets connectés et de leurs réseaux face aux attaques par injection de fautes électromagnétiques de demain. Ces solutions consistent en des bancs d'essais (plates-formes) produisant des injections électromagnétiques; des outils logiciels permettant de simuler les modes de défaillance ;
des contre-mesures logicielles et matérielles garantissant la sécurité des objets connectés.

PILAS



L'objectif du projet **PILAS** est de développer un système et une méthodologie d'injection de fautes multipoints avancés utilisant de 3 à 4 faisceaux laser ; et de proposer des implémentations logicielles et matérielles, avec contre-mesures spécifiques, qui permettront aux développeurs de produits embarqués de les sécuriser contre des attaques par injection de fautes selon différents niveaux et scénarios d'attaque.

PANDORE

Des conséquences sociétales, sociales et économiques désastreuses pourraient apparaître si les données confidentielles stockées dans les systèmes sécurisés devenaient facilement accessibles par des personnes mal attentionnées. Le niveau de résistance actuel de ces derniers n'étant pas suffisant, les concepteurs doivent très rapidement proposer et valider des protections efficaces et dont le coût devra être compatible avec les produits visés.

PACLIDO

Le projet **PACLIDO** a pour objectif de sécuriser l'Internet Des Objets par l'intégration dans des objets connectés d'algorithmes et de protocoles cryptographiques légers garantissant la confidentialité, l'intégrité et l'authentification des données échangées. Ces innovations apporteront des garanties de sécurité et de performance très attendues par les acteurs du domaine.

LCHIP

Le projet **LCHIP** vise à faciliter grandement le développement d'applications sûres à haut niveau de criticité en fournissant un environnement de développement complet permettant de générer et prouver mathématiquement et automatiquement du logiciel à algorithmie bornée, une plateforme sécurisée et à bas coût pour l'exécution de ces applicatifs, afin de garantir un niveau de sûreté maximal.

TEEVA

Les menaces qui pèsent sur la sécurité des téléphones mobiles et des services utilisant les données personnelles sont maintenant légions. Le projet **TEEVA** se propose d'évaluer et de sélectionner la meilleure technologie de sécurité permettant de prendre en compte ces nouvelles contraintes. Afin de s'assurer du niveau de sécurité de ces technologies, les attaques qui seront pratiquées tiendront compte des attaques actuelles sur smart phones mais incluront également des attaques dites « avancées ».

NOS FINANCEURS

Business Pôle - 1047 route des Dolines,
Allée Pierre Ziller, Bâtiment B, Entrée B, 1er étage
06560 Valbonne – Sophia Antipolis

Place Paul Borde
13790 Rousset

contact@pole-scs.org
www.pole-scs.org