Industries de sécurité

ANTICIPER LES RUPTURES TECHNOLOGIQUES

Cofis
Comité de la filière industrielle de sécurité

SOMMAIRE

EDITORIAL

En France, les acteurs de la filière des industries de sécurité sont parmi les plus innovants. Les laboratoires de recherche publics, les industriels de premier plan, les start-up et les opérateurs impliqués dans la sécurité, ont toujours été à la pointe des technologies et ont su anticiper les ruptures. Ainsi s'est construite une industrie qui pèse au plan national et européen, une filière qui est une des plus performantes à l'export sur un marché globalisé.

Le moment présent est cependant tout à fait particulier : nous sommes au début d'un changement d'ère technologique, industrielle et sociétale. L'avènement du numérique a un impact majeur sur les métiers de la sécurité et changera leur nature à long terme.

Pour le comité de la filière des industries de sécurité, qui regroupe toutes les parties prenantes, il est essentiel d'initier une réflexion de fond afin de faire collectivement les choix les plus pertinents, qui nous engagent pour les dix prochaines années.

Ce qui est en jeu : la sécurité de nos concitoyens, leur compréhension et leur acceptation des solutions mises en œuvre, la souveraineté nationale et la compétitivité de notre industrie.

Ces ruptures technologiques sont porteuses d'opportunités pour les missions de sécurité. Face à des menaces accrues par le recours à des solutions avancées, l'innovation et les ruptures associées sont nécessaires pour garantir la protection des institutions, des entreprises et des citoyens contre le terrorisme, les cyberattaques et toutes les formes de malveillance. La sécurité a déjà su s'impliquer précocement dans l'exploitation des avancées scientifiques (mobilité, identité, transmissions pour ne citer que quelques exemples). Le comité de la filière des industries de sécurité s'attachera à renforcer cette démarche pour accompagner l'évolution en cours des usages et améliorer les outils de la sécurité avec un triple objectif d'efficience, de proximité et de transparence vis-à-vis des citoyens.

A ces grandes opportunités s'ajoutent de grands risques. Dans un monde de plus en plus numérique, il est impératif d'anticiper les failles de cyber sécurité, de maîtriser et d'assurer la confiance dans les algorithmes, de planifier la résilience de la Nation tout entière en cas de défaillance.

Le travail collectif déjà engagé par la filière française des industries de sécurité est susceptible d'intégrer de nouvelles technologies disruptives. Les techniques d'intelligence artificielle mais aussi les matériels et composants micro-électroniques qui embarquent ces nouveaux logiciels, constituent le socle de nouveaux systèmes et du « security and ethic by design ». Cette démarche peut déboucher sur des solutions combinant efficacité et transparence, avec pour double avantage de répondre à la demande sociale et de valoriser à l'export la « marque France ». Inversement, la perte éventuelle de la maîtrise de ces technologies entamerait notre souveraineté nationale.

Les atouts de l'industrie française de sécurité pour faire face à cette révolution sont indéniables : l'excellence de notre recherche sur les domaines clefs de l'économie numérique, de grands groupes de renommé mondiale et de nombreuses PME. Néanmoins, la concurrence sera acharnée. L'économie de service, s'appuyant sur des technologies comme le big data, les objets connectés ou la blockchain, imposera des standards mondiaux, potentiellement hégémoniques et parfois antagonistes de nos normes de sécurité. Dans cette compétition mondialisée, pour nombre de sujets, il faudra choisir de bâtir une stratégie européenne.

Le CoFIS, depuis sa mise en place par le Premier ministre en 2013, est le lieu d'échanges et d'élaboration de stratégies communes entre le public et le privé, l'offre et la demande.

En 2017, il a défini sa politique industrielle autour d'objectifs majeurs pour la filière, à horizon 2025 : la création de 75000 emplois directs et le doublement de son chiffre d'affaire. Pour cela il s'appuie sur des ambitions à l'échelle mondiale, dans les domaines des Safe cities et de la cybersécurité de l'internet des objets, à l'échelle européenne, pour le développement d'une politique industrielle et d'une autonomie stratégique, à l'échelle nationale, pour le développement de la «marque» France et de start-up dans le secteur de la sécurité. L'observatoire de la filière des industries de la sécurité, mis en œuvre sur financement public et privé, permet de doter les acteurs d'une vision claire et partagée du marché, de nos forces et faiblesses mais aussi d'indicateurs clefs qui permettront en continu de mesurer les progrès accomplis. Une première liste de technologies à caractère souverain a été identifiée. Elle permettra d'établir des plans d'actions ciblés, à destination des entreprises et laboratoires concernées.

Cet opus, « anticiper les ruptures technologiques », est partie intégrante de notre feuille de route en 2018. Bâtir une stratégie de recherche et d'innovation à horizon 2025, à la hauteur des enjeux de sécurité nationale et de compétitivité de notre industrie, sera la prochaine étape. ///

Claire Landais
Secrétaire générale de la défense et de la sécurité nationale

Marc Darmon
Président du Conseil des industries de la confiance et de la sécurité

Thomas Courbe
Directeur général des entreprises

UNE POLITIQUE VOLONTARISTE ET AMBITIEUSE

Les ruptures technologiques induites principalement par l'avènement du numérique bouleversent le domaine de la sécurité comme tous les autres secteurs et domaines d'activité. Le numérique a un impact fort à la fois sur les usages qu'il crée, suscite ou rend obsolètes, et sur l'économie qu'il bouleverse en favorisant l'émergence rapide de nouveaux acteurs, en déplaçant les foyers de création de valeur et en révolutionnant les modèles économiques en vigueur.

La filière industrielle de sécurité a cependant ses spécificités. A ces impacts qui ne doivent pas être négligés, s'ajoutent les risques de disruption de la chaîne de valeur, de perte de maîtrise de certaines technologies ou de rachat incontrôlé par des entreprises étrangères de sociétés fortement impliquées dans la politique de sécurité nationale. Ces risques menacent directement notre souveraineté nationale. Imagine-t-on les forces de sécurité recourir à des plates-formes de services numériques qu'elles ne maîtriseraient pas pour gérer des véhicules autonomes ou des essaims de drones ou de robots ? Accepterions-nous de dépendre de fournisseurs non européens pour le développement de composants électroniques de confiance ? De même, pourrions-nous nous fier à des solutions d'intelligence artificielle ou d'analyse de données, que nous n'aurions pas développées, pour de l'entraînement par réalité virtuelle ou de l'aide à la décision lors de la gestion de crises majeures ?

Non, bien sûr ! Il s'agit avant tout de protéger les entreprises, les citoyens et la Nation, tant à titre individuel que collectif, mais aussi de soutenir le développement économique et stratégique de la filière, dont le secteur marchand emploie aujourd'hui 309 000 personnes. A l'heure où des entreprises géantes, principalement américaines et asiatiques, affichent leurs ambitions sur de nombreux domaines (santé, voiture connectée, énergie…), il est vital pour la filière industrielle de sécurité française de valoriser ses compétences et ses capacités afin de préserver sa souveraineté, sa position sur des marchés ainsi que la maîtrise des technologies stratégiques pour son développement. D'autant plus que la France dispose des ingrédients nécessaires à assurer sa compétitivité face à la concurrence : grands groupes leaders mondiaux, tissu dense de PME et d'ETI dynamiques, centres de recherche académiques et industriels à la pointe, moyens financiers publics et privés.

Fédérer les efforts

C'est pourquoi le CoFIS (Comité de la filière des industries de sécurité) a entrepris d'identifier les principales technologies et les scénarios de rupture pouvant bouleverser plusieurs domaines majeurs de la sécurité à l'horizon 2025. Cette analyse est essentielle pour la définition des grands axes stratégiques de la politique industrielle française. Elle contribue à élaborer et à hiérarchiser les plans d'actions qui permettront à la filière française des industries de sécurité de se développer et de jouer pleinement son rôle. Il s'agit de préparer l'avenir de la filière – et pas seulement à court terme –, de donner à tous les acteurs les moyens d'anticiper les évolutions technologiques et de mettre en œuvre des stratégies efficaces pour qu'ils se positionnent en tête des marchés et de la compétition internationale. ///

La filière des industries de sécurité en France, c'est :

309 000 emplois dans 11 000 entreprises dont 3000 réalisent plus de 2 M€ de chiffre d'affaires
1000 entreprises industrielles et 3500 entreprises de services de plus d'un salarié

Une double vocation

Créé en octobre 2013, le CoFIS définit la politique industrielle de sécurité dont le but est de protéger les entreprises, les citoyens et la Nation, mais aussi d'assurer la protection et le développement économique du secteur. Le CoFIS met en œuvre les moyens nécessaires pour que la France conserve son rang au meilleur niveau de la compétition mondiale en matière de sécurité et se positionne en leader de cette compétition sur les marchés émergents.
La filière couvre de nombreux domaines qui vont de la lutte contre le terrorisme ou la grande criminalité à la cybersécurité en passant par la protection des infrastructures d'importance vitale, la sécurité civile, la gestion des crises et la résilience de la Nation. En France, les industries de sécurité réalisent un chiffre d'affaires cumulé de 37 milliards d'euros en 2016. Leurs perspectives de croissance sont de 5 % en moyenne par an.

A L'HORIZON 2025…

L'avènement du numérique est synonyme de ruptures – parfois violentes – dans tous les domaines. Il redistribue les rôles et impose aux entreprises de se repenser, de se repositionner pour répondre aux attentes nouvelles, d'innover tant dans les produits et services proposés que dans les modes de production ou les canaux de distribution.
Surtout, les innovations en général et le numérique en particulier suscitent l'apparition de nouveaux usages, adoptés et déployés rapidement. Pour preuve, les applications collaboratives comme le covoiturage ou la location d'appartements entre particuliers, ou encore les crypto-monnaies ont conquis de larges audiences en très peu de temps. Il arrive aussi que le numérique fasse migrer des usages, qui existaient dans les domaines industriels et professionnels, vers le grand public, qui s'en empare rapidement et parfois les détourne pour en user plus facilement. Les drones dits « de loisir » ou les caméras de surveillance connectées illustrent cette appropriation par le grand public.

Menaces multiples

Les menaces ne sont plus seulement physiques ou matérielles ; les cyberattaques se multiplient, elles sont de plus en plus difficiles à détecter, à évaluer et parfois à contrer, et elles causent d'importants dégâts. La digitalisation des activités, qu'elles soient économiques, industrielles, culturelles ou sociales, les rend plus vulnérables aux attaques toujours plus massives et sophistiquées. Plus particulièrement, la connectivité de tous les objets, partout et tout le temps, dans les domaines professionnels ou privés, est certes fonctionnelle, mais elle est aussi potentiellement intrusive voire illicite et porteuse de menaces à très grande échelle.
Autres grandes tendances à l'horizon 2025, la mobilité et le nomadisme ne cessent de croître. Là encore, les technologies sous-jacentes apportent de précieuses fonctionnalités au domaine de la sécurité. L'avènement de la 5G va améliorer les débits, les temps d'accès et la fiabilité et permettra l'intégration massive des objets connectés aux réseaux de communication. Entre autres applications, citons la géolocalisation 4D « sans couture » en intérieur comme en extérieur ou la récupération d'images en temps réel en provenance des téléphones mobiles des forces de sécurité sur le terrain. Mais qui dit nouveaux modèles d'usages dit nouvelles menaces. La mobilité ou le nomadisme sans une sécurité adaptée et contextualisée sont synonymes de cible de choix pour le piratage, l'intrusion et les attaques.

Souveraineté nationale

Quels que soient les applications, les domaines ou les infrastructures, deux familles de technologies sont et seront omniprésentes. Il s'agit, d'une part, des outils de l'intelligence artificielle (IA) tels que le Machine Learning (ML) et le Deep Learning (DL) pour les principaux ; et, d'autre part, du big data, 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.

Enfin, un domaine doit retenir toute l'attention des acteurs de la filière, celui des plates-formes ouvertes et de services. Qu'il s'agisse de délivrer une identité numérique forte et d'en attester, de fournir une aide à la conduite en situation d'urgence, de donner accès à du logiciel libre souverain ou de mettre à disposition des jeux de données massifs pour le Machine Learning, l'enjeu de la souveraineté nationale est ici critique. Les GAFAM* et les BATX* imposent leurs plates-formes par la puissance des services offerts, la simplicité d'usage et la gratuité apparente. Il est urgent pour les industries de sécurité françaises et européennes de faire valoir leur expertise en la matière et de s'affranchir des plates-formes étrangères ou de coopérer avec elles dans un cadre réglementé.

Conséquences de toutes ces évolutions, les nouvelles pratiques permises par les innovations conduisent à repenser aussi la réglementation afin qu'elle s'applique aux nouveaux contextes. Définir des règles de circulation aérienne pour les drones de loisir, réglementer l'usage des robots ou des véhicules autonomes, ou encore inciter à intégrer la sécurité et la protection des données dès le stade de la conception des objets connectés sont quelques-uns des sujets qui doivent être abordés et réglementés au niveau national et en accord avec l'Europe. Cela est d'autant plus critique lorsqu'il s'agit des données à caractère personnel. L'actualité nous fournit chaque jour des exemples d'utilisation abusive ou de vol de données. Le Règlement Général sur la Protection des Données (RGPD), entré en vigueur en mai 2018, constitue un bon exemple d'adaptation de la réglementation. Les industriels français participent à de nombreux groupes de travail et de comités de standardisation. Il est essentiel que ce travail réglementaire soit intensifié en harmonie avec les pouvoirs publics tant à l'échelle nationale qu'à l'échelle européenne. ///

* GAFAM : Google, Apple, Facebook, Amazon et Microsoft ; BATX : Baidu, Alibaba, Tencent et Xiaomi

DOUZE DOMAINES DE RUPTURE

Le CoFIS a identifié douze domaines technologiques essentiels pour la sécurité nationale et l'avenir de la filière industrielle. Ces domaines impactent tout à la fois les métiers et l'économie de la filière et selon toute vraisemblance feront l'objet de scénarios de rupture à l'horizon 2025. Deux domaines technologiques, l'Intelligence artificielle (IA) et le Hardware de confiance, sont qualifiés de « génériques ». Ils sont considérés ici comme des facteurs de changement transversaux qui irriguent l'ensemble des douze domaines technologiques.

Véritables « game changers », les ruptures liées aux technologies sont autant d'opportunités pour développer de nouveaux produits, services et marchés. A condition d'en connaître les enjeux, d'en maîtriser les tenants et les aboutissants. Il ne s'agit pas de proposer une liste exhaustive des domaines et des métiers affectés, mais plutôt d'illustrer par des exemples choisis l'impact de la rupture sur les douze domaines identifiés par le CoFIS, sur les business modèles et sur les marchés actuels des entreprises de la filière.

Pour chacun des domaines identifiés, le CoFIS a analysé les scénarios disruptifs imaginables et les verrous technologiques ainsi que les forces, faiblesses, menaces et opportunités propres à chacun d'entre eux. Ces domaines ont été étudiés en fonction de leurs enjeux financiers, de leurs apports à la sécurité nationale, de leur capacité à créer de la valeur pour les acteurs économiques et à leur donner un avantage compétitif sur leurs concurrents étrangers. Pour chaque domaine, seront précisés les applications et les usages disponibles en 2018 et ceux attendus pour 2025. ///

Définition : technologie critique et technologie de rupture

Une technologie est dite **"critique"** lorsqu'elle est essentielle et sensible pour la mise en œuvre de missions de sécurité et que pèsent sur elle des risques de maîtrise en raison d'un nombre restreint de fournisseurs, d'une rentabilité insuffisante, d'une perte de savoir-faire ou de contrôle capitalistique, d'une absence de technologies alternatives...

Exemple : les sondes d'analyse en cybersécurité.

Une technologie est dite **"de rupture"** lorsqu'elle est susceptible de transformer radicalement des pans entiers d'activité de la filière de sécurité et qu'elle aura un fort impact sur le marché à l'horizon 2025.

Exemples : la blockchain ou l'identification/authentification.

Dans un exercice conduit en parallèle, le CoFIS a recensé les technologies critiques et les entreprises, particulièrement les PME, qui participent à la chaîne de valeur des technologies identifiées. Cet exercice, qui porte sur les technologies actuelles, sera amené à être actualisé, notamment en fonction des technologies de rupture identifiées dans ce travail prospectif.

Les douze domaines de rupture identifiés par le CoFIS :

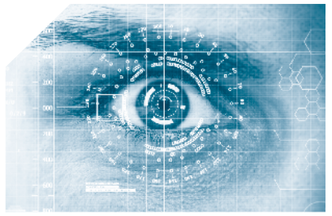
1 / Internet des objets et objets connectés

2 / Big data

3 / Analytique

4 / Conjuguer mondes réels et virtuels

5 / Identification, authentification



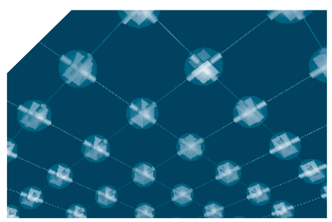
6 / Plates-formes intégrées véhicules/services

7 / Détecter les produits dangereux, illicites ou contrefaits

8 / Intervenant augmenté

9 / Observation locale

10 / Blockchain



11 / Ubérisation et post-ubérisation de la sécurité

12 / Plates-formes ouvertes pour la sécurité

NB : Les technologies d'**intelligence artificielle** et des **composants de confiance** sont stratégiques pour la souveraineté nationale, transverses aux domaines ci-dessus et potentiellement critiques.

QUELS SCÉNARIOS POUR 2025 ?

Afin de hiérarchiser et de structurer les plans d'actions qui permettront le développement de la filière, le CoFIS a positionné les domaines technologiques en s'inspirant des « scénarios de l'économie numérique en 2025 », tels que présentés dans le DigiWorld Yearbook 2017 de l'IDATE*. Celui-ci présente 4 scénarios types associés à des écosystèmes, qui préfigurent les nouvelles chaînes de valeur et les business modèles de l'économie numérique à l'horizon 2025. L'IDATE a positionné ces scénarios en croisant deux critères : l'ouverture des technologies et des données, qui permet à des acteurs d'exploiter des technologies sans avoir à investir eux-mêmes dans leur développement ; et l'intensité de l'usage des données personnelles fait par les acteurs. Ce dernier critère est tributaire à la fois du niveau de confiance des utilisateurs et de la réglementation en vigueur, deux paramètres qui pourraient évoluer d'ici à 2025 de façon relativement imprévisible. En témoignent les fréquents cas d'utilisation abusive des données personnelles par de grandes entreprises…

Dans une lecture croisant souveraineté économique et protection des données, le CoFIS a positionné les douze domaines de rupture identifiés sur les scénarios de l'IDATE. Le résultat est une cartographie cible réaliste du positionnement de la filière de sécurité nationale à l'horizon 2025. Cette analyse s'appuie principalement sur l'analyse FFOM des acteurs de la filière et sur les éléments clefs de la stratégie nationale en matière de sécurité. Ces scénarios sont représentatifs du comportement des acteurs et du schéma global de compétition propre aux grands domaines de l'économie sans être strictement exclusifs, certains acteurs correspondant à plusieurs scénarios en fonction de leur positionnement marché/géographie.

* IDATE Digiworld est un institut de recherche européen spécialisé sur les marchés télécoms, Internet, médias et territoires numériques

• Le scénario « Tech » alias « Lego-like », est celui de l'économie des start-up : collaborative, dynamique et décentralisée. De nombreux acteurs orientés sur l'innovation technologique proposent des solutions ouvertes et interopérables, générant ou s'appuyant sur des standards. Ils se rémunèrent principalement par d'énormes volumes de micro-paiements (en transaction ou publicité) et proposent des services ultra-ciblés grâce à un échange massif de données des utilisateurs.

Acteurs emblématiques de ce scénario : le Bitcoin, et plus généralement les start-up de la « Fintech »

Mot-clé : disruption

En matière de souveraineté économique et de protection des données, ce scénario positionne la filière de sécurité nationale en 2025 sur les domaines technologiques : plates-formes ouvertes, interface entre mondes réels et virtuels, intervenant augmenté, détection de personnes ou de produits, Blockchain, objets connectés, analytique pour la sécurité.

• Le scénario « Club » est celui du service Premium, basé sur le modèle de l'abonnement « tout inclus ». Il est dominé par les grands acteurs du numérique, qui internalisent les développements technologiques (souvent très avancés) et les infrastructures afin d'accélérer la mise sur le marché. Des plates-formes multi-services hégémoniques leur permettent d'exploiter les données utilisateurs pour développer de nouveaux services. Les utilisateurs bénéficient d'une expérience client très avancée et de bout en bout.

Acteurs emblématiques de ce scénario : Amazon, Google, BATX

Mot-clé : colonisation

En matière de souveraineté économique et de protection des données, ce scénario positionne la filière de sécurité nationale uniquement sur un domaine technologique : identification / authentification, seul des douze domaines de sécurité où la filière paraît en position d'occuper un rôle de leader mondial.

• Le scénario « Low cost » est celui du « moins disant économique » et de la massification. Il est basé sur une relation client ou utilisateur entièrement numérisée (self-service plutôt que magasin) et sur une infrastructure numérique qui fait la part belle à la virtualisation. Les acteurs se spécialisent pour optimiser les coûts, réaliser des économies d'échelle et atteindre la rentabilité grâce à un grand nombre d'utilisateurs. C'est le scénario de la rupture économique basée sur la désintermédiation, la mutualisation et l'automatisation.

Acteurs emblématiques de ce scénario : Uber, Netflix

Mot-clé : viralité

En matière de souveraineté économique et de protection des données, ce scénario positionne la filière de sécurité nationale sur les domaines technologiques : ubérisation et post-ubérisation, observation locale, plates-formes ouvertes pour la sécurité, objets connectés (grand public).

Le scénario « Shield » mise sur la confiance et la sécurité. Il s'agit essentiellement de matériels (composants, appareils, infrastructures). C'est le scénario des grands acteurs qui maîtrisent une bulle à la fois physique et numérique, et fermée. Ils investissent lourdement dans des infrastructures sécurisées. Les utilisateurs leur font confiance pour les protéger et sont prêts à payer pour cela.

Acteurs emblématiques de ce scénario : Apple, grands acteurs de l'énergie et des télécoms

Mot-clé : protection

En matière de souveraineté économique et de protection des données, ce scénario positionne la filière de sécurité nationale en 2025 sur les domaines technologiques : plates-formes, observation locale, objets connectés (industriels).

Souveraineté économique et protection des données : position nationale par rapport aux ruptures.

Source : DigiWorld Yearbook de l'IDATE

Les propositions d'action et de positionnement national faites par le CoFIS privilégient ainsi les scénarios « Tech » et « Shield » à horizon 2025. Pour deux raisons essentielles. D'une part, les domaines technologiques concernés par ces scénarios présentent de forts enjeux en matière de souveraineté économique et de protection des données. Par exemple, il n'est pas envisageable de déléguer la gestion des réseaux d'eau ou du trafic des villes à des plates-formes qui ne seraient pas localisées sur le territoire national. D'autre part, plutôt que de se battre sur tous les fronts, il s'agit d'exploiter au mieux les forces du tissu industriel français. Notre pays compte de nombreuses PME actives dans les différents domaines de la sécurité. L'excellence de nos ingénieurs et de nos centres de recherche n'est plus à prouver. Différents types d'infrastructures comme les pôles de compétitivité et les instituts de recherche technologique favorisent la collaboration entre les acteurs. En revanche, la France – et même l'Europe – ne compte pas (encore !) de champion numérique capable de rivaliser avec les GAFAM ou les BATX. Il convient donc de définir une politique industrielle et des plans d'action tenant compte de ces forces et faiblesses pour en maximiser les chances de réussite.

Pour le CoFIS, la filière industrielle de sécurité française ne peut d'emblée ambitionner atteindre une position de leader global (scénario « Club ») que dans le domaine de l'identification / authentification, dans lequel plusieurs entreprises ont d'ores et déjà atteint une dimension internationale reconnue.

Il ne faut pas pour autant écarter le scénario « low-cost » pour certains domaines technologiques. En effet, pour de nombreux usages et applications, les utilisateurs privilégieront l'accès gratuit à des plates-formes tout en sachant que leurs données seront exploitées. De même, les logiciels et matériels en « open Source » offrent d'importants avantages dans de nombreux domaines sans nuire à la souveraineté économique ou technologique du pays. ///

ANALYSES CROISÉES DES ENJEUX

En complément de l'analyse de **souveraineté économique et de protection des données** présentée plus haut, le CoFIS a également croisé les différents domaines par rapport aux enjeux de souveraineté, d'acceptation sociétale, d'efficacité industrielle et de retour sur investissement. Cela a permis d'identifier les domaines de rupture présentant les enjeux les plus importants à la fois pour la sécurité nationale, pour l'Etat et pour les acteurs économiques. A cet effet, le CoFIS a procédé à une analyse méthodologique formelle et structurée des douze domaines technologiques de manière à fournir une liste des critères les plus différenciants pour chacun de ces domaines.

Réalisée en positionnant chaque domaine de manière relative à son importance vis-à-vis d'une douzaine de facteurs socio-économiques (position de l'industrie nationale, marchés adressables, importance pour la protection des infrastructures vitales, impact sur la gestion de crise, risque cyber, enjeux économiques pour l'Etat, investissements nécessaires…), cette étude a fait émerger cinq critères particulièrement différenciants :

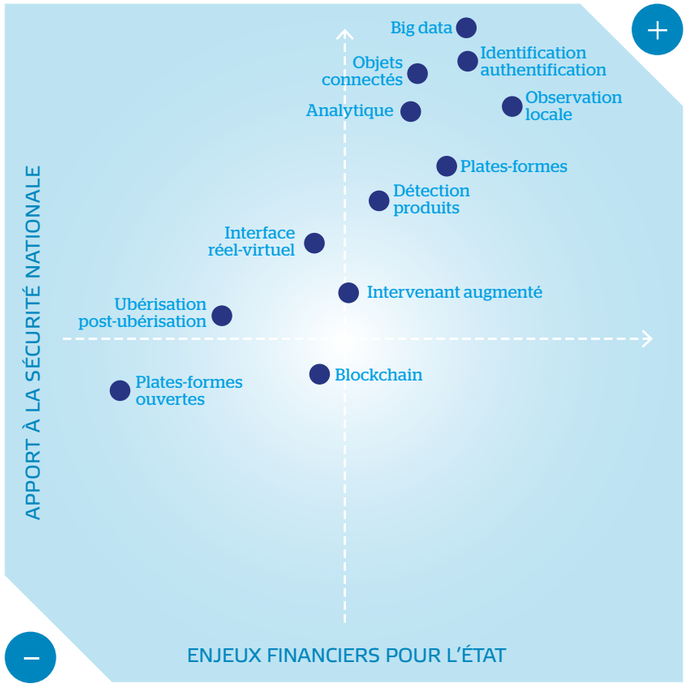
- Apport à la sécurité nationale (ajout de nouvelles capacités)
- Contribution à l'efficience de la sécurité nationale (évolution des coûts, organisation, processus)
- Création de valeur pour les acteurs économiques, notamment à l'export
- Acceptation et appropriation sociétales
- Enjeux financiers pour l'Etat

Ces critères ont été croisés de manière à fournir des matrices de lecture permettant de visualiser aisément le positionnement des différents domaines de rupture vis-à-vis des critères de différentiation.

Trois « croisements » de ces critères sont particulièrement porteurs d'information pour l'ensemble de la filière et sont présentés ci-dessous. **Les domaines qui portent les enjeux les plus importants sont dans le carré supérieur droit pour « Retour sur investissement » et « Efficacité de la filière » et dans le carré supérieur gauche pour « Acceptation sociétale ».** ///

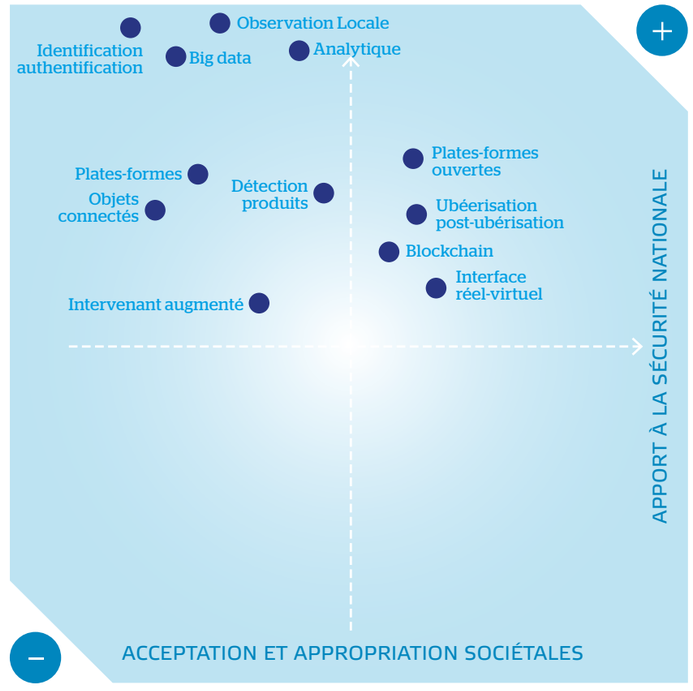
RETOUR SUR INVESTISSEMENT

Le croisement des critères « Contribution à l'efficience de la sécurité nationale » et « Enjeux financiers pour l'Etat » montre l'importance des investissements à réaliser dans les différents domaines pour optimiser l'efficacité de la sécurité nationale. La nécessité de disposer d'une infrastructure big data couplée à des techniques de traitement analytique avancées et à une maîtrise des technologies d'objets connectés et d'identification/authentification apparaît ainsi comme fondamentale pour l'efficacité de la sécurité nationale mais aussi comme la plus demandeuse en matière d'investissements de l'Etat (infrastructure, formation, changement des processus et des organisations). Ce premier type d'investissement peut être considéré comme une réponse à la menace croissante du risque cyber en particulier dans la perspective du développement des objets connectés. De même le domaine de l'observation locale (capteurs, dispositifs de vidéo-protection) est porteur d'efficacité pour la sécurité nationale (protection des infrastructures critiques, de grands événements, gestion de crise) mais reste un domaine fortement consommateur de ressources financières. A l'inverse, plates-formes ouvertes, blockchain, ubérisation et post-ubérisation sont peu consommateurs de ressources, mais ne sont pas supposés avoir une influence déterminante sur la sécurité nationale à horizon 2025, sauf sur quelques « niches » spécialisées.



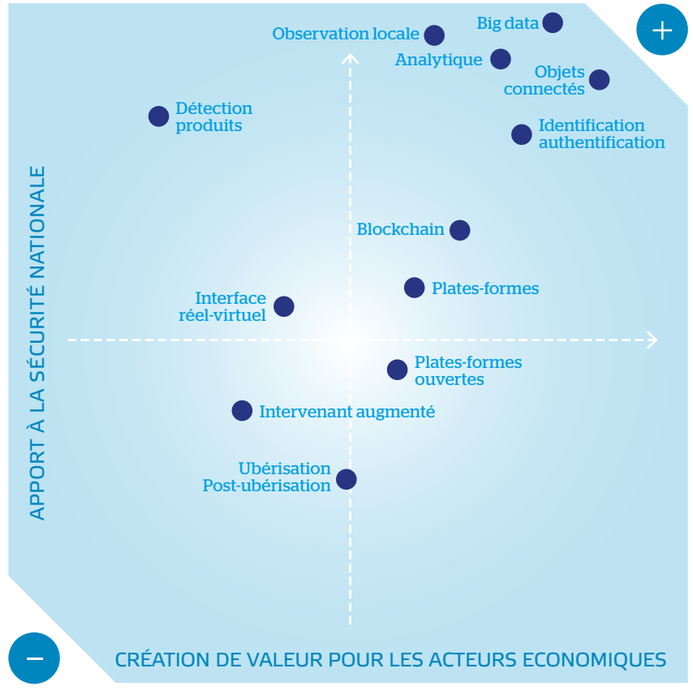
ACCEPTATION SOCIÉTALE

Le croisement des critères « Acceptation et appropriation sociétales » et « Contribution à l'efficience de la sécurité nationale » donne une grille de lecture pratiquement opposée à la précédente. Il met en évidence l'acceptation relativement aisée par les utilisateurs ou les citoyens des ruptures issues du domaine grand public (plates-formes ouvertes, ubérisation, blockchain). Les technologies de réalité augmentée ou virtuelle sont également bien acceptées ou faciles d'appropriation (filiation évidente avec le monde du jeu vidéo). A l'inverse, les domaines identification/authentification, observation locale, big data, générateurs de plus forts apports à la sécurité nationale, suscitent plus de réticence en termes d'acceptation ou d'appropriation. A noter aussi sur ce croisement, la mauvaise perception des plates-formes (véhicules connectés, robots, drones), probablement à cause des inquiétudes sur l'emploi ou sur la nature des emplois que ce domaine suscite, ainsi que le positionnement relativement neutre des techniques d'analytique, dû sans doute à une perception de l'intelligence artificielle plus grand public que celle du big data.



EFFICACITÉ DE LA FILIÈRE

Le croisement des critères « Création de valeur pour les acteurs économiques » et « Apport à la sécurité nationale » confirme le fort potentiel du marché, y compris à l'export, des domaines big data et analytique, observation locale, identification/authentification et objets connectés. C'est dans ces domaines que le potentiel de l'industrie de sécurité nationale est le plus générateur de valeur ajoutée, notamment par rapport aux objectifs de politique industrielle du CoFIS (CA à horizon 2025 et leadership national dans les domaines de la Safe-City et de l'Internet des objets industriel).
Un tissu dynamique d'intégrateurs, de PME et de structures de recherche laisse envisager de bonnes perspectives de chiffre d'affaires dans le domaine des plates-formes (drones et robots), de la blockchain (tirée par quelques secteurs comme la finance ou l'énergie) ou encore celui des plates-formes ouvertes (dans une perspective de marché sans doute plus régionale). A l'inverse, la filière nationale semble mal armée pour développer des services de sécurité en mode SaaS, ce qui soulève quelques inquiétudes quant au poids sans cesse croissant des grandes plates-formes de services américaines ou chinoises. De même, la filière de sécurité semble devoir se cantonner à un rôle « d'intégrateur » purement national pour les domaines de la réalité augmentée/virtuelle ou des solutions pour primo-intervenants.



INDICATIONS POUR LA FILIÈRE

Anticiper et préparer les situations de rupture permettra à la filière de définir des priorités et de faire les choix politiques en conséquence. Les douze domaines de rupture analysés dans ce document devraient contribuer de manière essentielle aux différents axes de la politique industrielle du CoFIS et à la mise en place de la Stratégie nationale pour le Numérique présentée en 2016 par le Premier Ministre. Quelques grandes tendances se dégagent des analyses croisées présentées ci-dessus.

- Le domaine de l'identification/authentification (des personnes, des objets) est un élément clef de la souveraineté économique sur lequel il est fondamental d'investir pour protéger efficacement l'économie numérique nationale. La maîtrise des technologies associées, couplée à la mise en place du RGPD, offre une occasion majeure de « rebattre les cartes » par rapport aux positions dominantes des grands opérateurs de service. Elle donne aussi l'occasion de renforcer le leadership de l'industrie nationale et de créer un environnement qui favorise la confiance numérique, la protection de la vie privée et des données à caractère personnel, et la lutte contre la cyber-malveillance. Ce domaine pourrait constituer un élément de base d'une souveraineté numérique européenne.

- La protection des intérêts fondamentaux de la Nation, la défense et la sécurité des systèmes d'information de l'État et des infrastructures critiques, la résilience numérique des grandes villes en même temps que les ambitions économiques de la filière passent par un investissement et un soutien massif aux thèmes de l'Internet des objets industriel, des technologies de l'intelligence artificielle et du big data, de l'observation locale et du traitement vidéo en particulier. La filière nationale de sécurité est bien positionnée sur ces domaines, avec un tissu d'acteurs compétents, capables de prendre d'importantes parts de marché au niveau mondial. L'investissement et le soutien associé ne seront cependant pas que technologiques. Ils devront prendre en compte l'ensemble des processus métiers et de formation. Ils devront également prendre en compte les réticences que ces technologies peuvent générer.

- Les domaines des plates-formes (drones, robots…), de la blockchain, de la réalité augmentée ou virtuelle, de la détection de produits dangereux ne constituent pas a priori des domaines de fort leadership national, qu'il soit technologique ou de marché. Par contre, ils pourraient offrir des perspectives d'expérimentation dans le domaine de la sécurité. Si des politiques incitatives étaient envisagées, notamment vis-à-vis de start-up, elles contribueraient peut-être à renforcer l'attractivité technologique nationale.

- Le développement des plates-formes ouvertes (matériel et logiciel) prendra de plus en plus d'importance dans le domaine de la sécurité, en particulier pour le déploiement de solutions à coût optimal, par exemple dans le domaine de l'IoT grand public ou des « smart-territoires ». La France possède en la matière un solide écosystème de PME et d'acteurs académiques, insuffisamment exploité dans le domaine de la sécurité. Cet atout est pondéré par l'absence de grandes plates-formes nationales de services, capables de répondre aux besoins du domaine des services de sécurité à la demande (SecaaS) et en particulier d'assurer le passage à l'échelle des applications. ///

LES DOMAINES DE RUPTURE

Internet des objets et objets connectés

Les objets connectés, désormais plus sobres en consommation d'énergie et adaptables à tous types de situation, se banalisent dans nos environnements tant professionnels que privés. La disponibilité progressive de nouveaux facteurs de forme de la carte SIM (e-SIM, e-SE, modules de sécurité logicielle) contribue à la connectivité de nouveaux capteurs, objets et autres équipements. La standardisation des protocoles de communication, longue portée (Sigfox, LoRa, cellulaires) ou courte portée (Wi-Fi, Z-Wave, Bluetooth Low Energy), et le déploiement des réseaux 5G permettent de configurer toutes sortes d'applications : industrielle ou domotique, comportant peu de capteurs mais nécessitant une large bande passante, ou avec un très grand nombre d'objets connectés simplement émetteurs, etc. Le roaming automatique d'abonnement simplifie la création d'un réseau mobile virtuel (MVNO) ou le déploiement de nouveaux services (MVNE) à la volée. Ces services–jusque là plutôt réservés au domaine industriel (M2M) gagnent à présent le grand public (B2C) et trouvent de nombreuses applications dans le monde de la sécurité, publique ou privée.

La conjugaison de ces avancées ouvre le champ à de nouvelles applications et à de nouveaux usages. Entre autres nouvelles capacités, l'IoT permet à présent une grande réactivité voire du temps réel, atout essentiel pour les filatures vidéo, les contrôles mobiles aux douanes ou sur les routes, le monitoring temps réel et massif d'activités ou d'équipements. L'installation potentielle d'un MVNO dans un réseau 5G en quelques secondes, par exemple, simplifiera considérablement la surveillance ad hoc d'événements (concerts, rencontres sportives, rassemblements), la tenue de situation ou la sécurisation ponctuelle ou permanente d'un site, d'une infrastructure de transport ou d'énergie, par exemple.

Les infrastructures connectées supporteront des réseaux IoT massifs et assureront la continuité avec les réseaux de type industriel. Elles faciliteront également l'hypervision, c'est-à-dire la connexion de capteurs de surveillance sur des moyens de communication haut débit, multi-protocoles et quelle que soit la distance entre les capteurs et les sites de traitement des données. Ces fonctionnalités s'appliqueront aux situations d'urgence, pour la communication entre ou avec les véhicules (V2X), ou pour les contrôles mobiles, par exemple. En optimisant les déploiements des forces de secours ou d'intervention, ces capacités favoriseront le recentrage des effectifs sur les missions à forte valeur ajoutée.

Ce domaine technologique, l'un des plus prometteurs pour la filière, contribue tout à la fois à la création de valeur pour les acteurs économiques, notamment à l'export, et à l'efficience de la sécurité nationale. La France est bien placée sur ce marché, grâce aux compétences nationales en mathématiques appliquées et en traitement du signal, compétences qui ont été jusqu'ici fortement mises à profit par les GAFAM ou les BATX*. Start-up, PME et grands groupes sont positionnés sur les produits et les protocoles ainsi qu'en recherche et développement. Plusieurs acteurs sont présents à l'international, certains en position de leader mondial. Des programmes et des réseaux nationaux tels Industrie du futur ou le réseau #IoT de la French Tech contribuent au bon développement économique et technologique de ce marché.

Toutefois, il reste des verrous technologiques à lever et des menaces à écarter. Les récentes attaques de type « DDoS » (déni de service), qui utilisent des objets connectés (routeurs, caméras IP…) pour saturer des sites Internet et empêcher d'y accéder ont montré la vulnérabilité des infrastructures IoT. D'importants sites informatiques ont vu leur activité bloquée pendant plusieurs heures. Ces risques sont d'autant plus critiques lorsqu'il s'agit des équipements des forces de sécurité ou de la protection des points d'importance vitale.

500, c'est le nombre moyen d'objets connectés qui fonctionneront dans une maison en 2022
(étude Joshfire)

A l'avenir, l'approche « security and ethic by design » intègrera 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. L'adoption du « security and ethic by design » pourrait être facilitée par :

- la mise en place d'un label IoT Security mondial
- le soutien au développement de briques sécurisées par défaut, intégrables facilement dans les offres de systèmes et munies de mécanismes d'intelligence artificielle
- le développement de composants logiciels et matériels open source
- des démonstrateurs d'objets et d'applications
- le test des vulnérabilités « bug bounty »** des objets avant leur commercialisation

Le respect de la vie privée est un autre sujet critique. Les objets connectés n'inspirent pas encore totalement confiance.

Beaucoup d'utilisateurs sont soucieux de la protection de leurs données notamment en matière de santé. S'ajoutent à cela la relative faiblesse des investissements français et le manque d'acteurs nationaux de taille significative pour le déploiement des plates-formes de services. Autant de points faibles qui pourraient laisser le champ libre aux GAFAM ou BATX, dont la stratégie d'intégration verticale en matière d'IoT est clairement affichée.

Plusieurs leviers peuvent être actionnés pour améliorer la position et les performances des industries françaises dans ce domaine, à commencer par la réglementation et la standardisation. L'entrée en application en mai 2018 du Règlement européen sur la protection des données (RGPD) harmonise les pratiques dans les pays de l'Union européenne. En parallèle, il faudra développer des standards européens de certification de la sécurité de l'IoT et analyser les besoins d'évolution de la réglementation française en la matière afin de tenir compte des spécificités du domaine de l'IoT. ///

* Google, Amazon, Facebook, Apple et Microsoft ; Baidu, Alibaba, Tencent et Xiaomi

** système de récompense des chercheurs lorsqu'ils trouvent des failles de sécurité

INTERNET DES OBJETS

2018 ce que l'on fait :
- approches verticales de la sécurité, plutôt grand public, mais avec des business modèles instables
- sécurité minimale assurée de « bout en bout »
- orchestration des applications IoT par kit de développement logiciel (SDK)

2025 ce que l'on fera :
- possibilité de gérer des configurations IoT massives grâce aux technologies de « slicing », de virtualisation et de définition logicielle (NFV, SDN) disponibles sur les réseaux 5G
- orchestration intelligente grâce à l'IA avec apprentissage
- la standardisation des protocoles et la disponibilité d'architectures et de composants IoT (industriel) garantiront la sécurité de bout en bout, ce qui rendra les infrastructures résilientes aux attaques de type botnet (Mirai, Bashlite…) telles qu'elles pourraient exister en 2025
- les algorithmes d'IA avec apprentissage seront présents à quasiment tous les niveaux de l'architecture

3 questions à… Richard Kalczuga, responsable de l'offre Sécurité, Thales Communications & Security.

De la smart city à la safe city

Quel rôle joue la sécurité dans les projets de ville intelligente, de « smart city » ?

Richard Kalczuga : Une ville intelligente est avant tout une ville sûre ! Pour réussir leur transformation digitale, les villes adoptent des technologies comme l'IoT, l'intelligence artificielle ou l'analyse des données, qui leur permettent de devenir intelligentes et plus efficaces. Le bon fonctionnement et la sécurité d'une « smart city » dépendent de l'interopérabilité des systèmes qui gèrent les différents services de la ville, transports, énergie, sécurité, trafic, prévention…

Comment cette interopérabilité peut-elle être mise en œuvre ?

R. K. : C'est l'objet du projet de recherche et d'industrialisation « Safe City », animé par Thales et composé de PME, de grands groupes et d'universitaires. Il s'agit de développer une plateforme ouverte de partage et de gestion des données entre les opérateurs de services et les acteurs de sécurité d'une grande ville afin que chacun dispose du juste niveau d'information au bon moment.

Quels sont les objectifs du projet « Safe City » ?

R. K. : Le projet aborde trois thèmes : le traitement intelligent des grands volumes de données issues notamment de l'IoT, le partage de la vue de situation, et la collaboration des acteurs de la sécurité. « Safe City » vise, entre autres, la mise à disposition de nouveaux systèmes de commandement collaboratifs, l'amélioration de la communication entre les centres de supervision et les équipes de terrain, l'accélération de la résolution d'enquêtes par le recoupement d'informations, etc.

Big data, analytique et data science

Les données, nouvel « or noir », sont devenues l'un des éléments les plus stratégiques du monde numérique. Elles sont générées par nos interactions sur les réseaux sociaux et nos échanges de messages, par nos achats en ligne et par nos moyens de paiement, par les milliards d'objets connectés et d'appareils intelligents qui nous entourent, par nos smartphones, par les équipements industriels et par les moyens de transport. L'analyse et le traitement de ces données ouvrent des champs d'application particulièrement prometteurs dans tous les domaines. Des algorithmes toujours plus performants et plus intelligents, sont capables de traiter simultanément d'importants volumes de données de n'importe quelle nature, audio, vidéo, texte ou simple signal, structurées ou non, pour en extraire de l'information.

Pour les industries de sécurité, ces capacités de production et d'analyse de données sont synonymes à la fois de nouvelles fonctionnalités et applications mais aussi de nouveaux risques. Le big data, la data science, le Machine Learning (ML) et l'intelligence artificielle (IA) peuvent aussi bien servir des intentions criminelles qu'aider à s'en protéger. L'analyse de grands volumes de données hétérogènes contribue à détecter voire à prédire des situations à risques (préparatifs, attaques, fraudes, etc) et donc à les anticiper afin de les éviter. Mais ces analyses sont aussi exploitées par des organisations

dans le but de nuire comme, par exemple, l'identification des parcours empruntés par des personnalités ou des forces de sécurité grâce aux données GPS et à leur fréquence. Les fonctionnalités analytiques posent également la question du respect de la vie privée et des libertés publiques, condition sine qua non de la confiance dans ces systèmes et de leur acceptation sociétale.

Les infrastructures de recueil, de transport et de traitement des données gagnent en intelligence. Grâce aux technologies d'IA et notamment d'apprentissage, chaque niveau (capteurs, nœuds de réseaux, sites) est capable d'apprendre et de s'adapter au contexte de façon dynamique. Cette intelligence distribuée apporte de nouvelles capacités à de nombreux domaines de la sécurité. A commencer par la détection de situations à risques. L'analyse conjuguée de signaux audio, vidéo, etc, en provenance de capteurs multiples permet de reconnaître des personnes ou des objets, par exemple, une arme, de lire sur les lèvres ou de reconnaître des émotions comme la peur. Il est possible de prédire la trajectoire d'une personne ciblée, de la suivre et de reconstruire sa trajectoire a posteriori. Le « data mining » (fouille de données) de grosses bases de données et le croisement avec des données en provenance de sources différentes contribuent également aux enquêtes judiciaires et aux analyses de cybersécurité, tout comme les différentes techniques d'IA auxquelles la cybersécurité recourt de plus en plus.

210 milliards de dollars, c'est ce que pèsera le marché mondial du big data et de l'analytique en 2020. Il était de 130 milliards de dollars en 2016 et il devrait atteindre 168,7 milliards de dollars en 2018. source : IDC

Plusieurs aspects, technologiques et organisationnels, devront être réglés afin que ces applications soient pleinement opérationnelles. Les technologies de Machine Learning et de Deep Learning nécessitent des jeux de données massifs pour que les algorithmes « apprennent ». Outre qu'il est relativement long, cet apprentissage comporte un risque de « biais », particulièrement critique lorsqu'il est question de sécurité. Les premières applications de prédiction des zones à risque ou d'études des demandes de mise en liberté sur parole ont montré que les algorithmes renforçaient les biais de discrimination raciale car ils avaient «appris» sur des bases de données de géolocalisation des crimes ou des libérations sur parole du passé. De même, pour garantir leur acceptabilité sociétale, les algorithmes doivent être transparents ; la façon dont ils fonctionnent doit pouvoir être expliquée et justifiée, voire certifiée dans certains cas. L'IA doit garder un rôle de détection et de prévention ; les décisions d'exercer des contraintes doivent rester du ressort de la personne humaine. Quant aux données, pour concilier impératifs de sécurité et protection de la vie privée, leur anonymisation doit être prouvée et garantie.

L'écosystème français de sécurité est présent sur toute la chaîne de valeur du big data et de l'analytique. Reconnue pour son excellence en IA et en ML, la recherche académique a favorisé la création de start-up, d'incubateurs, d'initiatives nationales (Hub France IA) ainsi que de services dédiés dans les grandes entreprises. Toutefois, grâce à l'importance de leurs ressources, les grands acteurs du logiciel et notamment les GAFAM multiplient les acquisitions de sociétés et de talents. Le manque d'acteurs de portée internationale et de fonds d'investissement dédiés ajoute à la vulnérabilité de la filière. Une autre des faiblesses de l'écosystème français est la difficulté à constituer ou à se procurer des jeux de données suffisamment importants pour l'apprentissage par les algorithmes. La génération automatique de données pourrait pallier en partie cette difficulté. ///

BIG DATA

2018 ce que l'on fait dans le domaine du big data :

- disponibilité de machines pétaflopiques (10^{15}), d'infrastructures cloud – des GAFAM notamment, de stockage HDD ou SSD
- modèles de données hétérogènes faiblement couplés et modèles de stockage hétérogènes, déconnectés des types de données traitées
- démarrage du cloud cognitif de type Watson analytics
- mesures de véracité et extraction des données pertinentes peu élaborées
- modèles de sécurité et protection de la vie privée souvent incomplets

2025 ce que l'on fera :

- disponibilité de machines hexaflopiques (1016), de cloud cognitif, de stockage photonique et des premiers calculateurs quantiques
- multiplication des logiciels d'IA et d'intelligence cognitive pour la préparation et l'analyse des données, en self-service
- disponibilité d'énormes jeux de données d'apprentissage, chez les GAFAM et les BATX en particulier
- modèles de sécurité et protection de la vie privée multi-niveaux

ANALYTIQUE

2018 ce que l'on fait dans le domaine de l'analytique :

- algorithmes pour analytique temps réel encore à « faible bande » de type batch ou streaming
- démarrage des algorithmes interactifs
- outils de data visualisation encore limités
- modèles analytiques peu robustes en termes de leur sécurité et sûreté intrinsèques
- début de l'intégration de puces neuromorphiques dans les smartphones

2025 ce que l'on fera :

- algorithmes bio-inspirés, algorithmes d'IA « large bande » permettant découverte et apprentissage à partir de données IoT
- premières démonstrations d'analytique basées sur le calcul quantique
- outils de data visualisation élaborés, en mode self-service
- analytiques à apprentissage dual (algorithme/professionnel) et premiers algorithmes à apprentissage non supervisé
- puissantes techniques d' « Adversarial Machine Learning » et nouveaux modèles d'attaque/défense associés

Calcul quantique et composants neuromorphiques

L'amélioration des performances du traitement et de la sécurité des données dépendent en partie des progrès qui seront effectués dans deux domaines clés : l'informatique quantique et les composants neuromorphiques. Les avancées technologiques en la matière contribueront à améliorer l'analyse d'images, la reconnaissance de voix ou de visages, la conduite autonome ou le chiffrement sécurisé des informations.

Le calcul quantique repose sur des qubits, qui, contrairement aux bits classiques, peuvent prendre simultanément n'importe quel état entre « 0 » et « 1 ». Encore au stade de la recherche, la cryptographie quantique semble le champ le plus prometteur, en particulier pour chiffrer et échanger des informations de manière très fiable grâce à l'échange de clefs entre l'émetteur et le destinataire. La capacité future du calcul quantique permettrait de casser les algorithmes de chiffrement classiques, nécessitant des travaux de recherche importants en cryptographie « post-quantique », capable de résister à la puissance d'un ordinateur quantique.

Dans l'espoir d'accélérer le traitement des informations, les chercheurs explorent également la piste des **microprocesseurs neuromorphiques.** Cette architecture de composants cherche à simuler le fonctionnement du cerveau pour le traitement et le stockage des données. Au lieu de séparer les deux fonctions, il s'agit de les intégrer dans un même composant. Cette solution réduit les échanges entre le processeur et la mémoire, ce qui améliore leur rendement (réduction de la consommation et de la déperdition d'énergie). Les puces neuromorphiques, alliées aux réseaux neuronaux, seraient particulièrement adaptées aux applications de reconnaissance d'objets dans des vidéos ou de mots dans des flux audio.

Conjuguer mondes réels et virtuels

Réalité virtuelle (VR pour Virtual Reality) et réalité augmentée (AR, Augmented Reality) ont dépassé le stade de la recherche. Ces deux technologies ont commencé à sortir des laboratoires et elles trouvent des applications intéressantes qui vont de la formation au tourisme en passant par l'industrie et le jeu vidéo. Certes, elles n'en sont encore qu'au début de leur industrialisation et leur utilisation n'est pas encore tout à fait banalisée. Toutefois, les perspectives d'application de l'AR et de la VR aux domaines de la sécurité sont particulièrement prometteuses tant en termes de développements technologiques que d'apparition de nouveaux usages.

Parce qu'elle peut reproduire fidèlement le réel, la réalité virtuelle trouve d'importants débouchés dans la formation et dans la simulation. Grâce aux technologies de rendu, les situations opérationnelles peuvent être simulées très finement. En VR, il est possible de reproduire de façon réaliste un environnement dans tous ses détails sensoriels : perception du terrain, environnement sonore, vision, retour d'effort, etc. Les « serious games » et les simulateurs fournissent ainsi de nouvelles techniques d'entraînement par simulation immersive.

143,3 milliards de dollars,
c'est ce que pèsera le marché mondial de l'AR et de la VR en 2020. Estimé à 17,8 milliards de dollars en 2018, ce marché bénéficiera donc d'une croissance de plus de 700 % en 3 ans !

source : IDC, novembre 2017

RÉALITÉ VIRTUELLE / AUGMENTÉE

2018 ce que l'on fait :
- casques à réalité augmentée pour la formation intégrant de la biométrie temps réel pour la reconnaissance faciale
- utilisation de l'IA dans les formations. Entraînement collaboratif immersif liant réalité et espace simulé

2025 ce que l'on fera :
- utilisation massive de l'IA y compris pour générer des situations inattendues, éventuellement avec apprentissage non supervisé
- assistant virtuel pour le coaching des apprenants et l'aide au debriefing
- déploiement massif de la simulation à tous les stades de la formation

La réalité augmentée consiste à enrichir le réel en y apportant des informations sur tablette, smartphone ou via des lunettes. Elle peut être utilisée en formation, mais c'est surtout un outil précieux pour la connaissance et le suivi en continu de la situation et pour l'aide à la décision en temps réel ou quasi réel sur le terrain. Dans l'industrie, elle trouve des applications en production et en maintenance. Elle apporte au technicien des informations complémentaires au réel et l'aide ainsi à accomplir ses tâches sur une chaîne d'assemblage ou en contrôle qualité, par exemple.

Les applications de VR sont encore balbutiantes dans le domaine de la sécurité, mais elles promettent de se développer rapidement. Conjuguée avec les technologies de géolocalisation, des objets connectés, du big data et de l'identification, l'AR démultipliera l'information accessible. De fait, elle augmentera la réactivité et l'efficacité de tous les acteurs, qu'il s'agisse des forces et agents de sécurité, ou, demain, des citoyens qui pourront être informés et alertés rapidement.

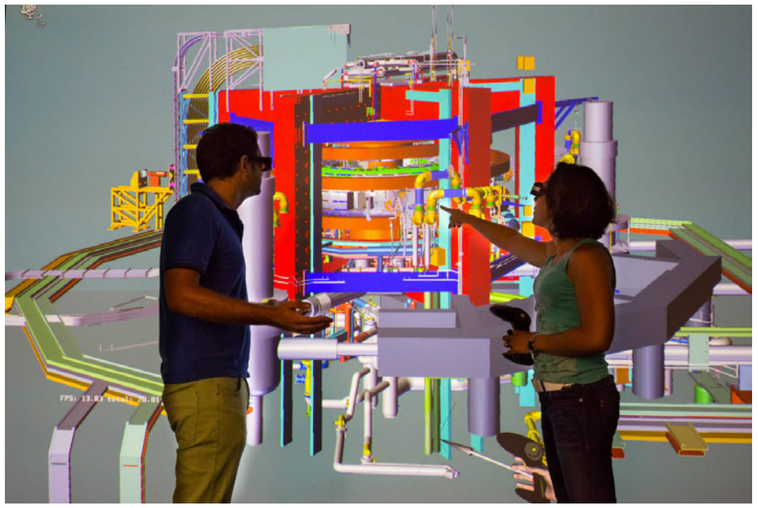
Les informations pratiques ou tactiques fournies via des lunettes connectées ou des lentilles de contact, éventuellement munies de vision thermique, peuvent aider un individu à se déplacer dans un espace qu'il ne connaît pas, lui indiquer l'itinéraire à suivre, les obstacles ou la présence d'humains. Demain, la convergence entre la micro-électronique et les nanomatériaux améliorera encore les performances humaines. A plus long terme, il est possible d'imaginer qu'un implant fournira une interface cérébrale et permettra au cerveau d'échanger directement avec le monde numérique.

Une des particularités des technologies d'AR et de VR est qu'elles associent des briques technologiques qui sont à des stades de maturité différents. Certaines existent déjà comme les lunettes connectées ou le rendu en 3D, d'autres sont en cours de développement : interfaces homme/machine adaptées aux contraintes de terrain, recalage réel / virtuel, apport de l'intelligence artificielle. Reste à rendre toutes ces briques interopérables et à en réduire le coût. L'utilisation de composants moins chers devrait contribuer à cette réduction, notamment pour les casques et les lunettes de VR. De même, la dissémination de ces technologies vers des marchés grands publics comme la santé, le tourisme, le cinéma ou les loisirs améliorera leur acceptabilité et donc leur diffusion.

La filière industrielle française, bien qu'encore fragmentée, dispose d'atouts forts dans ces domaines : un tissu dense de start-up, PME et grands groupes dont certains figurent parmi les leaders mondiaux, des laboratoires de recherche réputés et un marché national attractif. Cependant, la filière devra résoudre plusieurs problèmes pour gagner une position prédominante sur les marchés national et international. Outre les enjeux liés à la propriété intellectuelle, les applications de VR et d'AR devront aborder les questions règlementaires sur le droit à l'image et aux données à caractère personnel, mais aussi celles sur la sécurité d'utilisation et la santé. Pour cela, il conviendra de mettre en place un cadre juridique et de créer des bases de données opérationnelles. La normalisation des outils de simulation favorisera leur intégration et leur interopérabilité. ///

Algorithmes bio-inspirés et théorie de l'évolution

La simulation de la réalité dans un environnement virtuel s'appuie largement sur l'intelligence artificielle (IA) et particulièrement sur l'informatique biomimétique ou génétique. Celle-ci s'inspire du fonctionnement de l'humain et de la nature pour résoudre des problèmes.
Les réseaux neuronaux, qui s'inspirent de l'organisation structurale et fonctionnelle du cerveau, en constituent un bon exemple.
Pour mieux prédire les comportements de l'environnement simulé en VR ou en AR, on utilise des algorithmes bio-inspirés aussi appelés évolutionnaires.
Ces algorithmes sont ainsi dénommés car ils s'inspirent de la théorie de l'évolution, qui dit qu'au fil des générations, les êtres vivants s'adaptent à leur environnement. Les algorithmes bio-inspirés font évoluer plusieurs solutions afin d'identifier les meilleures et de les optimiser. Ils apprennent au fur et à mesure et optimisent également leurs propres méthodes de résolution.



Identité numérique, authentification

La numérisation de toutes les activités a un impact particulièrement critique sur le domaine de l'identification et de l'authentification. Toute personne doit pouvoir s'identifier en ligne pour interagir avec des services publics comme les impôts, la sécurité sociale ; consulter son dossier médical ou de retraite ; acheter sur Internet ; accéder à distance aux données de son entreprise… Mais les identifiants et les mots de passe ne répondent pas de façon satisfaisante aux exigences de sécurité de certains de ces services.

Trop nombreux, impossibles à mémoriser, les mots de passe découragent les utilisateurs qui contournent les règles de sécurité les plus élémentaires. Le classement annuel des mots de passe les plus utilisés place la suite de chiffres 01234567 ou les premières lettres du clavier en tête du palmarès, et ce depuis plusieurs années. Ce n'est pas mieux du côté des professionnels puisque le mot de passe le plus utilisé par les administrateurs de système informatique est « admin » ! Ce recours à la facilité rend les mots de passe particulièrement vulnérables. Conséquence, tant chez les particuliers que dans les entreprises, les vols de données, les paiements frauduleux et les usurpations d'identité font florès.

Si la multiplication des identités numériques pour une seule et même personne répond sans aucun doute à une demande des utilisateurs, elle présente toutefois plusieurs risques qu'il convient de prendre en compte. D'une part, l'utilisateur finit par contourner la sécurité car elle devient un frein à l'utilisation du service. D'autre part, les identités sont fournies par différents acteurs privés de l'Internet, notamment les GAFAM. Ceux-ci agrègent les données sur leurs plates-formes et les valorisent à leur profit. Ils privent ainsi les utilisateurs du contrôle sur leurs données à caractère personnel en même temps qu'ils colonisent peu à peu l'économie numérique française. Il y a là un enjeu important de souveraineté nationale.

L'utilisation d'une identité numérique forte doit permettre à un usager d'être identifié et authentifié dans toutes les transactions qu'il effectue au quotidien, que ce soit avec des services publics ou des fournisseurs de services privés. Et ce aussi bien sur un ordinateur qu'une tablette ou un smartphone. Cette identification pourra être activée par différentes technologies : biométrie (empreinte, voix, iris, ADN), carte à puce, sans contact, clé de chiffrement…

Une identité numérique forte doit bien évidemment être compatible avec les règlementations en vigueur en France (Référentiel général de sécurité, RGS) et en Europe (eIDAS, RGPD). Il conviendra de développer des outils règlementaires et d'audit de conformité aux différents règlements afin de s'assurer de leur respect par tous les acteurs, privés et publics. La chaîne de responsabilité juridique devra être définie clairement et des schémas de régulation mis en place en s'inspirant, par exemple, du GIE-CB.

La mise à disposition d'une identité numérique forte nécessite le déploiement d'architectures de « gestion des identités et des accès » (Identity & Access Management, IAM) qui soient tout à la fois sécurisées et transparentes. Elles doivent concilier un processus « sans couture » de l'identification en ligne, être agnostiques et adaptables au contexte d'utilisation des mécanismes d'authentification.

Pour inspirer la confiance des usagers et susciter leur adhésion, les mécanismes d'enrôlement devront être particulièrement faciles à utiliser et ne pas altérer la fluidité des échanges. Cela suppose des interfaces homme/machine (IHM) et des technologies d'opt-in et d'opt-out conviviales. L'utilisateur devra pouvoir gérer lui-même ses données personnelles ainsi que leur anonymisation ou « pseudonymisation ». La cybersécurité des solutions ne devra pas altérer la fluidité des échanges.

Les acteurs industriels français occupent des positions de leadership dans ce domaine, tant pour les éléments sécurisés que pour l'IAM ou l'intégration des solutions. Plusieurs d'entre eux maîtrisent les technologies clés que sont la cryptographie ou la biométrie. La rupture technologique qui s'amorce dans l'identification et l'authentification leur offre des opportunités, notamment en matière de développement de grandes plates-formes de services en ligne. Dans ce domaine, l'Europe souffre d'un déficit d'acteurs de taille significative. ///

10, c'est le nombre de mots de passe individuels utilisés en moyenne par un internaute en Europe.
En France, au Royaume-Uni et en Espagne, la moyenne est de 9.
Elle est de 11 en Allemagne et en Italie.

Source : étude IBM Security sur l'identité numérique et l'authentification (novembre 2017)

IDENTIFICATION / AUTHENTIFICATION

2018 ce que l'on fait :

- large diffusion d'identités fortes « verticales » : SIM cards, cartes bancaires, passeports…
- identités numériques délivrées par les GAFAM, majoritairement utilisées pour le e-commerce, Single Sign On (SSO) peu développé hors la sphère des GAFAM
- remplacement progressif du PIN par de la biométrie dans de nombreux domaines
- gestion minimale de la vie privée

2025 ce que l'on fera :

- large utilisation d'une identité forte pour des applications régaliennes et privées dans de nombreux pays
- l'utilisateur gère ses identités lui-même par identité dérivée numérique forte
- généralisation de la biométrie comportementale non invasive et de mécanismes d'enrôlement à distance
- identification et authentification contextuelles supportées par de l'IA
- systèmes d'IAM (Identity & Access Management) conformes au RGPD

3 questions à… Gwendal Le Grand, directeur des technologies et de l'innovation à la CNIL (Commission nationale de l'informatique et des libertés)

L'identité numérique : technologie clef pour la cybersécurité

Une « identité numérique » peut-elle servir aussi bien au citoyen qu'à l'internaute et au consommateur ?

Gwendal Le Grand : L'identité numérique permet l'identification et l'authentification, c'est-à-dire d'identifier une personne dans une population donnée et de prouver que l'identité qu'elle renseigne est bien la sienne. Mais cette identité doit rester multiple et contextuelle.

C'est-à-dire ?

G. Le G. : Nous utilisons tous différents noms, pseudonymes ou identifiants selon le contexte ou les services consultés. Ces identités sont vérifiées par des moyens variés, un couple identifiant - mot de passe, un certificat électronique ou de la biométrie, par exemple. Mais tous les services n'ont pas besoin du même niveau de vérification. Un service bancaire en ligne a besoin d'un plus haut niveau à la fois d'identification et d'authentification qu'un abonnement non subventionné à une piscine municipale pour lequel un simple badge avec photo est suffisant. La pluralité des identités numériques nous permet de séparer les différents aspects de notre vie et de ne fournir que les données nécessaires à chaque service. C'est une question de sécurité des données mais cela donne aussi à chacun la possibilité d'avoir plusieurs identités, plus ou moins complètes et non reliées entre elles.

La législation européenne est-elle homogène sur ce sujet de l'identité numérique ?

G. Le G. : Le règlement européen sur « l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur » est entré en application le 1er juillet 2016. Depuis, les autorités de protection des données européennes ont adopté une position commune sur ce que devrait être une identité numérique respectueuse de la vie privée et elles incitent les acteurs du numérique à ne propager que les informations strictement nécessaires.

Plates-formes intégrées véhicules/services

La multiplication des véhicules connectés et autonomes dans l'aérien, dans le ferroviaire et bientôt sur les routes laissent envisager de nouvelles applications pour les industries de sécurité. Les UAV (Unmanned aerial vehicle) en particulier, communément appelés les drones, offrent d'importantes perspectives dans le transport de personnes ou de colis, et surtout dans la surveillance aérienne. Dans un avenir très proche, des voitures de patrouille autonomes surveilleront la circulation et pourront verbaliser un excès de vitesse ou faire intervenir un drone pour suivre un véhicule en infraction.

Cette possibilité de communiquer et d'interagir entre les différents types de véhicules nécessite la mise en œuvre de plates-formes dédiées et sécurisées, qui intègrent l'infrastructure de communication et une offre de services. Ces plates-formes permettront, par exemple, de gérer le trafic afin de faciliter la circulation des véhicules autonomes prioritaires ou de coordonner en temps réel les véhicules d'intervention avec les systèmes de surveillance que sont les drones ou les robots terrestres.

640 milliards d'euros, c'est le marché mondial des véhicules autonomes en 2030, véhicules terrestres, train, air, mer et espace.
Les véhicules ne représentent que 22 % du marché mondial de l'autonomie qui s'élèvera à 2950 milliards d'euros. Les autres composantes de ce marché sont la maintenance et la révision (11 %), les flottes, la gestion du trafic et les infrastructures (34 %), les services, les systèmes et les données (33 %).

source : La révolution de l'autonomie, Oliver Wyman, 2017

L'avènement de ces plates-formes de services intégrées nécessite l'élaboration de nouveaux business modèles, reposant sur l'usage et non plus sur la propriété, et surtout d'une réglementation adaptée notamment pour la circulation des drones et leur mise en œuvre par les forces de sécurité. Les véhicules autonomes imposent d'assurer un haut niveau de cybersécurité afin d'éviter le piratage des systèmes de pilotage, par exemple. Cette cybersécurité devra par ailleurs être certifiée sur tous les aspects. Il est également important de concevoir de nouveaux logiciels et interfaces homme/machine à base d'intelligence artificielle et d'automatisation afin de limiter la charge cognitive des intervenants de sécurité et leur permettre de se consacrer entièrement à leurs missions. Les plates-formes devront être en mesure d'intégrer des données en provenance de systèmes très hétérogènes.

Le secteur français compte de nombreux acteurs déjà très engagés dans ce domaine de l'autonomie des transports et des plates-formes intégrées. Il faut encore consolider les efforts menés au niveau national, tant dans le public que dans le privé, dans la recherche comme dans l'industrie. Cette consolidation ouvrira la voie à l'élaboration d'une stratégie européenne équilibrée ainsi que de règlementations et de certifications homogènes. Car les GAFAM, les BATX, Tesla et les grands acteurs américains du logiciel ne demandent qu'à investir ce secteur particulièrement prometteur économiquement, mais stratégique pour la souveraineté de chaque Etat. ///

PLATES-FORMES INTÉGRÉES

2018 ce que l'on fait :
- robot rondier terrestre autonome
- expérimentation de véhicules autonomes en environnement limité, de niveau d'autonomie 3 ou 4 en Europe, de niveau 5 aux Etats-Unis et en Asie
- environnement limité en cybersécurité sur les drones

2025 ce que l'on fera :
- équipes cobotiques d'intervention sur le terrain (forces de police, sécurité civile ou privée) avec l'assistance de robots semi-autonomes, capables de traiter des données et de produire des analyses de situation, et de drones éclaireurs intelligents et sécurisés
- véhicules autonomes adaptés aux missions de sécurité : connexion complète avec les intervenants et les équipements des véhicules, coopération avec les agents, gestion des priorités…
- essaims de drones pilotés à distance pour des missions en continu indoor/outdoor

Détecter les produits dangereux, illicites ou contrefaits

EuroBioTox, un programme H2020

Consciente des risques d'attaques biologiques qui pèsent sur la société civile et face à la nécessité pour les pays européens de s'y préparer, l'Union européenne a inscrit le projet EuroBioTox dans son programme-cadre de recherche Horizon 2020.
Il s'agit de définir les standards pour les outils et les procédures d'analyse, sur la base de scénarios, d'incidents réalistes, et de créer un référentiel européen des toxines biologiques, qui sera mis à disposition des laboratoires, organisations et entreprises partenaires ou utilisateurs. EuroBioTox concevra les formations nécessaires et le programme de validation des connaissances. A terme, l'objectif est de disposer d'un réseau paneuropéen de compétences, de matériaux référencés et certifiés et de pratiques communes de gestion des incidents toxiques. Lancé en juin 2017 pour une durée de 5 ans, EuroBioTox rassemble 13 acteurs européens dont l'Institut Pasteur de Paris, le CEA et l'ANSES pour la France. Au total, 57 institutions de 23 pays ont répondu favorablement pour participer aux essais inter-laboratoires et formations qui seront proposés dans le cadre du projet.

Pour plus d'information :
https://www.eurobiotox.org

Les technologies de détection de produits dangereux ou illicites sont en train d'évoluer rapidement pour s'adapter aux nouvelles menaces. Sont concernées les armes, les attaques biologiques, la détection de stupéfiants ou de produits explosifs mais aussi l'identification rapide d'un composant chimique. Les progrès technologiques permettront entre autres une détection à la volée dans un flux de personnes ou de colis, le diagnostic et l'analyse en temps réel grâce à des méthodes physiques sans réactif spécifique, ou la surveillance en continu de l'environnement.

Pour que ces applications soient possibles, il faut parvenir d'une part à miniaturiser les systèmes et les appareils, et d'autre part à augmenter leur autonomie pour autoriser leur utilisation sur le terrain. Cela concerne, par exemple, le séquençage ADN haut débit ou le test par spectromètre de masse embarqué. Ces instruments devront également être faciles à utiliser par les agents sur le terrain. Il faut en outre réduire leur coût, ce qui pourra être atteint par l'effet de volume et par la dissémination des technologies vers les utilisateurs. L'intégration d'une fonction ou d'un instrument dans un smartphone pour des applications dans le domaine de la santé ou le contrôle d'objets connectés, par exemple, faciliterait cette diffusion à un large public.

Si la filière française est solide en Recherche & Développement et compte de nombreuses start-up et intégrateurs de solutions, elle est en revanche plus faible du côté industriel de l'instrumentation. Le marché est relativement

fragmenté, ce qui le rend vulnérable à la concurrence étrangère, notamment japonaise et américaine. Le sujet de la détection manque encore d'une réglementation forte et il devra être en conformité avec les règles de respect de la vie privée. La filière française doit se munir rapidement d'une feuille de route dans ce domaine et susciter la création d'une culture technologique auprès des opérateurs. Elle doit développer des plates-formes de démonstration qui intègrent les différentes technologies aux infrastructures critiques et définissent les usages, en étroite collaboration avec les acteurs du secteur. ///

DÉTECTION

2018 ce que l'on fait :
- multiplication des analyseurs de composition chimique miniaturisés de terrain, connectivité des capteurs aux smartphones qui traitent les données
- applications métier et grand public de lutte contre les contrefaçons
- coût d'un séquençage ADN en mode batch : environ 50 €

2025 ce que l'on fera :
- large déploiement des capteurs, dont le coût aura fortement baissé, ils seront portés par les intervenants ou intégrés aux bâtiments
- détection performante à la volée d'armes et de substances dans un flux de personnes, utilisation massive de capteurs individuels en réseau : fixes ou sur smartphone, grand public ou spécialisés métiers
- séquençage ADN quasiment à la volée

L'humain augmenté par la technologie

Les technologies numériques augmentent les capacités opérationnelles des forces d'intervention de manière importante. Et ce de différentes façons. Que ce soit par des dispositifs externes comme les exosquelettes ou par des services dématérialisés fournis par des applications logicielles, le digital transforme les agents en « intervenants augmentés », doués d'ubiquité et de résilience.

Les dispositifs externes comprennent les exosquelettes et les robots collaboratifs, alias les cobots. Les premiers augmentent la force et la résistance des agents en leur permettant de soulever et de déplacer de lourdes charges, jusqu'à une centaine de kg, sans problème. Ils améliorent également leur endurance dans des conditions de terrain accidenté, par exemple, et de fait, diminuent leur fatigue. Les cobots les assistent en automatisant certaines tâches, comme c'est déjà le cas pour le déminage ou la surveillance de lieux mal accessibles aux forces d'intervention. La réalité augmentée ajoute aussi des capacités nouvelles aux intervenants en enrichissant leur perception de l'environnement par des informations numériques en surimpression ou de la vision thermique.

3,3 milliards de dollars,
c'est le montant que devrait atteindre le marché mondial des exosquelettes en 2025
(Grand View Research)

L'augmentation des capacités opérationnelles des agents passe aussi par de nouveaux matériaux, plus performants. Il s'agit par exemple de textiles résistants au feu ou capables de changer de couleur en cas de présence de toxique dans l'atmosphère. Les textiles et les vêtements vont devenir de plus en plus intelligents grâce notamment aux nanotechnologies. S'y ajouteront des polymères dotés de capacités nouvelles, le graphène pour des batteries rechargeables rapidement et ayant une autonomie plus longue, des écrans souples et des capteurs intégrables aux vêtements qui deviendraient ainsi des dispositifs connectés… Les intervenants disposeraient alors de données de géolocalisation, de moyens de communication en continu avec le poste de commandement et d'outils d'évaluation de la situation et de décision en temps réel.

Quelques acteurs sont déjà positionnés sur le marché des exosquelettes. Ces derniers vont évoluer pour être à la fois ultra résistants et plus légers. Les domaines à investiguer pour la filière industrielle vont des capteurs ULP (ultra low power) sécurisés et auto-alimentés aux nouveaux matériaux en passant par l'électronique souple, les algorithmes et l'intelligence artificielle nécessaires aux robots, cobots et autres dispositifs. Un autre domaine à développer est celui des technologies vocales et des assistants conversationnels à base d'intelligence artificielle (bots). Ceux-ci permettront aux agents sur le terrain d'interagir avec les différents dispositifs par la voix, de se connecter au cloud et de bénéficier d'une assistance par intelligence artificielle tout en gardant les mains libres. Autrement dit, ils pourront intervenir en disposant des nombreux apports que leur offre la technologie, en mode collaboratif, mais en étant disponibles à 100 % pour leur mission. ///

INTERVENANT AUGMENTÉ

2018 ce que l'on fait :
- utilisation des smartphones avec applications métiers
- exosquelettes

2025 ce que l'on fera :
- exosquelettes légers, nouveaux matériaux (auto-décontaminants)
- les premiers capteurs connectés sont totalement intégrés dans la tenue
- agent avec équipement de réalité augmentée et interface homme machine vocale, connecté au cloud, assisté par IA et aides automatiques, et concentré à 100 % sur sa mission en mode collaboratif

Observation locale

Les technologies au service de l'observation ne sont pas nouvelles, mais les progrès accomplis dans certains domaines, comme la géolocalisation à l'intérieur des bâtiments, et l'utilisation d'outils d'intelligence artificielle (IA) et de Machine Learning (ML) ouvrent de nouvelles perspectives et font de l'observation locale un domaine de rupture.

Bientôt, pour assurer la sécurité d'un grand événement, par exemple un match ou un concert dans un stade, l'ensemble des informations et des incidents pourra être intégré, depuis le ciel (caméras embarquées sur des drones) jusqu'aux couloirs et aux tunnels du métro en passant par les locaux, les parkings, les voies d'accès (vidéoprotection), etc. Une telle application suppose la définition d'un modèle cartographique continu et unique – et donc d'une norme de représentation – afin de permettre la géolocalisation 3D « sans couture » à l'extérieur comme à l'intérieur des bâtiments. Elle suppose également de disposer de moyens de géolocalisation et de communication incluant les infrastructures et résilients à un sinistre ou à une explosion. Enfin, elle suppose l'interopérabilité entre les systèmes des différents acteurs dans une zone donnée et l'intégration des flux vidéo dans cette zone afin de pouvoir localiser rapidement un individu et le suivre.

Etape nécessaire à l'efficacité de ces applications, les images en provenance des caméras de vidéosurveillance devront être indexées automatiquement afin d'être interrogées par un outil de recherche universel, un « Google » de la vidéo en quelque sorte. L'IA et le ML faciliteront à la fois l'indexation et la recherche en accélérant le tri des données et en identifiant des schémas (patterns) qui se répètent pour la détection automatique de situations à risques. L'expérimentation opérationnelle de ces nouvelles capacités est clé pour faire progresser tout à la fois les applications analytiques de vidéoprotection et l'encadrement légal visant au respect de la vie privée. ///

En 2025, **le marché mondial des systèmes d'information géographique (SIG)** devrait atteindre **11,2 Mds US$**, dont la moitié aux Etats-Unis
(Grand View Research)

OBSERVATION LOCALE

2018 ce que l'on fait :
- système de surveillance vidéo 3D sans couture avec analyse en temps réel

2025 ce que l'on fera :
- observation indoor/outdoor 4D coopérative, anonymisée, sans couture, avec gestion automatique par IA dans les villes intelligentes et les bâtiments
- capacité d'indexation et d'exploration des données vidéo massives distribuées en temps réel (« Google » vidéo de la sécurité)
- déploiement massif de la vidéo en tout lieu, accès aux données en mobilité y compris intérieure traitées automatiquement grâce à l'IA

Victoria, l'analyse vidéo contre le terrorisme

Après un attentat, il est urgent d'analyser le plus rapidement possible toutes les sources d'information disponibles, y compris les vidéos. L'analyse des images en provenance des caméras de surveillance mais aussi des smartphones des personnes présentes, est pour l'instant essentiellement manuelle, et de fait limitée. Le projet Victoria (Video analysis for Investigation of Criminal and TerrORIst Activity) veut répondre à ce problème en développant une plate-forme d'analyse vidéo (VAP) dédiée. Le projet a été lancé en mai 2017 pour une durée de 3 ans dans le cadre du programme européen Horizon 2020. Les enjeux de Victoria sont de :
- définir une standardisation des formats pour le partage des flux vidéos entre les pays et l'interopérabilité des systèmes
- pouvoir analyser les flux vidéo en fonction de différents critères
- disposer de jeux de données de référence afin de « nourrir » les algorithmes d'analyse d'images.

A terme, Victoria ambitionne d'enrichir les vidéos de métadonnées, qui décriront et indexeront les images, ce qui les rendra interrogeables en fonction de critères comme par exemple, retrouver et suivre les hommes de telle taille portant un chapeau ou un sac à dos et qui sont arrivés par le train entre telle et telle heure. Le projet Victoria contribue également aux travaux de la plate-forme d'expérimentation de la vidéoprotection intelligente VOIE. Ce démonstrateur du CoFIS teste les performances des nouvelles applications analytiques en environnement réel au bénéfice des opérateurs de transport et du ministère de l'Intérieur.

Blockchain

D'abord associée aux cryptomonnaies et au Bitcoin en particulier, la blockchain s'impose comme un nouvel outil indispensable de la sécurité. Ce protocole enregistre et stocke les transactions sous forme cryptée dans une base de données décentralisée. Les informations sont, de fait, infalsifiables et non modifiables. Registre distribué et sécurisé de transactions, la blockchain est à la fois un vecteur de confiance et un outil de lutte contre la fraude. Elle est soit publique, tous les participants peuvent intervenir dans le processus, soit privée. Dans ce cas, seuls certains participants enregistrent des transactions et autorisent ou non leur lecture.

Utilisée dans un premier temps pour le « minage » de cryptomonnaies, la blockchain est à présent mise en œuvre dans de nombreux secteurs (finance, joaillerie, cadastre, art, santé, notariat, …). Dans le domaine de la sécurité, elle va rapidement trouver nombre d'applications : gestion des prestations sociales, protection des infrastructures des opérateurs d'importance vitale, mais aussi missions de sécurité civile ou intérieure et gestion du secret entre institutions. Ces applications réduiront la dépendance à une autorité centrale mais elles nécessitent l'évolution du système de confiance centralisé actuel vers un système décentralisé pour les applications de type régalien ainsi qu'une nouvelle organisation des opérations.

En 2024, **le marché global de la blockchain devrait atteindre 7,6 Mds US$.** Entre 2015 et 2024, il devrait progresser avec un taux de croissance annuel moyen (CAGR) de 37,2 %

(Grand View Research)

Citons quelques-uns des verrous technologiques qu'il faudra lever avant de déployer la blockchain dans des applications de sécurité. Les identifiants devront pouvoir être gérés de façon dynamique et traçable. Les solutions devront fonctionner a minima en mode non connecté. Les propriétés de sécurité et le modèle de sécurité de la blockchain devront faire l'objet de vérifications formelles. Enfin, le sujet de la protection des données à caractère personnel devra être abordé et l'évolution de la technologie vis-à-vis de la législation devra être anticipée.

Les acteurs français maîtrisent plusieurs des technologies clés du domaine de la blockchain (cryptographie, méthodes formelles…). Cependant, il faut souligner qu'il n'existe pas – encore – de blockchain « made in France » et que le niveau d'acceptation de la technologie par les utilisateurs est encore faible. La réalisation de démonstrateurs par filières (gestion du secret, protection des OIV, distribution des prestations…) contribuerait à augmenter la notoriété de cette technologie et favoriserait le développement d'une ou de plusieurs blockchains privées. ///

BLOCKCHAIN

2018 ce que l'on fait :
- large développement des cryptomonnaies
- nombreux projets pilotes dans les grands secteurs économiques (énergie, finance, IoT, cadastre…)
- capacités temps réel limitées, consommation d'énergie non maîtrisée

2025 ce que l'on fera :
- disponibilité d'algorithmes PoS (Proof of Stake, preuve d'enjeu) et PoW (Proof of Work, preuve de travail) temps réel et peu énergivores
- utilisation de la blockchain pour la gestion du secret en inter-institutionnel
- gestion par de la blockchain de subventions au niveau national (prestations sociales) ou international (PAC) et généralisation des « smart contracts »
- gestion de l'intégrité de certaines architectures IoT industrielles par des blockchains dont la sécurité aura été prouvée

Ubérisation, post-ubérisation

L'« ubérisation » et ses synonymes, la désintermédiation ou la disruption, ont vu le jour avec l'avènement des start-up et grâce aux moyens technologiques fournis par le numérique. Avec le haut débit et les smartphones, Internet est accessible partout à tout moment. Cet accès en mobilité associé à la géolocalisation fait que nombre de services sont accessibles en dehors des opérateurs habituels de ces services. Des plates-formes mettent en relation directe les fournisseurs d'un service – taxi, par exemple – et les utilisateurs, et ce à un coût généralement inférieur à celui des opérateurs traditionnels.

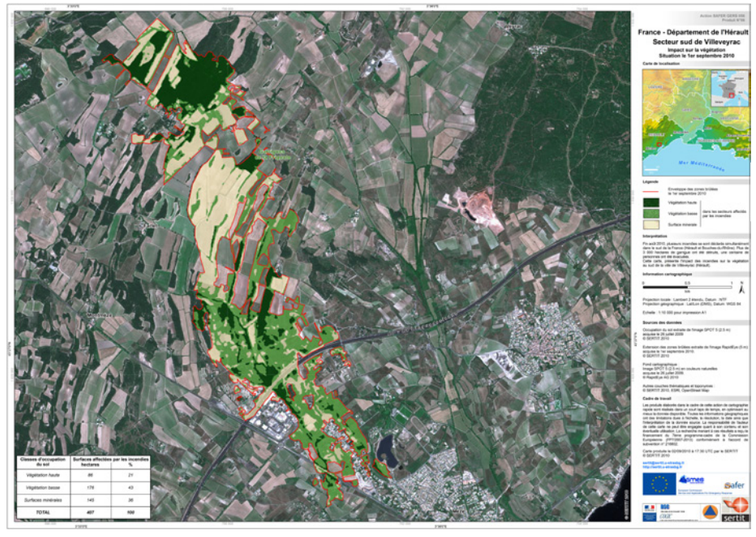
En matière de sécurité, cette « ubérisation » se traduit par de nouvelles capacités. Une plate-forme dans le cloud permet le déploiement de solutions « à la demande », pour la mise en place d'un service de supervision d'environnement opérationnel imprévu, par exemple. De même, des services ponctuels collaboratifs, associant des drones, des robots et des réseaux sociaux, peuvent être rapidement mis en œuvre pour des missions de surveillance du trafic, de la délinquance, des frontières, etc. Autant de solutions qui seraient disponibles en mode « Security as a Service », SECaaS.

Cette nouvelle organisation et l'économie qui en découle ouvrent des perspectives intéressantes, mais elles nécessitent plusieurs adaptations. Le modèle économique qui prévalait – vente de produits, de services ou de licences logicielles – laisse la place à l'abonnement, à la location et au paiement à l'usage. La logique fournisseur/acheteur est remplacée par un modèle de crowdsourcing et de co-construction associant aux concepteurs les utilisateurs des produits ou des services. Les applications orientées sécurité sont disponibles dans des « appstores », dédiés ou non. Les réseaux sociaux, les environnements IoT et les applications de big data se combinent et permettent de construire des services de sécurité quasiment à la demande.

Le marché de la Security as a Service (SECaaS) passerait de **4,25 Mds US$ en 2016 à 25,5 Mds US$ en 2025**

(Cision PR Newswire)

La France dispose d'un solide secteur du logiciel tant du côté industriel que du côté académique. Mais le pays compte aussi quelques points faibles, notamment le fonctionnement en silo de certains types d'acteurs et le petit nombre d'opérateurs de déploiement de services nationaux présents à l'échelle mondiale. S'ajoute à cela le choix des utilisateurs, qui privilégient les services à moindre coût parfois au détriment de la sécurité… ///



UBÉRISATION

2018 ce que l'on fait :
- premières applications disponibles sur smartphone, en smart-city en particulier
- premières applications de type Security as a Service (SECaaS), par exemple : Identity as a Service ou HSM as a Service…
- services de « tokenisation » du type HCE

2025 ce que l'on fera :
- disponibilité de plates-formes coopératives privées proposant des services de sécurité à la demande qui conjuguent des données des réseaux sociaux, du big data et de l'open data
- généralisation du concept de SECaaS
- disponibilité d'« appstores » orientés sécurité avec certification instrumentée par IA
- systèmes clé en main de gestion massive d'IoT

Plates-formes ouvertes en sécurité

Le partage de code logiciel ou de design de matériel et de composants est de plus en plus pratiqué. Les logiciels et les matériels en mode Open source accélèrent l'innovation en permettant aux développeurs et aux concepteurs de partager et de réutiliser les développements réalisés par d'autres. La re-publication en Open source des nouveaux développements alimente le processus d'innovation et bénéficie à toute la communauté.

Le secteur de la sécurité peut lui aussi profiter de ce principe d'intelligence collective. La constitution de bibliothèques de composants Open source, qu'ils soient logiciels ou matériels, accélère l'évolution des designs et diminue le coût de conception des nouveaux produits. A condition toutefois d'intégrer les notions de sécurité et de confidentialité dans tout le processus d'élaboration des produits et des services, et ce dès le stade de la conception, ce que l'on appelle « Security & Privacy by Design ».

Recourir à l'Open source, matériel ou logiciel, suppose l'adoption de nouveaux business modèles et de nouveaux modes de licences. Ceux-ci devront être adaptés aux modes de consommation du logiciel en libre-service ou à la demande. Les plates-formes dédiées à la gestion des objets connectés et les infrastructures cloud devront être sécurisées. La question des brevets et de la propriété intellectuelle ou industrielle devra également être abordée.

Software Heritage, le référentiel du code source

Le projet Software Heritage, lancé par INRIA en juin 2016, ambitionne de construire la « bibliothèque d'Alexandrie » du logiciel. Le but est de collecter, d'organiser, de préserver et de rendre accessible le code source des logiciels disponibles publiquement, c'est-à-dire en modeOpen source. Software Heritage est à la fois un grand instrument de recherche pour l'informatique et un référentiel, une sorte de catalogue, qui permet aux développeurs de nouveaux logiciels de trouver, de réutiliser et d'archiver des codes sources. En à peine deux ans d'existence, Software Heritage a déjà recueilli dans sa base de données plus de 83 millions de projets, qui représentent quelques 4,5 milliards de fichiers sources uniques, ainsi que l'historique de leur développement. Le projet bénéficie du parrainage de Microsoft, Société Générale, Intel, GitHub, DANS (Data archiving and networked services) ou Huawei entre autres.
Pour en savoir plus : www.softwareheritage.org

Les atouts de la France dans ce domaine de l'Open source sont nombreux. Le marché national est très développé, il représente le quart du marché européen. La communauté tant des chercheurs que des développeurs est sans conteste la plus nombreuse et la plus avancée. Cependant, la sécurité est peu présente dans le monde Open source. Le marché de la sécurité est encore dominé par les grands éditeurs de logiciels propriétaires, nord-américains pour la plupart. Une politique d'achat volontariste et l'incitation au développement de briques technologiques et de plates-formes orientées vers l'Open source contribueraient au renforcement de ce domaine. ///

PLATE-FORMES OUVERTES

2018 ce que l'on fait :

- projets Open HW (hardware) source essentiellement pour applications grand public
- large pénétration des logiciels Cloud Open source de type OpenStack avec conteneurisation mais de sécurité peu robuste
- nombreux logiciels de sécurité en Open source

2025 ce que l'on fera :

- plates-formes Open HW orientées sécurité avec certification
- généralisation des plates-formes virtuelles embarquant une carte circuit intégré (VPP UICC) pour applications IoT et embarquées
- disponibilité de bases de données de logiciels Open source instrumentés sécurité et confidentialité
- innovation en logiciel pilotée par l'Open source, y compris en sécurité

A propos du CoFIS

Le Comité de la filière des industries de sécurité a été mis en place par le Premier ministre en octobre 2013. Il a pour ambition de développer les moyens nécessaires pour faire face aux menaces et risques susceptibles de porter atteinte à la vie de la Nation et de soutenir l'activité des industries françaises de sécurité au travers d'un dialogue public-privé rénové (www.cofis.fr).

Avertissement :

Sur la demande du CoFIS, ces travaux ont été conduits de septembre 2016 à décembre 2017 par des experts issus du monde académique et industriel ainsi que des ministères.

Le contenu de ce document est le reflet du travail d'un groupe d'experts volontaires mis en place par le CoFIS, rédigé par une journaliste. Les analyses et les propositions qui y figurent n'engagent en aucun cas une position officielle du gouvernement.

Remerciements :

Aux participants du groupe de travail dédié mis en place par le CoFIS sous le pilotage de M. Jean-Pierre Tual, vice-président Recherche et Innovation du CoFIS et directeur scientifique du pôle Systematic.

L'institut IDATE DigiWorld.

La société RGA systems pour le soutien méthodologique sur les priorités.

Mme Sophy Caulier, journaliste indépendante, pour son aide dans la rédaction des conclusions du groupe d'experts.

Crédits photos :

p. 8 : Kiev.Victor / Shutterstock.com ; p. 9 : Shutterstock, Thales, Idemia ;
p. 14 : Shutterstock ; p. 16 : Idemia, Shutterstock ;
p. 18 : Thales ; p. 20 : P. Stroppa/CEA ;
p. 21 : P. Dumas/CEA ; p. 22 : Surys ; p. 23 : Idemia ;
p. 24 : SGDSN/ANR, HGH ; p. 25 : DR, Ouvry ; p. 26 : Airbus ;
p. 27 : Shutterstock ; p. 28 : DR ; p. 29 : TEB, Airbus ; p. 30 : Thales