Investissements d'avenir
Action : « Projets industriels d'avenir (PIAVE) »

Cahier des charges de l'appel à projets
« Sécurité des personnes et des biens, des infrastructures et des réseaux »
-
Annexe 2
Thématiques techniques

Axe 1 – Démonstrateur d'Identité numérique

L'identité numérique constitue le socle de la confiance numérique, qui est au cœur d'enjeux économiques et sociétaux majeurs. L'objet de ce démonstrateur est de développer les technologies innovantes nécessaires pour réaliser une plateforme ouverte, interopérable et multi-fournisseurs d'identification des personnes et de contrôle de leurs droits dans le monde numérique. Il s'agit de proposer des solutions d'infrastructure de délivrance et de gestion de gestion d'identités numériques, avec les services d'authentification associés. Une telle plateforme doit contribuer, au-delà-des aspects technologiques, à une mise en perspective d'un projet complet - dont les problématiques d'organisation et d'infrastructure de fourniture d'identité - d'utilisation à grande échelle dans le cadre d'un modèle économique associé.

Les points suivants sont à prendre en compte :

- la compatibilité avec le règlement Européen eIDAS entré en vigueur au 1er Juillet 2016 en visant les niveaux d'assurance « substantiel » et/ou « élevé »,
- la protection des données personnelles,
- l'interopérable des identités acquises et des services d'identification,
- la compatibilité avec France-Connect,
- la capacité à viser l'ensemble des applications de l'Identité Numérique depuis les messageries, les services en ligne, jusqu'aux applications régaliennes,
- l'appropriation par les usagers : facilité d'acquisition, facilité d'usage, couverture d'une partie large de la population, coût de revient faible,
- la maîtrise des coûts liés à l'identité numérique qu'il s'agisse des coûts portés par l'utilisateur, les services auprès desquels l'identité numérique est utilisée, les fournisseurs des moyens d'identité électronique et de mécanismes d'authentification,
- l'indépendance vis-à-vis des fournisseurs de services en ligne,
- l'ouverture pour développer un écosystème de l'identité numérique.

Le démonstrateur doit notamment inclure le développement d'innovations technologiques qui portent sur :

- l'amélioration des moyens de contrôle de l'identité et d'authentification en ligne,
- de nouvelles architectures de gestion de l'identité numérique, permettant notamment la gestion technique de l'enrôlement à distance et la prise en compte des spécifications FIDO (authentification double facteur),
- la possibilité de compatibilité ascendante ou de substitution avec les solutions d'identité numériques existantes basées sur un login/mot de passe,
- des dispositifs de lutte contre la fraude aux différentes étapes de la création et de l'utilisation de l'identité numérique, et la gestion technique (éléments de preuves et systèmes de détection) permettant la détection et l'alerte en cas de fraude, sur des identités délivrées au niveau national ou par un autre Etat membre,
- le développement de nouvelles infrastructures cryptographiques,
- les liens et protocoles techniques entre opérateurs de réseaux et gestionnaires d'identités, éventuellement étatiques, pour permettre notamment la gestion des identités virtuelles sur des supports type SIM,
- les protocoles entre l'identité numérique d'un usager et les objets intelligents qu'il détient ou auxquels il accède, notamment pour l'authentification.

Un modèle économique robuste est attendu avec un développement commercial important et des retombées économiques importantes sur le territoire national. Ce modèle économique doit prendre en compte les contraintes de coût global de possession pour les différents acteurs (usagers et également autorités publiques ou sociétés privées clientes ou partenaires de la solution).

Axe 2 – Démonstrateur de sécurité de la ville intelligente

Le bon fonctionnement et la sécurité de la ville numérique (ou « Smart-City ») dépend d'une interconnexion de systèmes complexes plus ou moins interdépendants : transports publics, énergie, télécommunications, infrastructure transactionnelle, sécurité civile et police, services gérés par la collectivité, trafic automobile, sécurité des citoyens dans leur environnement, prévention situationnelle, collecte des déchets, réseaux de capteurs urbains, etc…

L'objet de ce démonstrateur est de développer et intégrer in situ les briques technologiques permettant la réalisation d'une plateforme ouverte de partage et de gestion d'informations entre différents opérateurs de services et acteurs de sécurité d'une grande ville ou d'une aire métropolitaine (quartier d'affaires par exemple).

Les points à prendre en compte dans la conception des projets de démonstrateurs sont les suivants :

- la pleine implication de l'ensemble des acteurs de la sécurité pertinents sur le territoire,
- la résilience à différents scénarios d'incidents,
- les possibilités de simulation des incidents et des conséquences induites,
- la capacité à mesurer l'impact du démonstrateur et des technologies sur la sécurité de la ville intelligente,
- l'intégration et l'interopérabilité des systèmes des différents acteurs, collectivités, fournisseurs de services, opérateurs (énergie, transport,…),
- la sécurité des systèmes (depuis l'accès aux systèmes, les communications jusqu'au stockage des données),

- le partage, la consolidation et l'analyse d'un grand nombre informations,
- les enjeux sociétaux et notamment de protection de la vie privée,
- les enjeux de coordination et de gouvernance entre les différents acteurs de sécurité,
- l'environnement économique et les solutions possibles de financement.

Axe 3 - Démonstrateur protection des lieux ouverts et multimodaux

Si la problématique de sécurisation des lieux ouverts en amont de l'embarquement des trains sur les grandes gares et des aéroports vis-à-vis de la menace terroriste n'est pas nouvelle, les différentes attaques conduites sur le Thalys et dans l'aéroport de Bruxelles, pour ne citer que ces exemples, ont conduit l'Etat et les opérateurs à mener un état des lieux puis à faire des propositions dans le cadre du plan d'actions du gouvernement contre la radicalisation et le terrorisme.

Sur le moyen-long terme la principale proposition consiste à mettre en place une plateforme de test visant à la protection des lieux ouverts et multimodaux. A l'image de la plateforme sur la videoprotection intelligente VOIE, démonstrateur lancé par le CoFIS en 2015, cette plateforme aurait pour objectifs dans la durée de :

- mettre en situation des matériels et solutions techniques suffisamment matures pour être testés dans un contexte opérationnel afin d'en évaluer l'efficacité et la compatibilité avec les contraintes des opérateurs (réglementaire, organisationnel, impact sur les employés, les flux, le sentiment et le comportement des usagers) ;
- permettre aux opérateurs et administrations d'avoir accès, à coûts partagés, à un panorama des solutions techniques à l'état de l'art et à un retex opérationnel représentatif ;
- orienter les solutions et les travaux des industriels vers des approches répondant à ces contraintes selon une dimension système (complémentarité des solutions selon le concept de défense en profondeur) ;

Les conditions de la mise en œuvre d'une telle plateforme doivent être souples :

- il ne s'agit pas de créer une plateforme de test dans un lieu physique centralisé mais de mettre en réseau et de pérenniser les outils mis en place par les opérateurs souhaitant s'y associer, chacun gardant ainsi le contrôle de ses investissements ;
- les conditions de participation aux travaux de la plateforme doivent être ouvertes aussi bien aux opérateurs souhaitant s'y associer, qu'aux fournisseurs venant y tester leur matériel, cette dernière condition étant essentielle pour les éventuelles phases ultérieures d'achat public ;
- cette plateforme doit associer des opérateurs, des administrations et des industriels selon le type de travaux à réaliser.

Toutes les formes d'insécurité dans un lieu ouvert multimodal sont concernées mais un accent sera mis sur la gestion des colis suspects et l'empêchement de la circulation d'armes et d'explosifs dans de tels lieux.

La disponibilité d'une telle plateforme permettrait de construire une approche sécuritaire crédible et valorisable par les opérateurs et les industriels qui y auront été associés afin de proposer des évolutions en matière normative (réglementation, standards).

Axe 4 - Démonstrateur et projets de R&D pour la protection des infrastructures critiques type Seveso contre la malveillance

Les évènements survenus en 2015 à Saint-Quentin-Fallavier, dans l'Isère, à Berre-l'Etang, dans les Bouches-du-Rhône, ont démontré que les sites industriels peuvent être la cible d'attaques malveillantes voire terroristes. Les moyens mis en place sont souvent très liés aux contraintes de sûreté de fonctionnement et des obligations réglementaires liées aux sites classés ou à la protection de l'environnement et des populations environnantes et moins aux problématiques de sécurité. Cela est particulièrement vrai pour la réglementation des installations classées pour l'environnement, en particulier celle qui découle des directives européennes « Seveso ».

Les événements récemment ont également confirmé l'acuité de la menace interne liée entre autre à la radicalisation violente mais aussi à la réalité de la malveillance. Ces aspects ne sont que très rarement pris en compte, notamment dans les études de danger. Le démonstrateur vise à développer des solutions cohérentes des deux points de vue « sureté et sécurité », y compris au plan économique pour éviter l'empilement de moyens.

C'est pourquoi le gouvernement a prescrit un certain nombre d'actions relatives au renforcement de la sécurité des sites Seveso contre les actes de malveillance. Parmi celles-ci, la mise en place d'une réponse de nature technologique pour le renforcement de la sécurité des sites a été confiée au CoFIS fin 2015. Un groupe de travail interministériel avec la participation des opérateurs, des industriels et de bureaux d'études a conclu à la nécessité de :

- mettre en place un démonstrateur de plateforme de test de solutions techniques qui feraient sens selon une approche système et pour plusieurs types d'installations. Les solutions techniques de surveillance, de gestion de l'identité au moment de la délivrance de droit d'accès et de badge, de contrôle de matière à l'entrée et à la sortie des sites notamment, seraient testées dans un environnement représentatif en cohérence avec les moyens humains. Ces solutions bénéficieront en retour de cette évaluation technico-opérationnelle afin d'améliorer leurs performances.
- développer des briques technologiques adaptées aux besoins des opérateurs au moyen de projets de R&D collaboratifs comme la détection d'armes et d'explosifs aux entrées / sorties, la détection de matières dangereuses, des nouveaux capteurs ou systèmes intelligents pour la surveillance de sites pour s'assurer de la présence des personnes dans des zones autorisées, émettre des alertes et en assurer le suivi le cas échéant, de logiciels d'aide à la conception de protection de sites pour les directions de sécurité, de logiciel d'hypervision de la sécurité de sites complexes comprenant éventuellement des sites distants isolés, des outils pour faire converger la sécurité numérique et la sécurité physique des sites.

Axe 5 – Démonstrateur Cybersécurité des systèmes industriels

Les Systèmes Industriels présents dans les infrastructures critiques et les usines de fabrication, ont adopté massivement les nouvelles technologies de l'information pour former désormais des réseaux industriels hyper-connectés. La protection numérique de ces systèmes est désormais un enjeu vital de sécurité.

Il est attendu des propositions de démonstrateur CoFIS proposant des solutions innovantes de cyber-sécurité des systèmes industriels.

Les points suivants sont notamment à prendre en compte :

- le recensement et la connaissance des attaques possibles et des vulnérabilités actuelles ;

- la compatibilité avec la réglementation nationale de l'ANSSI concernant les OIV et avec les réglementations des marchés visés ;
- la compatibilité des solutions à la fois avec de nouvelles installations et avec des installations industrielles déjà existantes destinées à fonctionner encore pendant plusieurs années ;
- la prévention vis-à-vis des attaques et l'analyse de la résilience aux attaques ;
- la capacité d'intégrer la cyber-sécurité dans les automates industriels, depuis la prévention, la détection, jusqu'à la réponse à incident ;
- l'adaptation des outils de cybersécurité IT au domaine des systèmes industriels ;
- la capacité de simuler et de tester en situation les outils développés ;
- la capacité à détecter les signaux faibles précurseurs d'attaques ;
- la standardisation et la certification des solutions proposées ;
- la prise en compte des aspects humains et opérateurs dans les solutions développées ;
- la capacité à intégrer la dimension cyber aux outils de supervision de production ;
- la formation des personnels impliqués ;
- la cohérence avec les travaux déjà engagés, notamment autour de la plate-forme Chess de l'IRT SystemX.

Axe 6 – Briques technologiques pour la sécurité maritime

Riche de ses nombreux territoires ultra-marins, la France dispose de la deuxième zone économique exclusive du monde. 90% de ses flux commerciaux passent par les mers. Elle dispose d'armateurs puissants et d'une industrie de construction navale civile performante. Elle doit donc apporter une attention particulière à la sûreté maritime dont les axes majeurs ont été rappelés en octobre 2015 dans la Stratégie de sûreté des espaces maritimes.

Les principales menaces qui pèsent aujourd'hui sur la sécurité – au sens lutte contre les différentes formes de malveillance - du domaine maritime concernent :

- la piraterie ou le terrorisme qui, animés par la recherche du gain, se manifestent sous la forme de brigandage, de violence, de prise d'otage, qui peuvent être des prises d'otages massives, ou de demande de rançon ;
- le terrorisme visant à la prise de contrôle ou à la destruction d'un navire pouvant transporter des matières dangereuse que ce soit par arme, explosifs ou collision ;
- les cyberattaques qui conduisent à la prise de contrôle de navires, la perturbation de la navigation ou la récupération de données ;
- le développement des trafics, notamment ceux liés aux stupéfiants, aux médicaments, à l'alcool, aux cigarettes, aux migrants, aux armes ou aux vestiges archéologiques ;
- les pillages des ressources minérales et biologiques maritimes ;

Pour répondre efficacement à ces menaces, plusieurs besoins doivent être satisfaits au travers de développement de briques technologiques qui pourront permettre de :

- assurer une surveillance optimisée des espaces maritimes (par les airs, la terre et les mers) ;
- accroître la détection des navires, des objets, des comportements suspects à terre et en mer ;
- améliorer les contrôles des passagers, des équipages et des marchandises ;

- protéger et pouvoir intervenir face aux intrusions, à l'emploi d'engins explosifs et à l'usage malveillant de drones ;
- renforcer la cybersécurité du milieu maritime ;
- contrôler la traçabilité et la localisation des marchandises et des conteneurs.

Axe 7 – Briques technologiques pour les outils de Big data de sécurité

Les technologies Big Data sont ou seront utilisées par de nombreux acteurs de sécurité qu'ils soient publics ou privés. Ces techniques d'analyse des données (analyse dite « prédictive », observation en temps réel…) apportent des éléments de réponse aux différentes dimensions de l'action des administrations et des forces de l'ordre mais aussi des acteurs privés dont des industriels de sécurité.

Ainsi, certains acteurs font déjà un usage professionnel de ces « mégadonnées ». L'historique des incendies rend possible par exemple l'identification des sérialités de mises à feu. Les statistiques des crimes et délits passés permettent d'évaluer les risques de récidives en un lieu et à un moment donné. Il en va de même pour la cybersécurité. L'analyse des logs ou des journaux d'événements des équipements des réseaux permettent de détecter des fuites de données ou des attaques de type APT. Le Big Data permet également d'optimiser les ressources humaines, matérielles et financières, ce qui constitue un enjeu majeur dans un contexte persistant de maîtrise de la dépense publique et des coûts.

Les domaines suivants sont des utilisateurs potentiels de ces technologies pour remplir de manière plus efficace et plus performante leur mission :

- lutte contre la fraude et respect de la conformité pour déceler les écarts ou les tentatives de contournement des règles ;
- centre d'hypervision, centre d'opération de cyber sécurité (SOC), centres de supervision urbaine (CSU) et centre d'information et de commandement (CIC) : le traitement des sources d'information de natures différentes (alerte électronique, appels téléphoniques et communications électroniques, réseau radio, vidéo, journaux d'événement, main courante, logs, données de géolocalisation,…) permet d'établir des cartes de situation, de traiter et filtrer des alertes et de gérer des crises et les moyens associés voire d'anticiper les événements redoutés ;
- investigation, intelligence économique ou renseignement, ces métiers nécessitent de traiter de nombreuses sources de données et d'information différentes et de les croiser pour créer des informations intelligibles et aussi pour la mise en évidence de signaux faibles tout en respectant le cloisonnement des sources et l'anonymisation totale ou partielle des données.

Au centre du sujet des Big Data, se trouve naturellement la question de la donnée. Plusieurs points d'attention sont à souligner sur ce sujet:

- l'origine de la donnée est très variée. Elle est issue de dispositifs - personnels, privés ou publics - qui sont d'une grande diversité. Le développement de l'internet des objets accroît encore les canaux d'enregistrement et de stockage ;
- la « Véracité » des données est cruciale. Il importe de disposer d'informations parfaitement robustes et qualifiées pour pouvoir espérer les exploiter avec profit ;
- la conservation des données est essentielle. Il s'agit non seulement de savoir qui est le dépositaire de quelles données mais aussi pour combien de temps et sous quelles conditions. Un encadrement réglementaire ou contractuel est parfois nécessaire ;
- la construction de profil individualisé est possible. Les informations fournies sur internet et les réseaux y contribuent.

Un encadrement juridique adapté à cette nouvelle utilisation des données est à construire. La loi « Informatique et Libertés » du 6 janvier 1978 reste la référence actuelle en la matière. Elle précise les conditions dans lesquelles des données personnelles peuvent être sauvegardées par les opérateurs quels qu'ils soient, les conditions de transmission de ces informations à des tiers et les conditions de croisements de ces informations. Cependant, la loi du 24 juillet 2015 relative au renseignement permet, pour certains usages, d'aller plus loin dans la collecte et l'exploitation des données dans l'objectif de lutter contre le terrorisme. Les développements des briques technologiques doivent permettre de respecter ces contraintes juridiques.

Au-delà de la question des données, le Big Data pose un certain nombre de problèmes technologiques suivant les cas d'usage à traiter.

L'approche Big Data impose de changer de paradigme sur le traitement des données. Il s'agit de passer d'une approche déterministe (une cause produit un effet) à une approche probabiliste (un ensemble de causes produira probablement un effet donné). Ce mode de raisonnement conduit à approfondir les méthodes de *data mining*, de *machine learning*, de *deep learning* et d'une manière générale d'intelligence artificielle. Le développement de briques technologiques en ces manières méritera une association forte des métiers.

Pour le domaine des Big Data de la sécurité dont les usages sont multiples, tant pour les acteurs publics que privés, des développements sont nécessaires pour l'analyse et la visualisation des données. De tels développement doivent permettre, éventuellement dans le strict respect de l'anonymisation des données et du cloisonnement des sources, le traitement de données de nature très différentes (texte, image, voix, vidéo, base de données structurées ou non,…) et éventuellement dans des langues différentes. La visualisation des résultats pour permettre à un utilisateur de prendre ou faire prendre une décision dans des délais contraints est essentielle. Suivant les cas d'usage, il peut d'agir de cartes, de diagrammes de flux, de réseau de relation, de tableau de bord.

Les projets doivent porter sur ces outils d'analyse, de traitement des données et de leur visualisation dans l'environnement juridique et opérationnel du cas d'usage considéré. Ils ne concernent pas les capteurs.

Une cohérence avec les travaux déjà engagés, notamment autour de la plate-forme Chess de l'IRT SystemX, devra être recherchée.