ceis

Les objets connectés et la Défense

Par le G[al](2S) Christian Cosquer et Julie Lanckriet

Décembre 2015

Les notes σtratégiques

ceis

Les notes stratégiques

Policy Papers – Research Papers

Les auteurs souhaitent remercier l'ensemble des experts rencontrés au cours de cette étude.

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de CEIS ou des experts rencontrés.

CEIS est une société de conseil en stratégie.

Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action.

L'activité Défense et Sécurité de CEIS regroupe les expertises sectorielles et activités de CEIS dans ce domaine. La vingtaine de consultants et d'analystes du secteur Défense et Sécurité disposent d'un réseau international de plusieurs centaines d'experts et d'organisations.

Implanté à Bruxelles, le Bureau Européen de CEIS conseille et assiste les acteurs publics, européens ou nationaux, ainsi que les acteurs privés dans l'élaboration de leur stratégie européenne, notamment sur les problématiques de défense, sécurité, transport, énergie et affaires maritimes. CEIS - Bureau Européen participe également à des projets de recherche européens dans ces domaines. Pour mener à bien l'ensemble de ses missions, l'équipe s'appuie sur un réseau européen de contacts, d'experts et de partenaires.

Le SIA Lab est mis en œuvre et animé par CEIS qui agit sous la responsabilité de l'Architecte Intégrateur du SIA (Système d'information des Armées), la société SOPRA

Group. Ce concept innovant de la Direction Générale de l'Armement a pour objectif de détecter, expérimenter, et démontrer des briques technologiques sur étagère ou susceptibles d'être fournies par des PME/PMI innovantes ou des industriels.

Le SIA Lab vise à rapprocher les utilisateurs et concepteurs du Système d'Information des Armées (SIA) des potentiels fournisseurs de solutions, qu'ils soient industriels ou étatiques. C'est également un espace de réflexion et de discussion visant à cerner au mieux les besoins des utilisateurs et l'adéquation des solutions présentées.

Contact : CEIS
Défense & Sécurité
Axel Dyèvre – Directeur
adyevre@ceis.eu

Défense & Sécurité	***Bureau Européen***	***SIA Lab***
280, boulevard Saint Germain	Boulevard Charlemagne, 42	40, rue d'Oradour-sur-Glâne
F-75007 Paris	B-1000 Bruxelles	F-75015 Paris
+33 1 45 55 00 20	+32 2 646 70 43	+33 1 84 17 82 77

www.ceis.eu www.sia-lab.fr

Sopra Steria

+ 35 000
collaborateurs
-
3,4 Mds€
CA 2014
-
+ 20 pays
en Europe et dans le monde
-
+ 45 ans d'expertise
-
Des secteurs ciblés
Aéronautique & Spatial - Assurance, Santé, Social - Banque - Défense & Sécurité - Distribution - Énergie - Secteur Public - Télécoms & Médias - Transport

Sopra Steria, leader européen de la transformation numérique, propose l'un des portefeuilles d'offres les plus complets du marché : conseil, intégration de systèmes, édition de solutions métiers et Business Process Services. Il apporte ainsi une réponse globale aux enjeux de développement et de compétitivité des grandes entreprises et organisations.

Combinant innovation et valeur ajoutée dans les solutions apportées, ainsi que performance des services délivrés, Sopra Steria accompagne ses clients dans leurs programmes de transformation, aussi complexes soient-ils, et les aide à faire le meilleur usage du numérique.

Réussir la transformation. Ensemble.

Delivering Transformation. Together.

sopra steria

Une offre globale

Grâce à une chaîne continue de valeur ajoutée, Sopra Steria apporte une réponse globale aux enjeux métier des clients et les accompagne tout au long de leur transformation : compréhension stratégique, cadrage des programmes de transformation, conception et construction des solutions avec leur mise en œuvre, leur évolution et leur maintien en conditions opérationnelles.

Proche de ses clients, le Groupe garantit la pertinence continuelle de ses offres innovantes en adéquation aux vrais enjeux stratégiques.

Conseil

L'activité conseil de Sopra Steria Consulting s'étend du conseil en management au conseil en technologie. Les consultants interviennent au plan stratégique, puis conçoivent et mettent en œuvre des programmes de transformation, en France et en Europe, en tirant profit de la révolution digitale en cours.

Intégration de systèmes

Nos experts adressent l'ensemble du cycle de vie du patrimoine applicatif à travers des prestations d'intégration de systèmes et de gestion des applications allant de l'Application Management à l'Infrastructure Management. Ils s'appuient sur une solide politique industrielle afin de construire, maintenir et moderniser le système d'information en réponse à de profondes transformations d'entreprise.

Edition de solutions métier

Sopra Steria est un éditeur de solutions métier reconnu par les cabinets tels que Gartner et Forrester. Le Groupe offre des solutions leaders dans trois domaines : les services financiers (filiale Sopra Banking Software), les ressources humaines (filiale Sopra HR Software) et l'immobilier, fruits de plus de 40 ans de savoir-faire sur ces secteurs.

Business Process Services (BPS)

Sopra Steria possède une expertise unique en BPS et services partagés qui lui permet de concevoir des solutions alliant performance et rentabilité. Les clients peuvent ainsi lui confier l'externalisation des fonctions Finance, Comptabilité, Ressources Humaines et Achats.

L'innovation et la maîtrise des technologies

Sopra Steria vise en permanence à offrir le meilleur des technologies et est organisé pour détecter les innovations qui apporteront de la valeur aux métiers et aux SI de ses clients.

Sopra Steria bénéficie d'une expertise reconnue aussi bien dans le domaine des architectures IT que sur d'autres thèmes tels le big data, le cloud, les réseaux collaboratifs, la mobilité ou encore la cybersécurité.

Une solide démarche industrielle

Dans un contexte de globalisation et de maîtrise des coûts, Sopra Steria met en oeuvre une solide démarche industrielle pour servir ses clients : le Global Delivery Model. Grâce à des processus et méthodes de production industrialisés, alliés à un dispositif de centres de services mutualisés en France, en Espagne, en Pologne et en Inde, cette démarche assure la réussite de programmes de plus en plus complexes, dans le respect des délais et des coûts.

Projets emblématiques

-

AIRBUS GROUP

Manager de nombreux bundles en France, Allemagne, Royaume-Uni et Espagne pour Airbus Group

CRÉDIT AGRICOLE CONSUMER FINANCE

Accompagner la transformation de la relation client avec la refonte des centres de contacts consommateurs

Transformer les activités de support des administrations centrales et des agences nationales britanniques

EDF

Participer à la création et construction du nouveau SI de la branche Commerce

MINISTÈRE DES FINANCES

Construire la solution qui permettra de gérer plus de 100 millions de factures par an

MINISTÈRE DE LA DÉFENSE

Programme SIA – réaliser l'architecture et l'intégration du Système d'Information des Armées

SNCF

Refondre tout le système de production des horaires des trains

Sopra Steria
Direction de Communication Groupe
contact-corp@soprasteria.com

www.soprasteria.com

SOMMAIRE

Synthèse

L'utilisation d'objets connectés à des fins opérationnelles n'est pas nouvelle au sein de la Défense. Les plateformes de combat deviennent de plus en plus connectées, et il n'est déjà plus question de systèmes d'armes mais de systèmes de systèmes. Mais les contraintes qui pesaient sur les systèmes tactiques, notamment les limitations de débit et les règles de protection du secret, n'ont pas encore permis l'exploitation de toutes les potentialités offertes par cette évolution.

Les technologies innovantes qui apparaissent avec l'Internet des Objets pourraient permettre d'augmenter de façon exponentielle le nombre d'objets connectés sur les théâtres d'opération. Ces objets en recueillant passivement et activement l'information à des fins diverses peuvent constituer un point d'inflexion dans la conduite des opérations.

Le terme « Internet des Objets » (« *Internet of Things* » ou simplement *IoT* en anglais et *IdO* dans cette note) a succédé à celui de « *Machine to Machine* » (ou *M2M*[1]) pour désigner un marché en pleine croissance, qui promet de connecter à internet

[1] Le M2M se différencie en réalité de l'IoT, en tant qu'il recouvre la communication des machines entre elles (qui peut être distincte d'Internet telle que la communication par carte SIM, celle des relevés de compteurs automatisés etc..), quand l'Internet des Objets est l'arrivée d'Internet et de ses fonctionnalités dans le monde des objets.

vos objets du quotidien. Qu'y a t'il au delà des expressions médiatiques ? L'innovation technologique – des capteurs communicants peu couteux et peu gourmands en énergie - a été connue du grand public grâce aux « *wearables* » : montre, semelle ou encore lunettes connectées. Cependant, les perspectives du secteur sont bien plus vastes et s'étendent aux véhicules, aux habitations et plus généralement à la santé, l'agriculture ou l'énergie. Ces termes en vogue sont donc, en réalité, au cœur d'une nouvelle évolution numérique. En 2020, les estimations les plus basses montrent que le nombre d'objets connectés devrait être multiplié par 5 par rapport à 2015 et dépasser les 25 milliards.

Cette évolution (ou révolution) est rendue possible car le maillon principal de la chaîne (à savoir les réseaux de communication) devient opérationnel. Les réseaux et les technologies radios associées (réseau SIGFOX, protocole LORA, les technologies Bluetooth 4.0 ou DASH7,…) offrent aujourd'hui une réponse très efficace et fiable aux besoins spécifiques de communication des objets connectés grâce à un remarquable compromis débit/portée et avec d'excellentes performances de gestion d'énergie. L'émergence d'opérateurs et de réseaux facilite ainsi la mise en œuvre et le déploiement de solutions adaptées à différents services.

S'ils sont, dans un premier temps, perçus comme appartenant au domaine du bien-être et du loisir (bracelet connecté, santé connectée, jardin connecté pour l'arrosage, box pour la maitrise énergétique, détecteur de fumée, capteurs de polluants et même vêtements connectés, …), les objets connectés recouvrent pourtant une multitude de techniques, d'utilisations et de services possibles. La multiplication des capteurs entraîne une « numérisation du réel » : un monde numérique se créé, qui se superpose de plus en plus parfaitement au monde réel et engendre une quantité toujours plus grande de données qui analysent nos vies quotidiennes. L'Internet des Objets contribuerait ainsi à doubler la taille de l'univers numérique tous les deux ans, lequel pourrait représenter 44 000 milliards de gigaoctets en 2020, soit 10 fois plus qu'en 2013.

La France, dans cette nouvelle ère numérique qui commence, dispose de nombreux atouts. Premier pays européen représenté au *Consumer Electronics Show* de Las Vegas, le sommet de référence en matière de nouvelles technologies, la France et ses start-up connectées y font aujourd'hui autorité (SEN.SE, OPTINVENT ou encore WITHINGS ont été primées dès 2014). Aspect intéressant, les régions ne sont pas en reste : la cité de l'objet connecté a pris ses quartiers à Angers, tandis que l'IoT Valley de Toulouse lance son « *Connected Camp* », un accélérateur de start-up exclusivement axé sur les objets

connectés. L'émergence de plusieurs opérateurs de niveau international (SIGFOX, BOUYGUES, …) est, plus encore, signe du dynamisme du marché.

Sur le plan public comme privé, de nombreuses initiatives ont vu le jour en deux ans à peine : plan « objets connectés » en juin 2014 ; émulation entre grands groupes et jeunes pousses au sein de pôles de compétitivité ; implication du gouvernement dans la coordination des systèmes d'information de l'État et dans la réflexion sur l'accès au financement des startups, ….

Atout majeur dans la bataille de la visibilité, la promotion du label *FrenchTech* est soutenue par les différents acteurs publics nationaux (investissements d'UBIFRANCE, de BPI France,..), il est implanté dans les régions et surtout, tourné vers l'international. L'IdO a par ailleurs été classé comme principale priorité de la transformation numérique de l'économie européenne, à l'occasion du sommet numérique franco-allemand qui s'est tenu à Paris le 27 octobre 2015.

Les objets connectés, une étape dans la révolution numérique...

Une étape dans la révolution numérique

Le réseau Internet a évolué par étapes successives. Réseau technique de communication à ses débuts pour le milieu universitaire et industriel, il a évolué dés les années 1990 vers un usage public. Le début des années 2000 a vu l'émergence des réseaux sociaux et de l'e-commerce. La prochaine évolution sera celle de l'Internet des Objets et de ce qui est désigné sous le terme M2M (*machine to machine*). Le réseau Internet ne sera plus uniquement un vecteur de communication entre des individus et des machines, mais entre des machines autonomes et de plus en plus intelligentes.

Le prochain saut technologique, prévu entre 2020 et 2025, sera la généralisation des réseaux mobiles de cinquième génération (5G) qui décupleront les débits par rapport aux réseaux 4G LTE[2] actuels et optimiseront davantage l'énergie, donnant à ces objets connectés une plus grande autonomie.

[2] Le réseau 4G est l'évolution du réseau mobile de 3ème génération. Il est basé sur la norme LTE-Advanced (Long Term Evolution-Advanced).

Mais, dés à présent, de nouveaux réseaux cellulaires dédiés aux objets connectés permettent à très court terme une utilisation très satisfaisante. Ces réseaux, bas débit, sont par leur technologie spécifique mieux adaptés et moins chers que les réseaux mobiles en service. Ils utilisent la technologie radio UNB (*Ultra Narrow Band*) pour connecter des périphériques à un réseau d'infrastructure fixe. L'utilisation de l'UNB est essentielle à la fourniture d'un réseau de haute capacité, évolutif et à très faible consommation énergétique, tout en conservant une infrastructure cellulaire simple.

Ces réseaux fonctionnent dans la bande de fréquences 868 MHz qui est une bande ISM[3]. En matière de propagation, plus on monte en fréquence plus on peut transmettre de données; inversement, plus la fréquence est faible et plus il est facile d'aller loin et de transpercer la matière. Cette bande de fréquences a donc l'avantage de traverser la matière (usage urbain) et d'avoir besoin de peu de puissance (batterie minime). En revanche, elle est limitée en terme de débit (quelques Ko/s). Mais cet inconvénient n'est pas rédhibitoire compte tenu des informations à transmettre (objet ouvert/fermé, position géographique, …) qui ne nécessitent qu'un faible débit.

[3] Les bandes ISM (industriel, scientifique et médical) sont des bandes de fréquences qui peuvent être utilisées dans un espace réduit pour des applications industrielles, scientifiques, médicales, domestiques ou similaires.

L'Internet des Objets, compte tenu des marchés potentiels promis pour la prochaine décennie, connaît déjà une âpre compétition entre les opérateurs fraichement établis tels que SIGFOX et LORA, et les nouveaux venus du marchés que sont QOWISIO, ACTILITY ou KERLINK. Quelles sont leurs caractéristiques et comment les différencier ?

Le réseau SIGFOX

Dès 2014, la start-up toulousaine SIGFOX éveille l'intérêt des spécialistes en recrutant Anne LAUVERGEON à la tête de son Conseil d'Administration. Mais c'est en 2015 que la société sort réellement de l'anonymat avec une levée de fonds record de 100 millions d'euros, parvenant à convaincre à la fois des industriels renommés (GDF SUEZ, SAMSUNG,..), des fonds d'investissements (ELAIA PARTNERS, INTEL CAPITAL, ..) et des opérateurs européens établis (TELEFONICA, NTT DOCOMO,..). L'expansion progressive du réseau en Europe, en Amérique du Nord et jusqu'en Afrique et au Moyen Orient depuis octobre 2015, semble conforter SIGFOX dans son statut de champion technologique des réseaux cellulaires dédiés à l'IdO. Car c'est le positionnement exclusif de la société : offrir un réseau bas débit permettant d'envoyer loin un grand nombre de petits messages. Le coût extrêmement réduit de ces envois (l'abonnement varie de 1 à 14€ par an et par objet) et leur taille limitée (un message ne peut dépasser les 12 octets), complète pleinement les

solutions de connexion haut-débit inadaptées au modèle économique des objets connectés. Néanmoins, les inconvénients de SIGFOX existent et sont de deux ordres : une technologie propriétaire et fermée ; une entreprise unique opérateur de son réseau.

La technologie LoRa

Lancée en avril 2015 par des géants du marché des Telecom tels que CISCO ou IBM, l'Alliance LORA (*Long Range* ou longue portée) a convaincu plus de 130 membres en à peine six mois. Comme SIGFOX, sa technologie (d'origine française) repose sur l'utilisation des bandes ISM et offre donc des caractéristiques similaire de transmission : bas débit et longue portée. Néanmoins, l'Alliance LORA assure une couverture jusque dans les sous-sols, ce qui n'est pas le cas de SIGFOX. Sur le marché français, c'est BOUYGUES TELECOM qui a pris le leadership de l'Alliance, et d'autres opérateurs s'engagent dans différents pays, comme SWISSCOM pour la Suisse ou SINGTEL à Singapour. Le principal aspect différenciant de LORA réside dans son positionnement open source : tout industriel qui investit dans des capteurs compatibles LORA peut proposer une connexion certifiée par l'Alliance. Ayant fait de l'interopérabilité de ses membres un postulat de base, l'ambition du mouvement est donc de parvenir à constituer un standard unique au niveau international.

Sur le plan commercial, la technologie LORA et plus généralement les réseaux M2M incitent les opérateurs à revoir quelque peu leur modèle économique. Si le déploiement de l'Alliance LORA est encore trop récent pour proposer une tarification précise, l'avantage est qu'elle s'appuie justement sur des opérateurs historiques, disposant de leurs propres réseau : BOUYGUES TELECOM estime à quelques dizaines de milliers d'euros l'investissement nécessaire pour couvrir la France, contre plusieurs milliards d'euros pour les réseaux cellulaires.

Sigfox v.s LoRa

Quelle solution privilégier ? Les deux solutions présentent leurs propres limites. Au nombre des désavantages de SIGFOX, le fait que ses antennes fonctionnent de manière optimale quand installées sur des points hauts, peu fréquents en zone urbaine. De même, la société ne propose pas de fonction de géolocalisation à ce jour (des puces GPS seraient proposées pour 2017). À l'inverse, LORA permet de géolocaliser les objets grâce à la triangulation, grâce à une nouvelle révision des normes. Mais LORA, hormis le fait de disposer d'une couverture réseau moins étendue que celle de SIGFOX aujourd'hui, a également des désavantages. L'interopérabilité de l'Alliance est rendue possible par les modules qu'elle utilise, qui sont fabriqués par un équipementier unique : l'américain SEMTECH. Reposer sur un partenariat unique comporte toujours un risque (faillite,

imposition des prix, défaut de concurrence..), d'autant plus que le marché connaît une forte expansion. Le positionnement open source de LORA parait cependant lui promettre de meilleures perspectives, au vu de ses premiers pas très prometteur en seulement six mois.

Dans les années qui viennent, l'enjeu de la standardisation des protocoles sera crucial sur marché des objets connectés. La très grande majorité du marché étant encore à conquérir, la capacité des différents acteurs à sceller des partenariats-pays à l'échelle internationale sera déterminante. Sur ce plan, SIGFOX semble avoir une longueur d'avance, avec un plan d'action rodé (couverture de l'Europe réalisée en quelques années) et en passe de percer de nouvelles frontières (Moyen-Orient et Afrique en développement). L'évolution du modèle toulousain paraît toutefois délicate s'il persiste à rester propriétaire de sa technologie.

Pour la Défense, une utilisation mixte pourrait être envisagée ; une solution basée sur le réseau SIGFOX pour le territoire national et un réseau se basant sur la technologie LORA pour la création d'un réseau ad hoc en projection.

Des nouveaux usages

Les usages actuels et potentiels des objets connectés sont si divers que les répertorier ou procéder à une liste exhaustive présente un intérêt limité. Si tout équipement public, industriel ou individuel peut être raccordé à internet, les apports de cette bascule vers le « tout connecté » seront aussi variés que la nature initiale de ces objets. Aussi est-il plus pertinent – et plus prudent – de se concentrer sur les mutations sectorielles à même de survenir sous la montée en puissance de l'IdO.

Public : vers une gestion harmonisée des réseaux à grand échelle

L'intégration de logiciels communicants aux équipements urbains conduit à une visibilité encore plus précise que celle dont on dispose aujourd'hui sur les réseaux à grande échelle : voies de circulation (routier, ferré, aérien), éclairage, réseaux d'alimentation (eau, électricité, gaz), gestion des déchets. L'information microscopique, disponible en tout point du réseau, renseigne l'analyse macroscopique et induit une gestion harmonisée des équipements, c'est l'emblème de la Smart city. La maintenance est facilitée et se déplace du correctif vers le préventif. Les équipes de service public (sécurité, secours, ..) sont alertées par des détecteurs spécifiques (choc, fumées) au moment même de la survenance d'un sinistre. La distribution

des flux (eau, électricité, gaz) est réorganisée selon l'offre et la demande, et selon des critères géographiques et calendaires4. De même, le trafic routier est réparti selon l'affluence, et la dépense thermique est programmée (en fonction de l'ensoleillement, du voisinage,..) pour limiter les déperditions. L'ensemble de ces évolutions concourt également à réduire la pollution.

Privé: la donnée au service de « l'usine du futur »

Disposer des capteurs qui relaient des informations depuis les plans de travail, les entrepôts de stockage et l'ensemble de la chaine d'approvisionnement permet de générer du Big data, autrement dit un volume inédit de données. Analysées, ces données conduisent à une réévaluation des parcours, de l'allocation des équipements et des hommes pour atteindre l'optimisation logistique de l'entreprise. Là encore, le concept est déjà labellisé comme « l'usine du futur ». Le temps imparti à chaque cycle est réduit, les phases de validation et de tests étant réalisées directement par les objets, qui informent le poste de commande du respect des différents paramètres. Les phases de contrôle qualité, notamment, sont accélérées par cet « autocontrôle ». Sur une chaîne de valeur où interviennent de multiples acteurs, enfin, l'objet connecté renforce la sécurité

[4] Concept déjà à l'étude sous le terme de *Smart grids*

juridique relative aux questions de responsabilité, en apportant une traçabilité continue.

À l'échelle de l'utilisateur : devancer les besoins et rapprocher le service

Connecter les objets du consommateur permet là encore d'extraire la représentation d'un « comportement type ». Mais concernant l'individu, c'est l'aspect routinier qui va capter les innovations de l'IdO. L'automatisation des objets électroniques du quotidien permet de devancer le rythme de leur utilisateur : thermostat et machine à café du salon sont mis en route à la sonnerie de son réveil, l'éclairage le précède et son téléphone lui fournit les informations clés de son voyage à venir (état du trafic, plan du trajet et disponibilité du parking à l'arrivée). Un rendez-vous créé dans son agenda déclenche une réservation de train, d'hôtel et de restaurant.

Mais les consommateurs ne sont pas uniquement urbains, et l'un des atouts majeurs de l'IdO réside dans la connexion des sites et personnes isolées. Intervenir plus rapidement en cas d'urgence, soigner et faire un diagnostic à distance, c'est tout l'enjeu de la Silver economy, l'économie axée sur les seniors. Le secteur de la santé, avec des applications de suivi des paramètres biologiques ou des mécanismes simples tels le pilulier connecté, est ainsi appelé à prendre une importance majeure au sein de l'IdO. Néanmoins, l'accès à la commande et

à la surveillance de sites isolés concerne plus largement le monde rural, l'agriculture, mais également les infrastructures et sites sensibles de la Défense et des industriels (voir développements en partie 4.). Pour tout un chacun, la surveillance devient accessible, qu'elle concerne ses proches, ses objets de valeur ou sa maison.

Pour aller plus loin, il faut considérer la superposition de l'Internet des Objets à des secteurs aujourd'hui distincts, tels que la biométrie, la robotique ou l'intelligence artificielle. La biométrie permet d'envisager des pistes en terme de sécurisation des accès et de commandes des objets. La robotique, bien plus concrètement qu'actuellement, fournit toute une gamme de services d'assistance à la personne et de solutions de rationalisation industrielle. L'intelligence artificielle enfin, s'appuyant sur le Big data et l'analyse des données issues des objets, travaille à l'autonomisation du fonctionnement de ces objets. Cette dernière tendance présente des atouts pour contrer l'aspect chronophage du quotidien connecté : désengorger l'utilisateur de toutes les alertes et informations relayées par son parc d'objets. Néanmoins, la perte de contrôle qui l'accompagne rejoint les inquiétudes sécuritaires qui seront développées en partie 4.

De manière plus générale, on peut considérer l'Internet des Objets comme une technologie du savoir, qui donne à

l'utilisateur à la connaissance de l'environnement interne et externe des systèmes, équipements et personnes connectées.

Les objets connectés : un point d'inflexion pour la Défense ?

Depuis les années 1990, le développement spectaculaire dans le secteur civil des technologies de l'information et de la communication est à l'origine de nouvelles capacités d'acquisition, de circulation et de traitement de l'information. Cette généralisation de la numérisation a également contribué à la modification de l'environnement stratégique. Les développements dans le domaine technologique et, de manière concomitante, l'apparition de nouvelles menaces, ont suscité dans toutes les armées modernes des efforts de « transformation » et de « modernisation ». Ces technologies de l'information se sont également considérablement développées pour des usages civils. La technologie civile a dans ce cas précis « poussé » le besoin opérationnel. C'est le cas par exemple, des applications informatiques, comme le « chat » ou les portails collaboratifs, mais aussi dans des capacités plus importantes comme les drones ou encore l'imagerie satellite, qui sont devenus des composants essentiels de la préparation et de l'exécution de la manœuvre. Ces dernières années, ces deux technologies sont devenues facilement accessibles et représentent des marchés de plus en plus conséquents. Cette porosité entre les technologies civiles et militaires, conduit à une

acquisition de capacités par des adversaires, souvent asymétriques, dans des domaines où la supériorité des forces armées conventionnelles était jusqu'à présent incontestée.

Lors de son allocution devant l'IHEDN le 6 février 2015, le chef d'État-major des armées, le général de VILLIERS disait : « *L'avance technologique, qui dissuadait et nous donnait d'office l'ascendant, se réduit sous l'effet de capacités dites « nivellantes »* ». Les drones, l'imagerie satellite, les cyberattaques, internet aujourd'hui et les objets connectés demain sont des capacités « nivellantes », peu coûteuses et directement accessibles.

L'Internet des Objets va permettre de connecter le champ de bataille avec le monde numérique d'une manière susceptible de changer fondamentalement la conduite des opérations militaires. La capacité à relier des objets connectés de tout type, via un réseau intelligent et programmable, sera un facteur déterminant permettant d'obtenir la supériorité informationnelle de l'information.

Les réseaux de communications militaires avaient été construits dans un premier temps de manière très hiérarchique pour acheminer de la voix. Il s'agissait avant tout de raccorder des entités géographiques qui étaient peu mobiles. Ces réseaux ont ensuite été adaptés pour transporter de la donnée, mais sans

revoir leur architecture globale. Pour lever ces contraintes, l'architecture des réseaux de communication a été entièrement revue avec l'arrivée des réseaux IP (Internet Protocol). L'architecture des réseaux IP fournit des architectures distribuées, décentralisées et virtualisées, permettant de gérer la résilience, une plus grande centralisation des applications, et d'amener les infrastructures au plus près des clients finaux. Cette architecture tout IP, y compris au niveau tactique, en permettant l'échange d'informations entre tous les points du réseau, autorise une utilisation importante des objets connectés dans un usage opérationnel et rend réalisable la vision d'un champ de bataille connecté.

Le soldat individuel, la plateforme de combat, … deviennent des agents de collecte et de transmission de données vers l'échelon supérieur. Equipés de capteurs, ils deviennent une extension du réseau en permettant d'avoir accès à des données sur leur environnement réel.

Mais capacité d'anticipation, vision globale du théâtre et connexion permanente entre les acteurs ne pourront se transformer en gains opérationnels que si la compréhension commune de la situation est guidée par des processus décisionnels fluides, clairement définis et adaptables. Il s'agit donc en priorité de gérer ces objets pour obtenir, traiter, décider et diffuser les informations nécessaires aux différents

échelons sur le terrain. C'est à cette condition que l'homme restera maître de l'information, de la décision et, finalement, du rythme de l'opération.

Au-delà du champ de bataille et des théâtres d'opération à moyen et long terme, ces objets vont avoir à court terme un impact considérable dans le domaine du suivi des flux logistiques, de la maintenance et de la protection des installations.

Concernant la logistique, la possibilité de livrer la juste quantité nécessaire dans un délai imparti devrait permettre de mieux analyser, planifier et exécuter les différentes manœuvres logistiques sur des composants critiques comme les munitions, l'eau, le carburant, les pièces de rechange majeures,…

En ce qui concerne la maintenance, les capteurs et sondes que nous retrouvons sur nos véhicules civils vont se retrouver sur la prochaine de génération de véhicules militaires. Date des prochaines vidanges et visites, anomalie du moteur, état des différentes pièces, … l'informatique distribuée arrive sur toutes les plateformes.

Le lundi 29 juin 2015, le général Denis MERCIER, chef d'État-major de l'armée de l'air, a présenté le concept Smart Base sur la base aérienne 105 d'Évreux. S'inspirant du développement

des Smart Cities pour son volet technologique, le concept Smart Base consiste, entre autres, à ouvrir la base pour mieux exploiter le capital qu'elle renferme en recherchant, par le biais de l'innovation, à nouer des partenariats. Ce projet s'inscrit dans la dynamique de transformation des soutiens et des bases de défense (BdD) menée par le ministère de la Défense et pilotée par l'état-major des armées (EMA). A ce titre, il s'appuie sur les BdD pour mener l'expérimentation des projets portés par les directions et services du ministère qui concourent à l'atteinte de cet objectif et qui ont vocation à trouver application sur les bases aériennes, dans les ports militaires ou dans les régiments de l'armée de terre. Alimentation énergétique des sites, collecte des déchets, éclairage, distribution des fluides, administration et soutien du personnel, protection et sauvegarde sont des domaines dans lesquels l'Internet des Objets est un moyen de rationaliser les processus internes.

Dans la Défense, comme ailleurs, tout objet connecté fera partie d'une communauté : le véhicule dialoguera avec les autres véhicules, mais également le conducteur, le maintenancier ou le logisticien. Les plateformes joueront un rôle clef dans la structuration du secteur, car chargées non seulement de gérer ces échanges de données mais aussi de réunir les acteurs d'une communauté d'objets connectés — industriels, utilisateurs, logisticiens, etc. Elles donneront ainsi accès à des services qui

pourront être améliorés sur la base des retours des utilisateurs et des retours d'expérience.

Des enjeux sécuritaires

Sur le plan de la sécurité informatique (la cybersécurité), les objets connectés n'ont pas aujourd'hui une excellente réputation. Plusieurs raisons l'expliquent :

1) Tout d'abord, ils répondent en premier à une logique économique avec un cycle de vie qui peut être très court. Dans ce cadre, la sécurité est souvent négligée.
2) Certains objets, notamment grand public, doivent avoir un coût de fabrication extrêmement faible (de l'ordre de la dizaine d'euros) et doivent également être optimisés d'un point de vue performances et consommation énergétique. Les fonctions de sécurité, basées essentiellement sur la cryptographie, peuvent constituer un surcoût important.

A plus long terme, les objets connectés vont poser des enjeux de sécurité majeurs, qui vont s'amplifier avec leur expansion.

Le plus important est sans doute celui lié à l'utilisation des données personnelles. Un grand nombre d'informations personnelles transitera en effet sur les réseaux, d'autant plus que les objets ne solliciteront pas l'autorisation de leurs

propriétaires pour communiquer entre eux. Des informations confidentielles pourront être interceptées et exploitées comme celles relatives aux déplacements, à la santé, aux habitudes de consommation, …

Le second risque par ordre d'importance est celui des logiciels malveillants (malwares). Les objets, peu sécurisés, utilisent ou communiquent via un système d'exploitation (OS5), qui se trouvera exposé aux attaques des pirates informatiques de type DDOS6, par exemple. Une enquête récente menée par deux journalistes norvégiens a d'hors et déjà montré l'étendue des possibilités criminelles : prise de contrôle de la centrale électrique d'un immeuble, prise de possession d'imprimantes permettent de scanner un permis de conduire, ou encore l'accès à des webcams de domiciles privés placées dans des chambres d'enfants. Les objets connectés sont des ordinateurs miniatures. En tant que tels, ils sont soumis aux mêmes types de piratage et peuvent recevoir des spams7, tout comme une boite mail, et ainsi être contrôlés à distance.

[5] OS : Operating system, ensemble des programmes qui dirigent les capacités d'un ordinateur. Par exemple, Linux, Android, Windows 10 sont des OS.
[6] Une attaque DDoS vise à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.
[7] Un spam (le terme de pourriel est parfois également utilisé) désigne l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité.

Le troisième risque est celui de des utilisateurs eux-mêmes. Sous-informés sur les questions de sécurité informatique, ils ne perçoivent pas le danger et prennent des habitudes qui mettent en péril la confidentialité de leurs données personnelles (mot de passe, utilisation de clés USB, …). De plus, la multitude d'objets connectés va poser des problèmes d'échelle : il sera difficile pour chaque propriétaire de maitriser le parc d'objets sous sa responsabilité et de contrôler l'activité de ces objets.

Enfin, le dernier risque est celui de l'utilisation détournée des objets qui mettent en danger la sécurité physique. Le risque des objets à usage médical apparaît immédiatement (appareil à insuline, stimulateurs cardiaques,…) ainsi que les objets intervenants de manière croissante dans les systèmes de sécurité (serrures, systèmes d'alarmes,…).

En l'état actuel de la technologie et de l'extrême jeunesse des standards dans le domaine, la sécurité des systèmes informatiques chargés de la collecte, du traitement et des communications au cœur des objets connectés est un défi à relever. Les composants et systèmes mis en œuvre dans les objets connectés doivent être, pour un usage grand public, à la fois très peu couteux à produire et à maintenir, tout en étant particulièrement économes en consommation énergétique. Cet environnement contraint en termes de ressources (puissance de calcul, mémoire et énergie très limitées) rend inadaptées la

majorité des mesures de sécurité, communément utilisées par ailleurs dans le domaine des technologies de l'information.

Pour une utilisation dans un cadre défense, quatre défis, dont certains sont communs à certains usages publics, sont à relever. Le premier consiste à intégrer, dès la conception, des éléments de sécurité dans les composants. Le deuxième défi consiste à intervenir sur le partage d'informations. Il s'agit de donner aux objets une capacité à filtrer les demandes d'accès de manière à limiter les risques de piratage et de transmettre l'information utile au juste niveau de décision. Le troisième challenge est celui de permettre à l'ensemble des objets connectés de se transmettre mutuellement des informations de sécurité. Il s'agit de réagir le plus vite possible aux attaques identifiées avant qu'elles ne se propagent. Dans l'idéal, l'alerte doit se répandre plus vite que la menace. Enfin, le dernier défi est celui de l'éducation des utilisateurs.

*

* *

Si la technologie ne définit pas à elle seule les caractères de l'affrontement, elle en prescrit très précisément le cadre et les modalités. Une avancée technologique ne constitue pas en soi une avancée militaire. Mais la rencontre d'une possibilité

technique et d'un concept d'emploi pertinent peut être décisive. Dans le cas de l'Internet des Objets, c'est donc la rencontre de ces deux éléments, généralement d'abord technologiques (les réseaux et technologies radios accessibles qui offrent une réponse très efficace et fiable aux besoins spécifiques de communication des objets connectés grâce à un remarquable compromis débit/portée et avec d'excellentes performances de gestion d'énergie.), puis seulement ensuite militaires (qui exploitent les possibilités ouvertes par cette technologie), qui peut donner naissance à une rupture.

Ces technologies innovantes qui apparaissent avec l'Internet des Objets doivent être utilisées par la Défense afin de maîtriser l'information et d'accélérer encore le renseignement et le tempo des opérations. Ces objets en recueillant passivement et activement l'information à des fins diverses vont constituer un point d'inflexion dans la conduite des opérations.

Le SIA Lab se penche sur « la gestion multi-capteurs »

Le SIA Lab, plate-forme de co-innovation de la Défense, organise des sessions de démonstrations mensuelles visant à présenter des solutions nouvelles au personnel des Armées. Dans ce cadre, la session du mois d'octobre 2015 était consacrée au thème de « la gestion multi-capteurs ». L'un des objectifs d'une session de démonstration est de permettre à l'auditoire (représentants du ministère de la Défense issus des différents services concernés par la thématique) d'appréhender l'ensemble des usages opérationnels d'une technologie.

L'Equipe du SIA Lab a donc identifié trois segments présents sur le marché des objets connectés, en distinguant les fournisseurs de réseaux en amont, les concepteurs d'objets connectés, et enfin, en bout de chaine, les sociétés qui travaillent sur l'intelligence de la donnée.

Au terme de sélections successives en concertation avec l'EMA (État-major des armées), les sociétés SIGFOX, TRAQUEUR et INTESENS ont été conviées à présenter leurs solutions au SIA Lab le jeudi 29 octobre 2015. SIGFOX a détaillé les caractéristiques et les particularités son réseau; la société TRAQUEUR a présenté une

balise autonome qui permet de géolocaliser en temps réel tout équipement sur lequel elle est placée ; INTESENS, enfin, a illustré l'intérêt de ses capteurs sans fil pour la sécurisation des sites et la maintenance connectée.

La valeur ajoutée de ces solutions pour la Défense a été matérialisée par un scénario opérationnel simple et applicable au quotidien des armées :

« L'État-major souhaite déployer un réseau de communication sur une base opérationnelle des Armées françaises. Une fois installé un réseau de type SIGFOX, les objets sont connectés et envoient des messages. Les équipements de la base étant pourvus de balises communicantes, à l'exemple de celles de TRAQUEUR, le vol d'une caisse à munitions est rapidement déjoué après une géolocalisation en temps réel. La base renforce alors ses dispositifs de sécurisation : des capteurs de mouvements et d'intrusion tels ceux réalisés par INTESENS sont positionnés sur le périmètre extérieur de la base, et alertent le poste de contrôle en cas d'activation. «

Un tel scénario a permis de rendre immédiatement compte des potentialités de la Défense connectée, alors même que les sociétés présentées ne constituaient qu'un échantillon des solutions disponibles sur le marché français. Les participants de la session ont par ailleurs corroboré l'intérêt de l'Internet des Objets

au service de la Défense, en posant des appréciations positives sur les solutions présentées.

REFERENCES

BABINET, Gilles et VASSOYAN, Robert. *Big data et objets connectés. Faire de la France un champion de la révolution numérique*. Institut Montaigne, Rapport d'avril 2014.

Conseil National du Numérique et Beirat Junge Digitale Wirtschaft, *Communiqué de presse sur le plan d'action franco-allemand : "Agir pour l'innovation"*. Disponible sur : http://www.cnnumerique.fr/wp-content/uploads/2015/10/BJDW_CNNum_ActionPlan_Final_VF.pdf. (Consulté le 15/10/15).

France Stratégie, Note d'Analyse n°22 – *Demain, l'Internet des Objets*, 12/01/15. Disponible sur : http://www.strategie.gouv.fr/publications/demain-linternet-objets (Consulté le 20/10/15).

L'Observatoire Fives des usines du futur, *Cahier de l'Observatoire Fives des usines du futur*, 2eme édition 2014. Disponible sur **:**

http://dk8mx37zdr9bp.cloudfront.net/corporate/PublishPaper/cahier_observatoire_2/index.htm#/67 (Consulté le 04/11/15).

Ministère de la Défense DGA/DS/SASF/SDCP et Orange Consulting - *Etude sécurité Internet 2030* – Etude Prospective et Stratégique. Disponible sur : http://www.defense.gouv.fr/content/download/363921/5272321/file/EPS2013-R%C3%A9seau%20internet%20et%20s%C3%A9curit%C3%A9.pdf (Consulté le 26/10/15).

SERGÈRE Vincent. LoRa : LE futur réseau des objets connectés ? FrAndroid, 18 octobre 2015. Disponible sur : http://www.frandroid.com/telecom/313396_lora-futur-reseau-objets-connectes (Consulté le 22/10/2015).

LORA-ALLIANCE, site internet officiel, disponible sur : https://www.lora-alliance.org (Consulté le 12/11/15).

SIGFOX, site internet officiel, disponible sur : http://www.sigfox.com/fr/. (Consulté le 12/11/15).

Publications récentes

Le SIA Lab – Retour sur 2 ans d'activité – Juin 2015 – English version available

Systèmes d'information opérationnels et de communication en Europe – Mars 2015 – English version available

Les Centres de commandement et de contrôle (C2), un enjeu stratégique structurant. - Septembre 2014

Conditions d'utilisation des logiciels de l'OTAN par les Nations Alliées - Juin 2014 – English version available

Le programme SIA - Décembre 2013

Mission des Armées et systèmes d'information - Décembre 2013

PME et marchés de défense - Août 2013

R&D et PME de Défense - Août 2013

Retrouvez les Notes Stratégiques SIA Lab
et toutes les Notes Stratégiques sur le site de CEIS

http://www.ceis.eu/fr/toutes-publications

CEIS

Société Anonyme au capital de 150 510 €

SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris

Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60

ceis