



**MINISTÈRE
DE L'ÉCONOMIE
ET DES FINANCES**

**MINISTÈRE
DU REDRESSEMENT
PRODUCTIF**



**CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES**

TÉLÉDOC 792
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2012/25/CGEIET/SG

RAPPORT

Internet des objets et logistique « Vers des nets avec des objets »

Situation internationale, perspectives des acteurs et débats.

Etabli par

Jean-Pierre DARDAYROL
Ingénieur général des mines

Loïc Lenoir DE LA COCHETIÈRE
Chargé de mission

Claudine DUCHESNE
Contrôleur général économique et financier

Mars 2013

SYNTHÈSE

Paris, le 4 mars 2013

Note de synthèse et de propositions : Internet des objets et logistique.

Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET) a conduit une mission de conseil sur le recours aux technologies de l'Internet des objets dans les domaines intéressant la logistique transfrontière.

La mission s'est donc intéressée au vaste champ des fonctionnalités des systèmes d'information appliquées à la logistique transfrontière, principalement : l'intégrité, la traçabilité, l'identification ou l'authentification des produits et de leurs contenants ; le contrôle documentaire à des fins douanières ou de conformité réglementaire.

Le terme « Internet of things » – Internet des objets – est né en 1999 au MIT, où l'équipe de Kevin Ashton promeut un Internet des objets synonyme d'une connectivité ouverte de tous les objets en utilisant des étiquettes RFID, le protocole IPv6, ... Le secteur de l'aéronautique avec Boeing et celui des biens de grande consommation avec Wal-Mart s'emparent rapidement du sujet.

Autour du W3C naît alors une conception plus souple, acceptant une pluralité d'étiquettes. Dans les faits, c'est elle qui s'est imposée, même si pour beaucoup l'Internet des objets reste associé aux étiquettes RFID, à l'ONS et à IPv6, ce qui est apparu constituer un frein à son développement au cours de la mission.

Dans cette perspective, il est nécessaire de se poser trois questions :

- quelles sont les approches de l'Internet des objets pour le secteur de la logistique et la gestion des produits dans d'autres pays – pays comparables, prescripteurs ou concurrents de la France ;
- quels seront dans quelques années les caractéristiques structurantes de l'Internet des objets ? Quels invariants et quelles alternatives voient les acteurs dans les scénarios de développement ? A quel horizon temporel doit-on se projeter ?
- quels sont les points de passage clés pour s'approprier collectivement ou individuellement l'Internet des objets à moyen terme ? Pour passer à l'échelle de façon efficace et efficiente, que l'on soit une administration ou une entreprise ?

On constate que les applications des technologies de l'Internet au monde des objets ont dépassé dès à présent le stade de la preuve de concept. L'ère de la généralisation s'ouvre, avec des applications ciblées sur une entreprise, un produit, un groupe de produits ou bien encore une marque.

Les relations de machine à machine constituent un domaine pionnier mais des applications plus larges se développent comme celles visant à assurer, par exemple, la traçabilité des bouteilles de vin ou des paquets de cigarettes, la géolocalisation et la mesure de l'environnement et du contenu des containers frigorifiques, la configuration des composants d'un aéronef, l'authentification des pièces de monnaie, l'historicisation de la culture des arbres urbains, etc.

Les secteurs les plus porteurs de novations semblent être :

- le secteur hospitalier, de la santé, de la dépendance et du bien-être ;
- la ville intelligente et la gestion des flux – eau, énergie, véhicules, personnes ;
- le secteur du commerce et du marketing.

Dans ce mouvement, **les applications de l'Internet des objets peuvent répondre à des besoins de la logistique à longue distance** : notamment la vérification de l'intégrité, l'identification ou l'authentification des objets, la traçabilité et l'association de documents (contrôle réglementaire) tant des produits que des contenants.

Du point de vue de la chronologie, même si les analystes divergent sur les échéances, les communautés d'acteurs s'accordent pour considérer que **la période 2014 – 2020 sera cruciale** et connaîtra, si ce n'est la massification des applications des technologies de l'Internet des objets, du moins une extension et une généralisation de ses usages tant en termes de finalité que de catégories d'objets.

En ce qui concerne les modalités, les experts et les utilisateurs, notamment au sein des entreprises, envisagent, non pas un Internet prolongé au monde physique, vivant ou géographique, mais plutôt des applications et des systèmes s'intéressant aux objets en utilisant les technologies de l'Internet. Pour ces raisons, **il est plus exact de parler de nets avec des objets** – internets et intranets – que d'Internet des objets à proprement parler.

Dans la compétition économique et politique, les pays industriels d'Asie affirment leurs ambitions.

La Chine a mis en place de façon volontariste une politique holistique qui vise à faire de « **la Chine le pays de l'Internet des objets en 2015** ». Cette politique semble mobiliser des moyens considérables, elle est portée au plus haut niveau de l'État, favorisée par la place de ce pays en tant qu'exportateur – et importateur – d'objets de tous types.

Singapour a également mis en place une politique globale pour l'Internet des objets, associant les autorités et le secteur privé, créant des centres de ressources et développant des applications dans de nombreux domaines – ports, aéroports, environnement, transports, santé, ...

La Corée du sud et la Malaisie ont engagé des politiques qui semblent plus sectorisées et qui reposent sur des réalisations dans des secteurs à enjeux jugés immédiatement prioritaires : gestion de la ville, de l'eau et des transports, contrôle des pollutions ou des frontières, ...

L'approche aux Etats-Unis est moins médiatisée, cependant, de nombreux éléments montrent des investissements pour des réalisations concrètes et financièrement rentables. Les pouvoirs publics ne sont pas absents des réalisations - à titre d'exemple, la FCC vient de créer une direction des soins - healthcare - pour traiter le sujet de l'Internet des objets pour les soins, à domicile et à l'hôpital.

Les services de la Commission de l'Union européenne ont beaucoup communiqué sur ce sujet dans les années 2007 – 2009. Leur activité est redevenue plus réduite.

Cependant, le Royaume-Uni a défini et lancé une politique industrielle pour positionner favorablement ses entreprises et ses éco-systèmes dans la compétition mondiale autour des applications de l'Internet des objets ; la politique de coopération entre les entreprises et

d'émergence de champions de toutes tailles vise à dégager des compétences, des segments d'excellence et des effets clusters autour de réalisations concrètes. Depuis peu, le recours au « financement par la foule » - crowdfunding – est une composante de ce plan.

En Allemagne, les sources relatives à l'Internet des objets sont plus rares, mais le sujet est traité sous l'appellation des « réseaux intelligents » ou sous celle du M2M. L'angle adopté est celui de la R&D et de l'innovation.

En résumé :

- la Chine met en avant 2015 comme l'année de plénitude ; à Singapour, on parle de réalisations généralisées dans trois à cinq ans ;
- en Europe, les perspectives sont plus lointaines. Par exemple, 5 ou 7 ans paraissent des horizons plausibles de maturité pour la majorité de ceux qui ont répondu au questionnaire du CGEJET ;
- les activités intéressant la Douane sont partie prenante au développement d'applications, et de facilités mettant en œuvre l'Internet des objets ;
- la compétition à l'échelle mondiale et européenne entre les plates-formes et les territoires comportera un aspect Internet des objets pour la logistique, notamment transfrontière ;
- les pays industriels d'Asie privilégient des approches ambitieuses, holistiques avec des horizons courts.

La France a des atouts dans la compétition, encore ouverte, autour de l'Internet avec des objets :

- de nombreuses technologies innovantes dans les laboratoires et les entreprises ;
- des preuves de concept nombreuses et réussies – notamment grâce aux FUI – fonds unique d'investissement ;
- des secteurs dynamiques utilisateurs : l'aéronautique, le luxe, l'agro-alimentaire, le médicament, ... ;
- un savoir-faire en matière de systèmes complexes, d'intégration et de sécurité.

La méthode retenue dans le cadre de la mission pour **tracer les perspectives de l'Internet des objets** a été celle d'une consultation d'acteurs, selon la méthode du Delphi, complétée par des entretiens en face à face et un colloque-débat.

La restitution d'une synthèse de ces travaux a été faite lors d'un séminaire organisé dans les locaux de l'Institut Mines -Telecom le 18 octobre 2012. Ce séminaire réunissait une quarantaine d'experts invités. La restitution a été poursuivie par trois débats portant sur les trois sujets jugés les plus cruciaux par les participants à l'enquête :

- les données personnelles et la vie privée ;
- l'intelligence économique et la cybercriminalité ;
- le passage à l'échelle.

On peut retenir quatre messages consensuels des acteurs.

A - L'Internet des objets est une perspective motivante et crédible.

Récusant généralement le schéma d'un Internet global et universaliste, les acteurs consultés prévoient assez unanimement un développement rapide des Internets « avec des objets ».

B - Un mouvement de moyen-long terme est engagé pour tirer profit des potentialités des Internets des objets.

Les acteurs estiment que les Internets « avec des objets » seront largement diffusés d'ici 5 à 7 ans. Les technologies et les applications viseront d'abord les contenants pour les besoins de la chaîne logistique puis également les contenus.

Les principaux secteurs d'application seront ceux de la traçabilité, des contrôles réglementaires et de la lutte anti-contrefaçon.

Le constat partagé est que l'écosystème est disponible, de la recherche jusqu'à l'offre de services. Les technologies sont industriellement disponibles, mais le passage à l'échelle reste souvent à tester au-delà des preuves de concept abondantes.

C - La généralisation de l'Internet des objets repose sur des logiques originales, propres à chaque acteur dans un contexte aux aspects pluriels.

Le déploiement à large échelle d'applications de l'Internet des objets est devenu possible et réalisable à court-moyen terme, sous certaines conditions.

Les moteurs essentiels du développement des Internets des objets seront l'économie des entreprises (optimisation des chaînes de traitement en vue d'une réduction des coûts) et la sécurité, sous tous ses angles : de l'intégrité des contenants et des contenus jusqu'à l'anti-terrorisme. Les choix applicatifs et technologiques relèveront donc de postures pragmatiques dans des équations propres.

Les acteurs ne se projettent pas dans un système global mais dans un monde où coexisteront des pluralités de standards, de technologies, d'architectures et d'opérateurs.

De même, le cadre de mise en œuvre des applications sera très varié, du point de vue géographique (mondial, régional, national) comme du point de vue réglementaire et/ou métier (pour certains produits, pour une entreprise, pour une marque, etc.).

Deux grandes familles d'applications se distingueront :

- celles concernant la logistique, la traçabilité, l'intégrité, le contrôle réglementaire ;
- celles visant à la lutte contre la contrefaçon, et donc à la vérification de l'authenticité, *in fine* sous la maîtrise des titulaires des droits.

D - A terme, la massification des usages passe par la réponse à plusieurs défis, notamment concernant la protection de la vie privée et la cybersécurité.

Alors que cela n'était pas le cas pour l'Internet des documents, les utilisateurs sont cette fois « prévenus » ex-ante des difficultés et des risques potentiels.

La question du respect de la vie privée et de la gestion des données personnelles est considérée comme un point crucial. En effet, la question du statut des données traitées dans le cadre des Internets avec des objets pose de nombreuses questions au regard du cadre légal actuel :

- Quel est le statut de ces données au regard des dispositions « informatique et liberté » ?
- Pourra-t-on et comment mettre en œuvre un droit à l'expérimentation ?
- Qu'en sera-t-il des projets d'extension des dispositions « informatique et liberté », extension envisagée par exemple à l'adresse IP ?

- Existera-t-il des corpus de règles spécifiques (par exemple pour la technologie RFID, régimes d'autorisation ou de notification, etc.) ?

Les acteurs estiment que les orientations prises en matière de protection des données personnelles et de la vie privée auront un impact déterminant sur le développement des Internets avec des objets et donc sur les services et les processus des entreprises et des administrations.

De plus, la cybersécurité et l'intelligence économique offensive apparaissent constituer des menaces prégnantes. *Une réponse des pouvoirs publics est attendu en la matière.*

*
* *
*

Dans ces conditions et compte tenu notamment de l'existence d'un écosystème complet en France et des enseignements tirés de nombreuses preuves de concept réalisées à ce jour, il est opportun que les acteurs français s'engagent dans la coopération et la compétition internationale pour déployer des applications d'envergure.

Quatre mesures sont attendues par les acteurs et paraissent de nature à créer un environnement plus favorable aux entreprises, aux administrations et aux plates-formes françaises de logistique dans le domaine de l'Internet des objets appliqué à la logistique :

1. Mettre en œuvre un programme de recherche et de transfert relatif aux modèles d'affaires et aux conditions de succès des projets, notamment coopératifs. Ce programme pourrait s'appuyer sur les centres existants : Université du Havre, INRIA de Lille, Écoles des mines de Paris et Saint-Étienne, etc.

2. Assurer l'excellence de la France dans le domaine de la logistique internationale en déployant une gamme d'applications au profit des plates-formes aéroportuaires et portuaires ainsi que des administrations (DGDDI, DGCCRF, etc.) dans le cadre d'un plan national.

L'identification de ces applications devra se faire grâce à une mission ad hoc largement gérée par les professionnels des secteurs concernés.

3. Définir un cadre de protection des données personnelles et de la vie privée favorisant le développement compétitif des activités et des entreprises en France, par exemple sous forme d'une loi d'expérimentation ou de lignes directrices de la CNIL ;

4. Développer les compétences en matière de cybersécurité au sein des administrations compétentes – Police, Gendarmerie, ANSSI, etc. - et identifier un guichet unique de conseil et d'alerte pour les entreprises et les administrations.

SOMMAIRE

Internet des objets et logistique.....	1
« Vers des nets avec des objets ».....	1
Situation internationale, perspectives des acteurs et débats.....	1
Introduction	1
1. L’internet des Objets, Internet de la productivité.....	3
1.1 L’Internet des objets est une notion polysémique.....	3
1.2 L’histoire de l’Internet des objets se construit sans présupposés.....	4
1.3 La feuille de route des technologies et des systèmes fait apparaître des progressions et des changements structurants.....	6
1.4 L’Internet des objets peut répondre à des besoins de la logistique transfrontière ou à longue distance.....	7
2. La compétition entre l’Asie et l’Amérique marque la géopolitique de l’Internet des objets.....	8
2.1 Les pays industriels d’Asie affirment leurs ambitions.....	8
2.2 L’horizon de maturité de l’Internet des objets est perçu en Asie à plus court terme qu’en Europe.....	9
3. Les acteurs énoncent quatre messages et posent trois questions à l’horizon de 5/7 ans	11
3.1 L’internet des objets est une perspective motivante et crédible.....	12
3.2 Un mouvement de moyen-long terme est engagé pour tirer profit des potentialités des Internets des objets.....	12
3.3 La généralisation de l’Internet des objets repose sur des logiques originales, propres à chaque acteur dans un contexte aux aspects pluriels.....	12
3.4 A terme, la massification des usages passe par la réponse à plusieurs défis – non-technologiques, notamment concernant la protection de la vie privée et l’intelligence économique.....	13
4. Avis d’experts et débats autour des questions cruciales : vie privée et cybersécurité	14
4.1 La vie privée des objets	15
4.2 internet des objets : nouveau champ d’action pour la cybercriminalité.....	21
Annexe 1 : Lettre de mission.....	26
Annexe 2 : Présentation de l’Internet des objets sur le portail du Gouvernement de Singapour	27
Annexe 3 : Looking to Industry for the Next Digital Disruption, article du New-York Times, le 23 novembre 2012 – sans les photos	28
Annexe 4 : Making the Internet of Things a Reality : Mobility meets Big Data in the Cloud – “Triple Word Score”!.....	31
Annexe 5 : Questionnaire pour les attachés douaniers	33
Annexe 6 : Réponse des douanes de Singapour.....	37
Annexe 7 : Liste des organismes rencontrés ou interrogés	42
Annexe 8 : Questionnaire – Version française.....	43

Introduction

Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEJET) a conduit une mission de conseil sur le recours aux technologies de l'Internet des objets dans les domaines intéressant la logistique transfrontière.

Les technologies de l'internet sont appliquées dès aujourd'hui au monde des objets dans des conditions à la fois prometteuses quant aux gains d'efficacité ou d'efficience mais décevantes au regard des caractéristiques annoncées il y a quelques années au sujet de l'Internet des objets – absence d'interopérabilité, normes fermées, protocoles immatures ou encore peu utilisés : ONS, IPv6, ...

Le caractère polysémique du terme « Internet des objets » qui recouvre tantôt des réalisations immédiates, tantôt des utopies étant lui-même porteur de difficultés, nous lui préférons souvent le terme d'Internet avec des objets, plus modeste mais plus proche de la richesse des applications existantes ou en cours de construction et de déploiement.

La mission s'est donc intéressée au vaste champ des activités concernant la logistique transfrontière, principalement : l'intégrité, la traçabilité, l'identification ou l'authentification des produits et de leurs contenants ; le contrôle documentaire à des fins douanières ou de conformité réglementaire ...

Dans cette perspective, il est nécessaire de se poser trois questions :

- quelles sont les approches de l'Internet avec des objets pour le secteur de la logistique et la gestion des produits dans d'autres pays – pays comparables, prescripteurs ou concurrents de la France ?
- quel sera dans quelques années les caractéristiques structurantes de l'Internet (avec) des objets ? Quels invariants et quelles alternatives voient les acteurs dans les scénarios de développement ? A quel horizon doit-on se projeter ?
- quels sont les points de passage clés pour s'approprier collectivement ou individuellement l'Internet des objets à moyen terme ? Pour passer à l'échelle de façon efficace et efficiente, que l'on soit une administration ou une entreprise ?

Après une première partie consacrée à la présentation de l'Internet des objets - **l'internet des Objets, Internet de la productivité**, le sujet est donc abordé sous trois angles : la compétition internationale, les perspectives des acteurs, l'approfondissement des questions jugées cruciales.

Les éléments de situation internationale s'appuie sur une revue documentaire et sur l'exploitation d'une consultation conduite par les attachés douaniers dans une sélection de pays (notamment Etats-Unis, Royaume-Uni, Allemagne, Suède, Italie, Pays-Bas, Dubaï, Singapour, Australie et Chine). Elle se fonde sur un questionnaire établi par la mission.

Le contexte est marqué par la compétition entre l'Asie de l'est et les Etats-Unis, les ambitions et les réalisations de la Chine, portées au plus haut niveau politique.

La description à dire d'experts des **perspective des acteurs à l'horizon de 5/7 ans, invariants et alternatives** identifie ou rappelle les points de consensus et les divergences constatées dans la vision des organisations, des centres de recherche et des entreprises

actrices des secteurs de la logistique ou au profit de celui-ci, à partir d'une méthode de prospective auprès des acteurs institutionnels, experts et chercheurs, opérateurs de technologies, utilisateurs, etc.

Les acteurs, choisis dans l'ensemble de l'éco-système, des centres de recherche aux assureurs ont délivré **quatre messages** :

- L'Internet des objets est une perspective motivante et crédible ;
- Un mouvement de moyen-long terme est engagé pour tirer profit des potentialités des Internets des objets ;
- La généralisation de l'Internet des objets repose sur des logiques originales, propres à chaque acteur dans un contexte aux aspects pluriels ;
- A terme, la massification des usages passe par la réponse à plusieurs défis – non-technologiques, notamment concernant la protection de la vie privée et l'intelligence économique.

Un approfondissement des débats a été mené avec des experts et en dialogue avec les acteurs autour des trois questions jugées les plus prégnantes par ces mêmes acteurs.

Deux questions sont apparues comme cruciales :

- la question des données personnelles et de la vie privée ;
- la cyber sécurité.

1. L'Internet des Objets, Internet de la productivité

1.1 L'Internet des objets est une notion polysémique

L'encyclopédie Wikipédia donne une définition simple et communément admise de l'Internet des objets ; elle est reprise ci-dessous. Le site spécialisé sur l'Internet des objets du portail du Gouvernement de Singapour en donne une vision synthétique et contextualisée, on la trouvera en annexe 2.

L'Internet des objets¹ représente l'extension d'Internet à des choses et à des lieux dans le monde physique. Alors qu'Internet ne se prolonge habituellement pas au-delà du monde électronique, l'internet des objets (IdO) a pour but de l'étendre au monde réel en associant des étiquettes munies de codes, de puces RFID ou d'URLs aux objets ou aux lieux.

Il n'existe pas de définition standard et partagée de l'IdO.

Certaines définitions insistent sur les aspects techniques de l'IdO (« des objets ayant des identités et des personnalités virtuelles, opérant dans des espaces intelligents et utilisant des interfaces intelligentes pour se connecter et communiquer au sein de contextes d'usages variés ») , d'autres portent sur les usages et les fonctionnalités (« la convergence des identifiants numériques » notant qu'il devient possible d'identifier de manière unifiée des éléments d'information numérique (adresses) et des éléments physiques (une palette dans un entrepôt, ou un animal dans un troupeau).

Il est parfois suggéré que l'objet deviendra un acteur autonome de l'Internet, c'est-à-dire capable de percevoir, analyser et agir par lui-même dans les contextes des processus dans lesquels il sera engagé.

L'IdO n'est pas une technologie mais un système de systèmes. L'interopérabilité entre ces systèmes et l'intégration de tous les composants induisent une complexité forte. La capacité à gérer les interfaces est donc déterminante.

Lier un objet ou un lieu à Internet est un processus plus complexe que la liaison de deux pages Web. L'Internet des objets exige sept composants :

- 1. Une étiquette physique ou virtuelle pour identifier les objets et les lieux. Quelques systèmes d'étiquetage sont décrits ci-dessous. Pour permettre aux étiquettes physiques plus petites d'être localisées, elles doivent être embarquées dans des marqueurs visuels.*
- 2. Un moyen de lire les étiquettes physiques, ou de localiser les étiquettes virtuelles.*
- 3. Un dispositif mobile tel qu'un téléphone cellulaire, un organizer ou un ordinateur portable.*
- 4. Un logiciel additionnel pour le dispositif mobile.*

¹ Source : wikipédia, article Internet des objets, accédé le 21 novembre 2012.

5. *Un réseau sans fil de type 2G ou 3G afin de permettre la communication entre le dispositif portable et le serveur contenant l'information liée à l'objet étiqueté.*
6. *L'information sur chaque objet lié. Cette information peut être contenue dans les pages existantes de WWW, les bases de données comportant des informations de type prix, etc.*
7. *Un affichage pour regarder l'information sur l'objet lié. À l'heure actuelle, il est des plus probables que ce soit l'écran d'un téléphone mobile.*

4.2 L'histoire de l'Internet des objets se construit sans présupposés

Le terme « Internet of things » – Internet des objets – est né en 1999 au MIT, où l'équipe de Kevin Ashton promeut une connectivité ouverte de tous les objets en utilisant des étiquettes RFID, le protocole IPv6, ... Le secteur de l'aéronautique avec Boeing et celui des biens de grande consommation avec Wal-Mart s'emparent rapidement du sujet.

Autour du W3C naît une conception plus souple, acceptant une pluralité d'étiquettes. Dans les faits, c'est elle qui s'est imposée, même si pour beaucoup l'Internet des objets reste associé aux étiquettes RFID, à l'ONS et à IPv6, ce qui est apparu constituer un frein à son développement au cours de la mission.

Cette notion a connu une phase de popularité en Europe en 2007/2008. On envisageait alors avec optimisme la mise en place d'un Internet des objets global, ubiquitaire et ouvert, à l'instar de l'Internet gouverné par l'ICANN. A cette vision quelque peu idéaliste a succédé une approche moins intégrée de gestion par projets dans des domaines de plus en plus variés.

Les applications des technologies de l'Internet au monde des objets ont ainsi dépassé aujourd'hui le stade de la preuve de concept. L'ère de la généralisation s'ouvre, avec des applications ciblées sur une entreprise, un produit, un groupe de produits ou bien encore une marque. Les relations de machine à machine constituent un domaine pionnier mais des applications plus larges se développent comme celles visant à assurer, par exemple, la traçabilité des bouteilles de vin.

Le déploiement d'applications amples est favorisé par les performances et le faible coût, d'une part des technologies d'échanges d'information issues de l'internet ainsi que celles d'accès rapide aux informations de masse – infonuagique et *big data* – et, d'autre part des technologies optiques. Les technologies disponibles seront donc multiples, y compris pour l'identification des objets, l'objet pouvant porter lui-même son identification.

Même si les analystes divergent sur les échéances, les communautés d'acteurs s'accordent pour considérer que la période 2014 – 2020 connaîtra, si ce n'est la massification des applications des technologies de l'Internet des objets, du moins une extension et une généralisation de ses usages tant en termes de finalité que de catégories d'objets.

Les experts et les utilisateurs, notamment au sein des entreprises, envisagent, non pas un Internet prolongé au monde physique et géographique, mais plutôt des applications et des systèmes s'intéressant aux objets en utilisant les technologies de l'Internet.

Leurs degrés d'ouverture et d'interopérabilité seront choisis au cas par cas en fonction :

- du contexte – notamment économique, juridique et de sécurité ;
- du besoin – intégrité, lutte contre le vol, contrôle documentaire, lutte anti-contrefaçon,... ;
- des objets concernés – alimentation, produits de luxe, médicaments, ... ;
- des contraintes réglementaires.

Pour ces raisons, il est plus exact de parler, à ce stade, de **nets avec des objets** – internets et intranets – que d'Internet des objets à proprement parler.

Il n'y a pas que la pluralité des technologies, la capacité à maîtriser l'ouverture et l'interopérabilité des applications qui distingueront le domaine qualifié d'internet avec des objets de l'Internet, il y a aussi la géopolitique. Les pays d'Asie – et les Etats-Unis – sont engagés dans une compétition ambitieuse pour être les acteurs clés de cette révolution – cf. *infra*.

On trouvera dans un article récent du New-York Times une vision de l'approche d'un grand industriel polyvalent : GE – General Electric, intéressante par son ubiquité et son volontarisme : <http://www.nytimes.com/2012/11/24/technology/internet/ge-looks-to-industry-for-the-next-digital-disruption.html> - accédé le 26 novembre 2012.

L'article est reproduit en annexe 3.

L'article de Sanjay Poonen, directeur de la mobilité et de l'innovation chez SAP, daté du 1^{er} octobre 2012, donne une bonne vision d'une approche centrée sur le prolongement de l'existant, par l'amplification de la mobilité en commençant par les applications de machine à machine – M2M : [Making the Internet of Things a Reality : Mobility meets Big Data in the Cloud – "Triple Word Score"!](#) Il est en annexe 4.

Cette approche est répandue en Europe, notamment en Allemagne ; elle est aussi souvent celle des opérateurs de communications électroniques.

Les articles suivants donnent une bonne présentation de l'intérêt sectoriel de l'Internet des objets :

- **le secteur hospitalier et de la santé** : Tam Harbert. FCC Gives Medical Body Area Networks Clean Bill of Health : <http://spectrum.ieee.org/tech-talk/biomedical/devices/fcc-gives-medical-body-area-networks-clean-bill-of-health> ;

- **le secteur de la distribution et de la consommation d'énergie** : Korea Smart Grid Institute. Korea's Jeju Smart Grid Test-bed Overview : <http://www.smartgrid.or.kr/10eng3-1.php>

- **le secteur du commerce et du marketing** :

Rsasirekha. Gartner's IT Top Predictions for 2011

<http://itknowledgeexchange.techtarget.com/enterprise-IT-tech-trends/gartners-it-top-predictions-for-2011>

Retail Pro. Gartner: Context-aware technology to change consumer spending
<http://www.retailpro.com/community/blog/index.php/2011/10/31/gartner-context-aware-technology-to-change-consumer-spending>

1.3 La feuille de route des technologies et des systèmes fait apparaître des progressions et des changements structurants

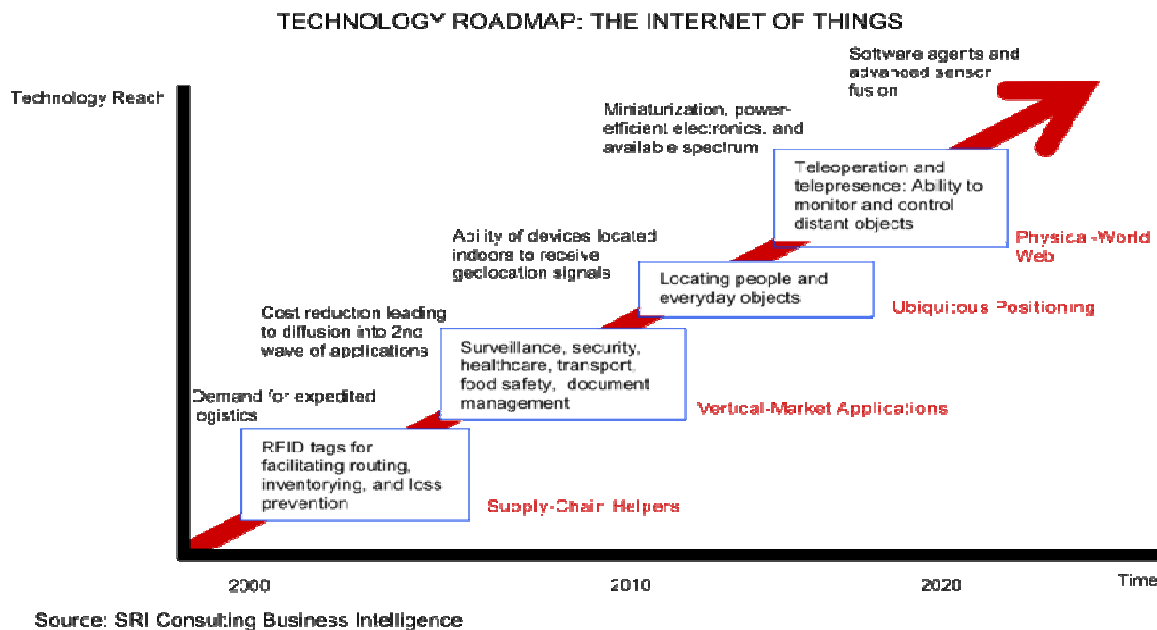
L'Internet des objets repose sur une multiplicité de technologies, notamment les senseurs, les systèmes embarqués, les technologies de « *big data* » - qu'il s'agisse de stockage ou de traitement intelligent, réseaux intelligents, etc.

S'agissant de systèmes complexes, les capacités d'intégration sont cruciales pour leur déploiement puis leur généralisation.

La feuille de route jointe, extraite de travaux du SRI *Consulting Business Intelligence* rythme les perspectives envisagées pour le développement de l'Internet des objets d'ici 2020.

Son examen montre quatre choses :

- à ce stade, les développements se poursuivent selon la feuille de route anticipée ;
- l'enrichissement des possibilités et des applications va se poursuivre à un rythme important ;
- les technologies vont évoluer ou changer sur chacun des segments ;
- la décennie 2010 sera cruciale – comme l'affirment les gouvernements de Singapour et de Chine – *cf. infra*, ou la presse d'affaires des Etats-Unis – *cf. supra*.



La France a des atouts dans la compétition, encore ouverte, autour de l'internet avec des objets :

- de nombreuses technologies innovantes dans les laboratoires et les entreprises ;
- des preuves de concept nombreuses et réussies – notamment grâce aux FUI – fonds unique d'investissement ;

- des secteurs dynamiques utilisateurs : l'aéronautique, le luxe, l'agro-alimentaire, le médicament, ... ;
- un savoir-faire en matière de systèmes complexes, d'intégration et de sécurité.

1.4 L'Internet des objets peut répondre à des besoins de la logistique transfrontière ou à longue distance.

L'usage des applications et/ou des technologies de l'Internet au monde des objets répond, selon les catégories d'acteurs et les secteurs concernés, à des besoins de divers ordres.

Ces besoins sont notamment la vérification de l'intégrité, l'identification, l'authentification, la traçabilité et l'association de documents (contrôle réglementaire). Ils concernent tant les produits que les contenants.

Les définitions des trois premiers peuvent mériter un rappel.

Identification :

C'est le processus visant à reconnaître un produit au vu d'éléments tangibles.

Process of recognizing the attributes that identify the object (source ISO/IEC29115)*

Ces éléments n'ont qu'une valeur indicative proposée par le fournisseur et soumise à l'appréciation du end-user. Une inadéquation évidente sera un premier élément de doute.

Exemples :

L'étiquette, la forme, le nom, la marque d'un produit permettent de le reconnaître. Une identité codée (n° de série, code à barres, code matriciel, RFID...) permet de corréler le produit qui la porte à une description dématérialisée et des informations de traçabilité.

Une bouteille d'eau est porteuse de son identité (étiquette), des mentions obligatoires et du lien vers la traçabilité (n° de lot). Un code à barres permet une identification "type de produit / fournisseur" qui facilite la gestion de stocks et le passage en caisse.

Authentification :

C'est le processus permettant la vérification des éléments caractéristiques d'un produit authentique.

Process of corroborating an entity or attributes with a specified or understood level of assurance (source ISO/IEC29115)*

L'absence de ces éléments ou leur non-conformité constitue un élément de preuve de faux.

L'authentification est corrélée à l'identification afin de pouvoir initier le processus ad hoc.

L'authentification peut être réalisée à l'aide d'éléments authentifiants visibles, interprétables à l'œil nu (hologramme, encre variable), codés, visibles ou invisibles, et interprétables à l'aide d'un outil (nanoparticules, chaos de bulles, signature cachée) ou nécessitant des moyens de laboratoire (ADN, formulation, isotopes)

* ISO/IEC DIS 29115 : Information technology -- Security techniques -- Entity authentication assurance framework.

Exemples :

Un billet de banque comporte un grand nombre d'éléments authentifiants, visibles ou invisibles, connus ou non du profane.

Une pièce plastique, une peinture peuvent être marqués par des nanoparticules luminescentes donnant une signature lumineuse spécifique.

Le DoD vient de recommander le marquage ADN des composants sensibles.

Intégrité :

Caractère démontrant qu'un couple contenu-contenant n'a pas été violé. Ceci peut s'appliquer à des biens matériels, des documents ou des échanges immatériels. L'intégrité n'est pas en soi une preuve d'authenticité si les sceaux peuvent être contrefaits.

Exemples :

Un dispositif anti-effraction (tamper-proof, tamper-evidence) sur un emballage, ou l'emballage lui-même, peut être contrefait. Il convient donc d'y associer un moyen d'authentification (scellés sécurisés, marquage de la matière par nanoparticules...).

2. La compétition entre l'Asie et l'Amérique marque la géopolitique de l'Internet des objets

2.1 Les pays industriels d'Asie affirment leurs ambitions

La géopolitique des STIC – sciences et technologies de l'information et de la communication – et de l'émergence de l'Internet des objets, qui a commencé vers 2000/2005, n'est en rien comparable à celle du développement de l'Internet dans les années 1980 et 1990 : la suprématie incontestée des Etats-Unis a laissé la place à une compétition entre les grandes puissances, notamment entre les Etats-Unis et la Chine.

Une revue documentaire ciblée permet de voir l'affirmation d'ambitions dans ce domaine à très court terme en Asie et aux Etats-Unis, alors que l'Europe peine à s'engager.

La Chine a mis en place de façon volontariste une politique holistique qui vise à faire de « **la Chine le pays de l'Internet des objets en 2015** ». Cette politique semble mobiliser des moyens considérables, elle est portée au plus haut niveau de l'Etat, favorisée par la place de ce pays en tant qu'exportateur – et importateur – d'objets de tous types.

Singapour a également mis en place une politique globale pour l'Internet des objets, associant les autorités et le secteur privé, créant des centres de ressources et développant des applications dans de nombreux domaines – ports, aéroports, environnement, transports, santé, ...

La Corée du sud et la Malaisie ont engagé des politiques qui semblent plus sectorisées et qui reposent sur des réalisations dans des secteurs à enjeux jugés immédiatement prioritaires : gestion de la ville, de l'eau et des transports, contrôle des pollutions ou des frontières, ...

L'approche politique aux **Etats-Unis** est visiblement moins médiatisée, bien que, ou parce que, le concept – ubiquitaire et ouvert – de l'Internet des objets soit né dans ce pays, pensé par les pères fondateurs de l'Internet.

Cependant, de nombreux éléments montrent un intérêt certain et des investissements pour des réalisations concrètes et financièrement soutenables : les publications du Gartner et les articles du Wall Street Journal s'en font échos, pour prendre deux exemples. Les pouvoirs publics ne sont pas absents des réalisations - à titre d'exemple, la FCC vient de créer une direction des soins - *healthcare* - pour traiter le sujet de l'Internet des objets pour les soins, à domicile et à l'hôpital.

Les services de la Commission de **l'Union européenne** ont beaucoup communiqué sur ce sujet dans les années 2007 – 2009. Leur activité est redevenue plus réduite. A l'opposé de l'Asie, l'Europe semble être entrée dans « la vallée des déceptions ».

Cependant, le **Royaume-Uni** a défini et lancé une politique industrielle pour positionner favorablement ses entreprises et ses éco-systèmes dans la compétition mondiale autour des applications de l'Internet des objets ; la politique de coopération entre les entreprises et d'émergence de *champions* de toutes taille vise à dégager des compétences, des segments d'excellence et des effets clusters autour de réalisations concrètes. Depuis peu, le recours au « financement par la foule » - *crowdfunding* – est une composante de ce plan.

En **Allemagne**, les sources relatives à l'Internet des objets sont plus rares, mais le sujet est traité sous l'appellation des « réseaux intelligents » ou sous celle du M2M. L'angle adopté est celui de la R&D et de l'innovation ; les discours faits par les ministres en charge du secteur au CeBit 2012 en sont de bons exemples.

2.2 L'horizon de maturité de l'Internet des objets est perçu en Asie à plus court terme qu'en Europe

Il convient de remarquer toutefois que **l'Asie et l'Europe n'envisagent pas la maturité de l'Internet des objets** au même horizon :

- la Chine met en avant 2015 comme l'année de plénitude ; à Singapour, on parle de réalisations généralisées dans trois à cinq ans ;
- en Europe, les perspectives sont plus lointaines ; par exemple, 5 ou 7 ans paraissent des horizons plausibles de maturité pour la majorité de ceux qui ont répondu au questionnaire du CGEJET.

Il est donc apparu stratégique de rassembler des éléments de comparaison internationale concernant le secteur logistique et les activités douanières, en matière de politiques, de réalisations ou de projets.

Une consultation des Douanes a été conduite par les attachés douaniers dans une sélection de pays (notamment Etats-Unis, Royaume-Uni, Allemagne, Suède, Italie, Pays-Bas, Dubaï, Singapour, Australie et Chine) sur la base d'un questionnaire établi par la mission en liaison avec la DGDDI.

Les résultats des contacts pris par les attachés de Douane sont décevants, en raison à la fois du faible nombre de réponses, et pour certaines d'un contenu particulièrement réduit.

On retiendra que :

- Singapour dispose dès maintenant d'une gamme étendue d'applications relatives aux objets, aux activités aéroportuaires et portuaires et aux contrôles douaniers, la réponse intéressante est en annexe 6. Ce constat n'est pas surprenant compte-tenu de la mise en œuvre d'une politique globale volontariste par les secteurs privés et publics ;

- la Douane américaine réalise un effort d'équipement systématique des agents en moyens de lecture des identifiants ;
- les Britanniques, les Néerlandais et les Allemands n'ont pas voulu communiquer au-delà d'une réponse de courtoisie ;
- les autres Douanes n'ont pas répondu.

La question qui est posée relativement à l'attitude des Douanes européennes est celle des raisons de leur discrétion : absence de politique et de projets ou volonté de disposer d'avantages compétitifs dans la concurrence entre les plates-formes et les territoires.

La mission a retenu les constats suivants de la situation internationale :

- certains pays, notamment en Asie, mettent en œuvre une politique pour l'Internet avec des objets ;
- les activités intéressant la Douane sont partie prenante au développement d'applications, et de facilités mettant en œuvre l'Internet des objets ;
- la compétition à l'échelle mondiale et européenne entre les plates-formes et les territoires comportera un aspect Internet des objets pour la logistique, notamment transfrontière ;
- les horizons de maturité sont courts, ou plus exactement plus courts que souvent anticipé en Europe ;
- les pays industriels d'Asie privilégient des approches ambitieuses, holistiques avec des horizons courts.

3. Les acteurs énoncent quatre messages et posent trois questions à l'horizon de 5/7 ans

La méthodologie : une enquête de type Delphi, des entretiens et une conférence débat.

La méthode retenue dans le cadre de la mission pour tracer les perspectives de l'Internet des objets a été celle d'une consultation d'acteurs, selon la méthode du Delphi, complétée par des entretiens en face à face.

La restitution d'une synthèse de ces travaux a été faite lors d'un séminaire organisé dans les locaux de l'Institut Mines -Telecom le 18 octobre 2012. Ce séminaire réunissait une quarantaine d'experts invités.

La restitution de a été poursuivie par trois débats portant sur les trois sujets jugés les plus cruciaux par les participants à l'enquête :

- les données personnelles et la vie privée ;
- l'intelligence économique et la cybercriminalité ;
- le passage à l'échelle.

Les articles rédigés par deux experts à la suite de ces débats constituent la quatrième partie du présent rapport.

Des entretiens préparatoires avec les services de la direction générale des douanes et droits indirects et avec des acteurs couvrant l'ensemble de l'écosystème, de la R et D aux utilisateurs (centres de recherche, entreprises de technologie, entreprises utilisatrices, intégrateurs, experts, administrations, assureurs, cabinets d'avocats, etc.) ont permis d'élaborer le questionnaire joint en annexe 7.

Toute la filière est concernée, de la technologie aux assureurs en passant par les offreurs.

Les acteurs consultés, incluant les « leaders » de la filière, étaient de tailles diverses. Plus de 35 réponses ont été reçues, couvrant bien l'éventail des catégories d'acteurs concernés. Peu d'acteurs sollicité n'ont pas répondu, ce qui est un indice fort d'intérêt.

Conformément à la méthode retenue, l'enquête était itérative, les participants recevant les réponses à un "premier tour de questionnaire" et pouvant, le cas échéant, modifier leurs réponses et les justifier. Le questionnaire s'adressait aux responsables exécutifs des entreprises et des administrations concernées ainsi qu'aux experts. Il était fermé au sens où il a été adressé à des personnes physiques ou morales pré identifiées - notamment sur recommandation des participants. Les réponses pouvaient concerner, au choix du répondant, tout ou partie du questionnaire.

En complément de l'envoi du questionnaire, une vingtaine d'entretiens individuels ou en petit groupe ont permis d'approfondir « la toile de fond ». La liste des organisations et des entreprises ayant participé à l'enquête – questionnaire ou entretiens – est en annexe 8.

Enfin, la synthèse des réponses a été présenté lors d'une conférence débat à l'Ecole des mines, précédant trois interventions relatives aux trois questions posées par les répondants – cf. partie IV *infra*. Une quarantaine d'experts ont répondu à l'invitation qu'ils avaient reçu.

Les développements qui suivent retracent la synthèse les quatre principaux enseignements tirés de la consultation des acteurs sur les perspectives à 5/7 ans de l'Internet des objets.

3.1 L'Internet des objets est une perspective motivante et crédible.

Récusant généralement le schéma d'un Internet global et universaliste, les acteurs consultés prévoient assez unanimement un développement rapide des Internets « avec des objets ».

3.2 Un mouvement de moyen-long terme est engagé pour tirer profit des potentialités des Internets des objets.

Les acteurs estiment que les Internets « avec des objets » seront largement diffusés d'ici 5 à 7 ans.

Les technologies et les applications viseront d'abord les contenants pour les besoins de la chaîne logistique puis également les contenus.

Les principaux secteurs d'application seront ceux de la logistique, des contrôles réglementaires et de la lutte anti contrefaçon.

Les moteurs essentiels du développement des Internets des objets seront l'économie des entreprises (optimisation des chaînes de traitement en vue d'une réduction des coûts) et la sécurité, sous tous ses angles, de l'intégrité des contenants et des contenus à l'anti-terrorisme.

Les choix applicatifs et technologiques relèveront de postures pragmatiques dans des équations propres.

Le constat partagé est que l'écosystème est disponible, de la recherche jusqu'à l'offre de services.

Les technologies sont industriellement disponibles, mais le passage à l'échelle reste souvent à tester au-delà des preuves de concept abondantes.

Sur ce point, les utilisateurs ont tendance à se distinguer des entreprises de recherche et de technologie sur trois points :

- la nécessité de donner « le temps au temps » ;
- la nature et l'ampleur des sujets à traiter ;
- une perception propre de la conjugaison de l'interopérabilité et de la clôture des applications, en termes de caractère souhaitable et/ou de faisabilité.

3.3 La généralisation de l'Internet des objets repose sur des logiques originales, propres à chaque acteur dans un contexte aux aspects pluriels

Le déploiement à large échelle d'applications de l'Internet des objets est devenu possible et réalisable à court-moyen terme, sous certaines conditions.

Les usages respecteront des logiques originales, chaque contexte de solution étant marqué par des réalités économiques, des besoins, des intérêts géopolitiques différents, voire, le cas échéant, divergents ou antagonistes.

Les acteurs ne se projettent pas dans un système global mais dans un monde où coexisteront des pluralités de standards, de technologies, d'architectures et d'opérateurs.

De même, le cadre de mise en œuvre des applications sera très varié, du point de vue géographique (mondial, régional, national) comme du point de vue réglementaire et/ou métier (pour certains produits, pour une entreprise, pour une marque, etc.).

Deux grandes familles d'applications se distingueront :

- celles concernant la logistique, la traçabilité, l'intégrité, le contrôle réglementaire ;
- celles visant à la lutte contre la contrefaçon, et donc à la vérification de l'authenticité, in fine sous la maîtrise des titulaires des droits.

Des applications et des systèmes de degrés de compatibilité « choisis » coexisteront et coopéreront, les uns ouverts et interopérables, les autres « réservés » et « fermés », partiellement interopérables.

3.4 A terme, la massification des usages passe par la réponse à plusieurs défis – non-technologiques, notamment concernant la protection de la vie privée et l'intelligence économique

Alors que cela n'était pas le cas pour l'Internet des documents, les utilisateurs sont cette fois « prévenus » ex-ante des difficultés et des risques potentiels.

La question du respect de la vie privée et de la gestion des données personnelles est considérée comme un point crucial.

La question du statut des données traitées dans le cadre des Internets avec des objets pose de nombreuses questions au regard du cadre légal actuel :

- Quel est le statut de ces données au regard des dispositions « informatique et liberté » ?
- Pourra-t-on et comment mettre en œuvre un droit à l'expérimentation ?
- Qu'en sera-t-il des projets d'extension des dispositions « informatique et liberté », extension envisagée par exemple à l'adresse IP ?
- Existera-t-il des corpus de règles spécifiques (par exemple pour la technologie RFID, régimes d'autorisation ou de notification, etc.) ?

Les acteurs estiment que les orientations prises en matière de protection des données personnelles et de la vie privée auront un impact déterminant sur le développement des Internets avec des objets et donc sur les services et les processus des entreprises et des administrations.

Pour reprendre la formule d'Eric Barbry, avocat, intervenant sur ce point lors du séminaire du 18 octobre, s'agira-t-il de mettre en œuvre « *un droit de l'Internet des objets ou bien un droit pour l'Internet des objets* » ?

La cybersécurité et l'intelligence économique offensive apparaît comme une menace prégnante.

Par ailleurs, les risques inhérents à l'existence de positions dominantes sont signalés.

La reconfiguration des rôles des acteurs de la chaîne logistique est jugée parfois inévitable, parfois souhaitable, souvent possible.

Sur le plan des moyens à mettre en œuvre pour atteindre les objectifs, la mobilisation des ressources est présentée comme pouvant poser des difficultés, notamment en matière de formation et de normes juridiques.

Enfin, le sujet de la standardisation apparaît soluble à la quasi-totalité des répondants ; il ne figure ni dans leurs sujets d'inquiétude, ni parmi leurs priorités.

4. Avis d'experts et débats autour des questions cruciales : vie privée et cybersécurité

La mission a organisé une conférence-débat le 18 novembre 2012, à l'Ecole des mines autour des sujets jugés les plus sensibles par les participants à l'enquête précitée.

Cette conférence-débat a été l'occasion de deux contributions à la revue « Réalités industrielles » des Annales des mines qui font le point sur ces sujets.

Le premier, par importance, concerne **la vie privée et les objets**, par Alain Bensoussan et Eric Barbry du cabinet Alain Bensoussan.

Il est reproduit ci-dessous, sa conclusion est : « Le choix est donc celui d'un « droit de l'internet des objets » empreint de règles et de contraintes ou un « droit pour l'internet des objets » basé sur le droit à l'expérimentation et le contrôle des usages et noms de l'objet lui-même. »

Le second est celui de **la cybercriminalité et de l'Internet des objets**, par le Colonel Eric Freyssinet, du pôle judiciaire de la Gendarmerie nationale.

Il met en avant la nécessité d'un changement d'attitude : « Il ne faut donc pas en douter, la cybercriminalité sera présente dans l'Internet des objets, c'est ce qu'aussi bien les exemples du passé que l'actualité récente nous enseignent. Comme pour toutes les évolutions technologiques, il ne faut surtout pas que cette perspective en freine le développement, mais il faut prendre en compte dès la conception des systèmes ces risques nouveaux et de plus en plus présents. Et ne nous y trompons pas, autant il était raisonnable de considérer que les activités illégales dans l'univers numérique restaient anecdotiques ou émergentes dans les années 1990, autant la leçon des dix dernières années est qu'elles sont une partie intégrante du développement technologique aujourd'hui.

Partant de ce constat, il ne faut plus se contenter d'utiliser à la marge les technologies de l'Internet des objets pour protéger les activités légitimes des activités criminelles ou envisager de sécuriser les activités classiques grâce aux technologies de l'Internet des objets, mais inventer de nouveaux usages. On peut par exemple imaginer des objets de confiance qui effectueraient des sortes de patrouilles numériques, sous le contrôle de ceux qui sont chargés de la sécurité des systèmes ou même des services de police. Ceux-ci obéiraient évidemment à des règles de transparence et de respect de la vie privée adaptés, mais ils seraient nettement plus efficaces qu'une observation totalement extérieure telle qu'on la réalise aujourd'hui. »

4.1 La vie privée des objets

Par **Alain BENSOUSSAN** et **Eric BARBRY** *

Introduction

« Vie privée d'un objet », le titre peut paraître surprenant et pourtant c'est sans doute une des questions les plus prégnante de l'ère du numérique.

Car derrière ce titre se cache un sujet qui va révolutionner le monde : celui de l'internet des objets.

L'internet des objets recèle un nombre impressionnant de questions de nature juridique : statut juridique de l'objet connecté, responsabilité de l'objet ou par l'objet, identité de l'objet, maîtrise et gouvernance de l'ONS (Object name system) ... mais il est une question qui cristallise toutes les angoisses ou les attentes selon que l'on soit négativement ou positivement orienté : celle des données personnelles et de la vie privée.

Cette question n'est pas une interrogation futuriste c'est une question très actuelle. Il suffit pour s'en convaincre de compter les ouvrages, articles, études et autres conférences consacrés à ce sujet.

L'internet des objets touche tous les secteurs. Le monde de l'automobile planche depuis de nombreuses années sur le « véhicule intelligent » qui réagit à son environnement (son conducteur / la circulation / l'environnement). Le monde du bâtiment en fait de même autour de concepts tels que la « maison intelligente »... et mieux encore à la « ville intelligente » qui « réagit » et s'adapte à son propre environnement (consommation d'énergie, environnement, qualité de vie, ...)

D'autres secteurs sont déjà conquis par l'IdO comme celui de l'énergie qui consacre énormément d'argent au smart grid (réseau d'énergie intelligent). Des capteurs tous azimuts dialoguant entre eux, interprétant des données endogènes (consommation réelle) et exogènes (environnement/climat/prix instantané de telle ou telle source d'énergie/événement exceptionnel) le tout pour optimiser la création et l'exploitation du parc énergétique.

Certains projets sont directement supportés par l'Union européenne comme la « voiture vertes », le « bâtiment économe » ou « l'usine du futur ».

L'internet des objets est une véritable révolution en 3D.

La première dimension est celle de la « fusion » des mondes ; le monde physique (moléculaire) d'une part et le monde numérique d'autre part ;

La seconde dimension est celle de l'homo connecticus, les hommes naissent égaux en droit ... et connectés en fait ;

La troisième dimension étant celle de l'objet intelligent et (quasi) autonome à savoir l'avènement du M to M [machin to machin].

A la différence de l'internet 1.0 où le législateur est intervenu trop tard et le web 2.0 où il n'est tout simplement pas intervenu, le Politique s'est saisi très rapidement de l'internet des objets.

En témoigne la conférence ministérielle du conseil de l'Union européenne des 6 et 7 octobre 2008.

Mais il y a mieux avec la publication, le 18 juin 2009, d'une communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions intitulée précisément : « Internet des objets - Un plan d'action pour l'Europe. »

Au sein de cette communication 14 lignes d'action ont été retenues parmi lesquelles figurent : la nécessaire mise en œuvre d'une gouvernance au moins au plan européen ; la sécurisation de l'IdO principalement confiée à l'ENISA ; le couple IdO et infrastructure d'importance vitale ; la nécessaire normalisation des technologies de l'IdO ; l'importance de la R&D et le lancement de projets pilotes ...

Sur le plan juridique la communication évoque deux problématiques juridiques :

La ligne d'action 2 - Evoque la nécessité d'un « Suivi du contenu des questions relatives à la vie privée et à la protection des données personnelles. Il s'agit là assurément d'une ligne d'action purement juridique ».

La ligne d'action 3 - Retient le besoin de reconnaître le droit à la déconnexion autrement appelé le droit au « silence des puces ».

Si ces deux questions sont importantes, il faut s'attendre à ce que l'internet des objets bouleverse la donne juridique en matière de données personnelles sous deux axes :

- le premier axe, dit « axe d'accélération », où des questions et des débats résiliants devront nécessairement être purgés ;
- le deuxième axe, dit « axe de mutation », qui verra naître des concepts propres à l'internet des objets

L'INTERNET DES OBJETS, ACCELERATEUR DE REFLEXION SUR LE DROIT DES DONNEES PERSONNELLES

Le droit à la neutralité technologique et contre le techno-droit

Qu'est que "le techno droit". Un droit conçu spécifiquement autour d'une technologie et non des usages que l'on peut faire de cette technologie au regard du droit des données personnelles.

Existe t-il un techno droit des données personnelles ? Oui.

Qui en est la victime : la biométrie.

Pourquoi parler ici de « victime » ? Tout simplement car la biométrie est la seule technologie visée dans la loi informatique et libertés.

La situation de la biométrie est d'ailleurs assez ubuesque car il s'agit de la seule technologie considérée de par la loi comme « suspecte » au point de mériter un traitement spécial : celui de l'autorisation préalable dans tous les cas...

L'erreur fatale pour la biométrie a été d'être : "at the bad place at the bad time !" Autrement dit avoir émergé au moment même où était adoptée la loi Informatique et libertés 2.0 en France (2008).

Ceci explique qu'il n'existe rien de tel pour le sans contact, la géolocalisation ou les scanners corporels qui sont toutes des technologies « sensibles » ou plus exactement des technologies qui peuvent être utilisées de manière plus ou moins raisonnables car à la vérité ses technologies sont « neutres » ce sont ceux qui les utilisent qui sont en cause.

Il serait regrettable que l'internet des objets suivre le même chemin que la biométrie. Or, la chose est tout à fait possible dans la mesure où l'Union européenne est sur le point d'adopter un règlement sur le droit des données personnelles.

Le pire pour l'internet des objets serait de se voir réguler avant même d'exister.

Le droit à l'expérimentation

Même en l'absence de loi dédiée on ne peut que craindre des positions « dures » de la part des régulateurs du secteur des données personnelles des positions restrictives.

Entre le tout interdit et le tout permis il existe une troisième voie celle de l'expérimentation.

La Cnil a eu recours à plusieurs reprises à cette procédure particulière (paiement par authentification du réseau veineux, dossier pharmaceutique, mobile sans contact, scanner corporel, ...).

Si l'expérimentation est un droit elle reste encore limitée pour deux raisons :

- expérimenter s'est ralenti. L'expérimentation est souvent synonyme de « limitation » qu'elle soit temporelle, géographique ou liée à une « cible » ;

- l'expérimentation est très encadrée et très contraignante et il n'est pas certain que tous les élus soient finalement recevables pour une généralisation ;

Il faudrait donc pour l'internet des objets, mais ce peut être vrai pour toutes les technologies en devenir, un « droit opposable » à l'expérimentation.

A charge pour celui qui en bénéficie de dresser dès l'origine du projet une cartographie précise des risques à traiter, des moyens de les appréhender et le cas échéant des voies à explorer pour les traiter.

Le droit à la propriété des données

Il y a encore quelques années lorsque nous parlions de « propriété des données » nous passions pour des juristes excentriques.

Ce concept s'est pourtant concrétisé avec l'avènement des réseaux sociaux. D'un droit de « protection » des données personnelles, nous sommes passés à un droit de « propriété » sur les données personnelles.

La différence est fondamentale. Le droit de données personnelles est un « droit opposable », c'est un droit à accepter ou refuser que des données ne soient exploitées par un tiers ; le droit de propriété des données est beaucoup plus fort encore, c'est à « droit de disposition » c'est à dire un droit de faire ce que l'on veut de ses données voir même de les commercialiser.

Si le droit des données est d'ordre légal (directive 95-45, loi informatique et libertés I et II, règlement à venir) le droit de propriété des données lui est pour l'heure contractuel.

Ce sont les plates-formes web 2.0 (Facebook, twitter, linkedin et les autres) qui, au travers de leur conditions générales, reconnaissent, contractuellement, à leurs abonnés un droit sur « leurs » données.

Ce faisant et de manière plus subtile encore, ces mêmes plates-formes s'arrogent contractuellement le droits d'exploiter, commercialiser et d'échanger ces mêmes données.

L'internet des objets accélèrera à n'en pas douter la question de la propriété des données car il sera difficile de maintenir des concepts tels que le « consentement » et « l'accord préalable » qui sont faciles à maîtriser dans un environnement traditionnel mais sera nettement plus compliqué dans un monde où tout sera connecté par principe et où la capacité à consentir sera faible, voire nulle.

La propriété des données sera un sujet d'autant plus important que dans le monde de l'internet des objets la donnée de base sera nécessairement « enrichie » et que se posera nécessairement la question de la valeur et de la propriété de cette « donnée augmentée ».

Le droit de la propriété des données, s'il est admis, révolutionnera en profondeur le droit des données personnelles. Ainsi il ne serait plus question uniquement d'un droit d'accès et de rectification de ses données ; mais aussi d'un droit de copie ou d'obtention des données. Ainsi l'utilisateur serait en droit à première demande d'obtenir une copie de toutes ses données, enrichies au besoin, pour son propre usage, et le cas échéant les commercialiser lui-même auprès d'un autre prestataire.

Ce droit est d'ores et déjà envisagé à l'article 18.1 de la proposition de règlement du Parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) en ces termes :

« Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée. »

Le droit à la personnalisation anonyme

Sur ce droit aussi nous avons sans doute été parmi les premiers à affirmer qu'entre le droit des données personnelles d'une part et l'anonymisation d'autre part, il pouvait exister une troisième voie : la « personnalisation anonyme ».

Il s'agit ici à l'instar d'autres de nos concepts comme la « vie privée résiduelle » ou la « vie privée partagée » de reconnaître une réalité de l'internet d'aujourd'hui : il est possible de tout savoir sur quelqu'un et de lui proposer des services adaptés sans savoir qui il est !

Là encore l'internet des objets n'est pas à l'origine de cette réalité mais il risque fort d'en être le catalyseur.

Le web connaît en effet déjà cette notion de personnalisation anonyme à travers des techniques d'analyses comportementales telles que les cookies.

Et si l'on en vient aux cookies c'est après la biométrie la seconde technologie considérée comme « sensible » dans notre environnement juridique, au point qu'ils font l'objet d'une régulation spéciale.

Mais à la différence de la biométrie, et c'est heureux, les cookies ne relèvent pas d'un régime d'autorisation préalable mais la loi impose pour certaines catégories d'entre eux un consentement exprès de l'internaute...

Imaginons la même règle pour l'internet des objets et nous risquons fort d'être submergés de pop-up et autres alertes qui, inondant les utilisateurs, rendrait l'internet des objets quasi impraticable.

On constate d'ailleurs qu'à ce jour très peu, pour ne pas dire, aucune des entreprises ne respectent les nouvelles règles en termes de cookies.

Il faudra sans doute, si l'on veut promouvoir et développer l'internet des objets reconnaître un droit à la « personnalisation anonyme » et en définir les règles afin qu'elle puisse être mise en œuvre sans contraintes excessives.

Le droit à la sécurité et à la traçabilité

Le droit à la sécurité et à la traçabilité est un élément important de la réflexion sociétale. Or dans bien des cas la technologie est au service de l'un ou l'autre de ces objectifs. Biométrie, vidéoprotection, géolocalisation ou encore scanner corporels en sont les meilleurs exemples.

L'internet des objets est sans doute un des moyens les plus efficaces de tracer les produits et de lutter contre les contrefaçons en tout genre.

Mais il est clair que les consciences ne sont toujours pas mûres pour admettre que le droit à la sécurité ou le droit à la traçabilité collective pourrait supplanter le droit à la vie privée individuelle.

Avec l'internet des objets la question va devoir être débattue sinon tranchée car assurément l'internet des objets est un janus dont l'une des faces est de pouvoir tout tracer, tout le temps, sur tout...

L'INTERNET DES OBJETS, CREATEUR D'UN NOUVEAU DROIT DES DONNEES PERSONNELLES

L'internet des objets n'est pas simplement le catalyseur, l'accélérateur, d'une réflexion sur le droit des données personnelles ou de la vie privée mais peut, à bien des égards, être créateur de nouveaux droits ou de nouveaux concepts.

Il en est ainsi d'au moins trois d'entre eux : Le droit au silence des puces ; le droit à l'invisibilité (disparition) et le droit à la portabilité des données

Le droit au silence des puces

Le droit au silence des puces est le concept le plus connu de ce que pourrait être un nouveau droit des données personnelles lié directement à l'internet des objets.

Ce concept a d'ailleurs été expressément retenu au sein de la communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions intitulée précisément : « Internet des objets - Un plan d'action pour l'Europe » du 18 juin 2009.

La problématique posée par le droit à la désactivation des puces autrement appelée « le droit au silence des puces » est qu'elle est basée sur un mode « opt ou » : je décide de rendre inactive des puces par nature en mode « actif ».

D'autres préfèrent déjà la démarche « opt in » autrement dit de reconnaître non pas un droit au silence mais un droit à la « parole de puce » : A l'utilisateur de décider s'il active ou non la puce qui par nature est en mode « inactif ».

Que l'on soit pour le silence ou la parole des puces, les deux concepts ont leur limite : une fois activées ou désactivées la manipulation est souvent irréversible.

Or, plutôt qu'un droit manichéen entre droit à la parole ou au silence des puces c'est sans doute un droit à la « gestion des puces » qu'il faudrait reconnaître. Seule contrainte à ce

nouveau droit et elle est de taille : nous transformer tous en dresseurs de puces... autrement dit en administrateur système !

Par ailleurs il conviendra sans doute non pas uniquement comme c'est le cas aujourd'hui de pénaliser l'accès illicite à des informations nominatives (rappelons en effet que les lois relatives aux données personnelles pénalisent la collecte déloyale) mais de criminaliser le fait de placer des connecteurs et autres puces sans information préalable et capacité de déconnexion des dits connecteurs. De même si le « droit à l'oubli » est une nécessité dans un environnement où l'information est la norme le concept devra sans doute migrer vers un droit à l'effacement des traces s'agissant de l'IdO.

Le droit à la portabilité des données

Enfin le droit à la portabilité sera à n'en pas douter un autre droit important dans le monde des objets connectés. Pouvoir porter ou reporter des données d'un SI vers un autre est une question fondamentale de l'internet des objets.

Ce droit est d'ores et déjà fixé à l'article 18.2 de la proposition de règlement du Parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) qui dispose :

« Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle. »

CONCLUSIONS

Réguler ou ne pas réguler l'internet des objets là est la question. Mais d'emblée l'exercice paraît aussi délicat que demander au cloud de ne pas sortir des frontières de l'Union européenne. Par nature l'internet est mondial et il en sera ainsi de l'internet des objets.

De fait, on peut s'interroger sur l'intérêt et la portée de régulation nationale dans le domaine.

Si la voie de la régulation est envisagée, il conviendra, alors d'en définir le contenu : s'agira-t-il d'une loi d'expérimentation sous contrôle : ode loi bioéthique ; ou d'une loi de confiance qui comme la loi pour la confiance dans l'économie numérique fait primer la confiance de l'internet au détriment de celle des acteurs ; ou encore d'une loi de contrainte de nature à privilégier le contrôle et l'internet sur l'innovation.

Le choix est donc celui d'un « droit de l'internet des objets » empreint de règles et de contraintes ou un « droit pour l'internet des objets » basé sur le droit à l'expérimentation et le contrôle des usages et noms de l'objet lui-même.

Entre la peur et le mépris c'est au Politique aujourd'hui de se saisir de la question.

NOTE

* Cabinet Bensoussan

4.2 internet des objets : nouveau champ d'action pour la cybercriminalité

Par Eric FREYSSINET*

L'observation de la cybercriminalité et des différentes formes d'abus des technologies numériques a montré au cours des dix dernières années que les activités illégales ne se contentaient plus d'un rôle marginal dans l'univers numérique, mobilisées par l'appropriation financière et informationnelle. L'émergence d'un Internet des objets, support des activités humaines, doit évidemment faire prendre en compte ce type de risques, d'autant plus que les conséquences en sont encore difficiles à évaluer, ne serait-ce que par les dimensions d'une telle évolution (nombre d'objets, nombre de réseaux qui interagissent, nouveaux usages). Ce sont une multitude d'axes de recherche en sécurité qui doivent être ouverts ou soutenus, y compris ceux qui permettront de profiter de ces technologies nouvelles pour améliorer la sécurité.

En matière de cybercriminalité, il faut en permanence observer les nouvelles technologies et les nouveaux usages, parce que les auteurs d'infractions, mais aussi leurs victimes, les appréhendent toujours très vite et en exploitent les faiblesses ou les forces, qui vont faire émerger de nouvelles façons de réaliser des infractions ou des infractions nouvelles. Ils peuvent aussi être l'occasion de développer de nouveaux modes de collecte de la preuve des infractions. Enfin, il faut toujours conserver un œil dans le rétroviseur et ne pas oublier les enseignements du passé.

Nous verrons que c'est particulièrement vrai lorsque l'on considère les évolutions que devraient permettre les technologies que l'on regroupe sous la terminologie de l'Internet des objets : il y aura de nouvelles opportunités pour tous, mais malheureusement y compris pour l'activité criminelle. Nous nous attarderons d'abord sur quelques leçons passées, puis nous envisagerons certaines nouvelles formes de délinquance envisageable et enfin nous pourrions détailler la façon dont l'Internet des objets pourrait être une opportunité de développement des criminalités existantes ou émergentes.

Bien entendu, comme toute analyse de risques et de menaces, ce texte ne remet pas en cause l'intérêt du développement de ces technologies.

DES OBJETS DE PLUS EN PLUS COMMUNICANTS

La notion d'un Internet des objets n'est pas une évolution complètement abstraite ou radicale, elle repose beaucoup sur le développement progressif d'un nombre d'objets qui communiquent ou interagissent et nous entourent peu à peu, et cette tendance ne date pas d'hier.

Le plus emblématique de ces objets pour les Français est peut-être la carte à puce, un objet que nous avons tous dans notre portefeuille et qui utilise un protocole de communication simple mais efficace : pour dialoguer localement avec un terminal de paiement ou un distributeur de billets et en réalité indirectement avec un serveur qui va valider les transactions en temps réel ou en temps différé. Certaines de ces cartes contiennent même un serveur Web (par exemple, des modèles de cartes utilisant la technologie JavaCard). Évidemment, de par les applications qu'elles permettent (paiements électroniques, support de données personnelles,...) toutes les générations de cartes à puce ont été l'objet de tentatives réussies ou non de les abuser : contrefaçon de cartes bancaires ou de cartes de téléphone à péage, ou encore de décodage des émissions télévisées payantes. A chaque fois, des contre-mesures ont dû être implémentées.

Au passage, un des aspects intéressants des fraudes qui ont pu être constatées est que de plus en plus elles exploitent l'ouverture croissante des standards technologiques, aussi bien que des méthodes de rétroconception utilisées pour comprendre le fonctionnement des systèmes qui ne sont pas documentés publiquement et le partage public des résultats. Ainsi, dans l'exemple récent de la mise en cause de la sécurité des cartes bancaires sans contact (dites NFC, du nom des technologies de communication utilisées, near field communications) notamment sur le plan des données personnelles, ce sont avant tout les spécifications publiques de ce protocole qui ont permis de découvrir ces vulnérabilités potentielles. En tout état de cause, l'information est de plus en plus facilement accessible pour ceux qui auraient de mauvaises intentions et il est essentiel d'adapter le temps de réaction aux découvertes de vulnérabilités à cet état de fait.

Badges de télépéage, puces d'identification par radiofréquences (étiquettes RFID passives pour la gestion de stocks, la prévention du vol,...) sont autant d'éléments supplémentaires attachés à nos véhicules, aux objets que l'on achète, dans notre environnement de travail. Pour chaque situation, il y a pu y avoir des tentatives de les contourner, par exemple pour les copier, les désactiver ou les rendre inopérants. Parfois les méthodes sont assez basiques, papier alu ou four à micro-ondes sont couramment utilisés, mais plus récemment on a vu apparaître des sortes de brouilleurs utilisés par des voleurs dans des magasins.

Dans le même ordre d'idée, les automobiles ont dès le début des années 2000 intégré de plus en plus d'électronique, pour contrôler l'accès à l'habitacle ou faciliter le diagnostic au garage. Ces technologies sont très communicantes : réseau local dédié (ou CAN – Controller Area Network) au dialogue entre les calculateurs et les capteurs du véhicule, clés sans contact avec pour les plus récentes détection de leur position exacte à l'intérieur ou à l'extérieur du véhicule et communication par les réseaux de téléphonie mobile et de radio pour obtenir des informations de trafic, permettre aux utilisateurs de communiquer - évidemment, et permettre à certains modèles de voiture de communiquer (appels de secours, positionnement, diagnostic à distance, etc.). Dans ce contexte, les voleurs n'ont pas tardé à recruter des électroniciens et développer toutes sortes de méthodes pour contourner ces sécurités ou les exploiter à leur profit pour prendre le contrôle du véhicule de façon plus avancée encore.

Les ordinateurs portables, téléphones mobiles, tablettes numériques sont autant d'objets communicants qui ont envahi notre quotidien. Quelle que soit l'avancée des technologies de communication existantes, elles ont toutes fait l'objet d'attaques : le protocole très local Bluetooth - sensible parfois à des interceptions de communication, il fut un des premiers vecteurs de virus sur téléphones mobiles, les protocoles de réseaux sans fil Wifi dont la sécurité a été souvent mise à mal - ce qui n'empêche pas de nombreuses connexions aujourd'hui d'être établies en clair, ou encore évidemment les protocoles de téléphonie mobile qui ont beaucoup attiré récemment l'intérêt des chercheurs en sécurité.

L'environnement industriel, enfin, n'échappe pas à cette tendance. Du centre de recherches au site de production, tous les systèmes sont évidemment en réseau. Cela a permis de faire progresser les méthodes de supervision comme de commande des chaînes de production. Cela a aussi introduit un nouveau potentiel pour des attaques. On ne compte plus les publications - scientifiques ou plus simplement journalistiques - qui dénoncent la faiblesse de protection des SCADA (1) - les systèmes de commande industriels - et leur trop grande présence sur Internet, à la portée du premier attaquant qui les découvrirait.

INTERNET DES OBJETS : AVANT TOUT UNE PROBLÉMATIQUE DE SURFACE D'ATTAQUE

Les progrès techniques sont donc - inexorablement ? - attachés à un développement des attaques, ou en tous cas à une potentialité plus forte de ces attaques : l'augmentation de la surface d'attaque, c'est-à-dire le nombre de systèmes connectés et la variété des moyens qui leur permettent de communiquer augmente mécaniquement les possibilités d'attaques, quant en parallèle le nombre de personnes susceptibles de réaliser ces attaques augmente certainement proportionnellement à la population connectée dans chaque pays et dans le Monde.

On a bel et bien constaté l'effet de cette dimension purement quantitative des choses sur le nombre de victimes d'infractions en ligne (en témoigne la croissance difficilement maîtrisée des fraudes aux paiements bancaires via Internet).

Cet effet est multiplié par une évolution des usages. Ainsi, ce qu'on appelle l'Internet dans les nuages - ou cloud computing en anglais - mais aussi l'augmentation de la capacité des outils communicants et le développement d'un nombre exponentiel d'applications, incitent tout un chacun à stocker des informations personnelles - ou les secrets des entreprises - en plus grand nombre, à les partager ou encore à les déposer à distance, sur des serveurs.

Le constat que font les chercheurs en sécurité sur l'avènement du protocole IPv6, qui va permettre de connecter des milliards d'objets à travers la planète grâce à un nombre beaucoup plus important d'adresses possibles, est qu'il présente autant de failles - et ce sont souvent les mêmes que l'on connaissait avec IPv4, il semble qu'on apprenne jamais du passé. Il se pourrait même qu'il apporte ponctuellement quelques risques supplémentaires, avec des équipements dont la connectivité IPv6 est activée par défaut alors que les dispositifs de sécurisation des réseaux dans les entreprises ne le prennent pas encore en compte.

Et c'est bien là un des risques les plus importants, la multiplication d'objets connectés dont on n'aura pas perçu l'importance - on l'a déjà vu pour les SCADA alors qu'en sera-t-il de tous les autres objets plus anodins. Ils risquent de multiplier les portes d'accès vers l'information et vers les systèmes d'information des organisations sans qu'il soit toujours envisagé de les prendre en compte dans les politiques de sécurité. C'est d'ailleurs le problème principal que pose à mon sens la question du BYOD - bring your own device : des systèmes que l'on maîtrise mal et qui ont accès peu ou pro au système d'information des organisations. Qu'en sera-t-il des véhicules des sociétés, des stocks en cours de transport ou des milliers d'interrupteurs, capteurs, caméras... ? Leurs interactions avec de nombreux autres systèmes, comme celles aujourd'hui de nos ordiphones, pourraient être autant de portes d'entrées.

Enfin, une autre des tendances est que ces nombreux objets sont de plus en plus souvent jetables. On les déploie, ils sont peu coûteux et permettent de rendre un service efficace immédiat, mais ils sont ensuite oubliés, abandonnés, contenant parfois des informations qui restent sensibles ou laissant de multiples portes ouvertes vers l'intérieur des réseaux.

Pensera-t-on par exemple à désactiver systématiquement l'accès d'une nuée de micro ou nano-robots qu'on aura déployés pour nettoyer ou explorer un site, à effacer ou révoquer leurs certificats de sécurité ? Saura-t-on construire les référentiels complets de ces déploiements ou se contentera-t-on de les considérer inutiles au regard de la courte durée de vie des systèmes mis en œuvre.

MAIS AUSSI DE NOUVEAUX TYPES D'ABUS POSSIBLES

Les enjeux sécuritaires nouveaux sont tout aussi intéressants à examiner. Le premier est corollaire à ce que l'on vient d'évoquer dans le paragraphe précédent : l'Internet des objets pourrait entraîner la tentation de déployer des systèmes moins sécurisés pour remplir les mêmes besoins qu'auparavant.

On le voit par exemple avec l'arrivée de certains dispositifs d'acquisition de paiements par carte bancaire qui se contentent d'être un adaptateur pour un terminal mobile (tablette ou téléphone) alors qu'on a fait d'énormes progrès dans la sécurisation des terminaux de paiement. Certains réseaux ou nouveaux modes de commercialisation pourraient être tentés d'opter pour ces solutions moins coûteuses et qui paradoxalement paraissent plus modernes.

Les botnets, réseaux construits par la prise de contrôle d'un nombre plus ou moins grand de systèmes compromis et utilisés pour commettre une grande variété d'activités illégales, pourraient connaître un nouveau terrain de jeu avec l'Internet des objets, d'autant plus inquiétant si ceux-ci sont mal sécurisés ou sécurisables. Les botnets sont d'ores et déjà en train de nettement prendre pied dans les réseaux de téléphonie mobile, elle ne manquera pas d'exploiter ces nouveaux espaces.

Le second est plus intrinsèquement lié à ces nouveaux objets : ils créent de nouvelles formes de communication qui n'ont pas encore toutes été testées ou dont la sécurisation n'est pas totalement aboutie. Ainsi, la recherche est particulièrement active sur les méthodes de sécurisation des communications dans les réseaux de type MANET (2) (vérification des certificats, révocation des certificats des objets auxquels on ne fait plus confiance,...).

Ou encore, lorsqu'il s'agira de construire des réseaux où l'ensemble des véhicules, des feux tricolores, des systèmes de mesure du trafic communiqueront entre eux pour échanger énormément d'informations, aura-t-on auparavant testé toutes les configurations ? Que se passera-t-il lorsqu'un seul objet transmet des informations erronées ? Ou toute une gamme d'objets de la même série ? Quelles sont les risques d'une atteinte non accidentelle sur ce genre de configurations alors qu'on sait pertinemment que dans l'univers bien mieux connu des systèmes informatiques classiques on découvre toutes les semaines des vulnérabilités et qu'elles sont exploitées de façon massive dans la nature ? Autant de questions qui doivent être prises en compte lors du calcul des décisions pour la conduite des véhicules ou la gestion du trafic.

Plus généralement enfin, ce sont les détournements des fonctions permises par ces nouveaux usages qui peuvent être envisagées : par exemple, la surveillance du transport de marchandises avec des étiquetages électroniques permet aussi d'imaginer pour des groupes criminels organisés de faciliter leurs méfaits en identifiant rapidement les transports les plus intéressants (nombre et nature des produits transportés).

CONCLUSION

Il ne faut donc pas en douter, la cybercriminalité sera présente dans l'Internet des objets, c'est ce qu'aussi bien les exemples du passé que l'actualité récente nous enseignent. Comme pour toutes les évolutions technologiques, il ne faut surtout pas que cette perspective en freine le développement, mais il faut prendre en compte dès la conception des systèmes ces risques nouveaux et de plus en plus présents. Et ne nous y trompons pas, autant il était raisonnable de considérer que les activités illégales dans l'univers numérique restaient anecdotiques ou émergentes dans les années 1990, autant la leçon des dix dernières années est qu'elles sont une partie intégrante du développement technologique aujourd'hui.

Partant de ce constat, il ne faut plus se contenter d'utiliser à la marge les technologies de l'Internet des objets pour protéger les activités légitimes des activités criminelles ou envisager de sécuriser les activités classiques grâce aux technologies de l'Internet des objets, mais inventer de nouveaux usages. On peut par exemple imaginer des objets de confiance qui effectueraient des sortes de patrouilles numériques, sous le contrôle de ceux qui sont chargés de la sécurité des systèmes ou même des services de police. Ceux-ci obéiraient évidemment à des règles de transparence et de respect de la vie privée adaptés, mais ils seraient nettement plus efficaces qu'une observation totalement extérieure telle qu'on la réalise aujourd'hui.

NOTES

* Lieutenant-colonel de gendarmerie, coordinateur du plateau d'investigation Cybercriminalité & Analyses Numériques (CyAN) du pôle judiciaire de la gendarmerie nationale.

(1) De l'anglais : Supervisory Control And Data Acquisition, systèmes destinés à la surveillance, la supervision et le contrôle à distance des systèmes industriels. Ce sont aussi bien des interfaces permettant d'accéder à l'état d'un système (données mesurées, images,...) que de lui transmettre des ordres.

(2) Mobile *ad-hoc* networks : réseaux IP construits dynamiquement sur la base d'objets mobiles

Annexe 1 : Lettre de mission

CGEIET

2 mai 2012

LETTRE DE MISSION

Mission « enjeux des technologies de l'Internet appliquées aux objets pour les procédures douanières ».

Les technologies de l'internet sont appliquées aujourd'hui au monde des objets dans des conditions à la fois prometteuses quant aux gains d'efficacité ou d'efficience mais décevantes au regard des caractéristiques annoncées de l'Internet des objets – absence d'interopérabilité, normes fermées, protocoles immatures : ONS, IPv6, IP lui-même.

Il est donc nécessaire de se poser deux questions : dans quelle mesure et dans quelles conditions les technologies de l'Internet associées à d'autres technologies pourront apporter une contribution :

- à la police douanière de la chaîne logistique - traçabilité et intégrité des contenants et des contenus, problématique spécifiques aux plates-formes, etc. ;
- à la lutte contre la fraude et la contrefaçon ;
- enfin à une plus grande dématérialisation des procédures.

La DGDDI a demandé au CGEIET de contribuer à mieux cerner les évolutions en cours afin de lui permettre de mieux se préparer à saisir les éventuelles opportunités.

Cette mission comportera quatre aspects :

- D'abord une tentative de contextualisation du sujet en évoquant les éventuelles limites de l'exercice, limites tenant à la fois à l'étendue des attentes de la douane, et à la maîtrise de certains sujets ou décisions par les professionnels ou les seuls détenteurs de droits ;
- Une toile de fond des applications identifiant ou rappelant les points de consensus et les divergences constatées, cela à partir d'une méthode de prospective auprès des acteurs institutionnels, experts et chercheurs, opérateurs de technologies, utilisateurs, etc. ;
- Des éléments de comparaison internationale, par l'exploitation d'une consultation conduite par les attachés douaniers dans une sélection de pays (notamment Etats-Unis, Royaume-Uni, Allemagne, Italie, Pays-Bas, Australie et Chine) sur la base d'un questionnaire établi par la mission avec la DGDDI ;
- Enfin d'éventuelles recommandations relatives à l'urbanisation des systèmes d'information de la DGDDI.

Elle sera réalisée courant 2012.

Annexe 2 : Présentation de l'Internet des objets sur le portail du Gouvernement de Singapour

Source : Portail du gouvernement de Singapour - www.gov.sg , accédé le 21 novembre 2012.

Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analysed and used to initiate action, providing a wealth of intelligence for planning, management and decision-making. This is the world of the Internet of Things (IOT).

The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community circa in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.

Since then, many visionaries have seized on the phrase "Internet of Things" to refer to the general idea of things, especially everyday objects, that are readable, recognisable, locatable, addressable, and/or controllable via the Internet irrespective of the communication means (whether via RFID, wireless LAN, wide-area network, or other means). Everyday objects include not only the electronic devices we encounter or the products of higher technological development such as vehicles and equipment but things that we do not ordinarily think of as electronic at all - such as food and clothing. Examples of "Things" include :

- People
- Location (of objects)
- Time Information (of objects)
- Condition (of objects)

In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Cisco forecasts that this figure is expected to double to 25 billion in 2015 as the number of more smart devices per person increases, and to a further 50 billion by 2020.

Annexe 3 : Looking to Industry for the Next Digital Disruption, article du New-York Times, le 23 novembre 2012 – sans les photos

SAN RAMON, Calif. — When Sharoda Paul finished a postdoctoral fellowship last year at the Palo Alto Research Center, she did what most of her peers do — considered a job at a big Silicon Valley company, in her case, Google. But instead, Ms. Paul, a 31-year-old expert in social computing, went to work for [General Electric](#).

Ms. Paul is one of more than 250 engineers recruited in the last year and a half to G.E.'s new software center here, in the East Bay of San Francisco. The company plans to increase that work force of computer scientists and software developers to 400, and to invest \$1 billion in the center by 2015. The buildup is part of G.E.'s big bet on what it calls the "[industrial Internet](#)," bringing digital intelligence to the physical world of industry as never before.

The concept of Internet-connected machines that collect data and communicate, often called the "Internet of Things," has been around for years. Information technology companies, too, are pursuing this emerging field. I.B.M. has its "Smarter Planet" projects, while Cisco champions the "Internet of Everything."

But G.E.'s effort, analysts say, shows that Internet-era technology is ready to sweep through the industrial economy much as the consumer Internet has transformed media, communications and advertising over the last decade.

In recent months, Ms. Paul has donned a hard hat and safety boots to study power plants. She has ridden on a rail locomotive and toured hospital wards. "Here, you get to work with things that touch people in so many ways," she said. "That was a big draw."

G.E. is the nation's largest industrial company, a producer of aircraft engines, power plant turbines, rail locomotives and medical imaging equipment. It makes the heavy-duty machinery that transports people, heats homes and powers factories, and lets doctors diagnose life-threatening diseases.

G.E. resides in a different world from the consumer Internet. But the major technologies that animate Google and Facebook are also vital ingredients in the industrial Internet — tools from artificial intelligence, like machine-learning software, and vast streams of new data. In industry, the data flood comes mainly from smaller, more powerful and cheaper sensors on the equipment.

Smarter machines, for example, can alert their human handlers when they will need maintenance, before a breakdown. It is the equivalent of preventive and personalized care for equipment, with less downtime and more output.

"These technologies are really there now, in a way that is practical and economic," said Mark M. Little, G.E.'s senior vice president for global research.

G.E.'s embrace of the industrial Internet is a long-term strategy. But if its optimism proves justified, the impact could be felt across the economy.

The outlook for technology-led economic growth is a subject of considerable debate. In [a recent research paper](#), Robert J. Gordon, a prominent economist at Northwestern University, argues that the gains from computing and the Internet have petered out in the last eight years.

Since 2000, Mr. Gordon asserts, invention has focused mainly on consumer and communications technologies, including smartphones and tablet computers. Such devices, he writes, are “smaller, smarter and more capable, but do not fundamentally change labor productivity or the standard of living” in the way that electric lighting or the automobile did.

But others say such pessimism misses the next wave of technology. “The reason I think Bob Gordon is wrong is precisely because of the kind of thing G.E. is doing,” said Andrew McAfee, principal research scientist at M.I.T.'s Center for Digital Business.

Today, G.E. is putting sensors on everything, be it a gas turbine or a hospital bed. The mission of the engineers in San Ramon is to design the software for gathering data, and the clever algorithms for sifting through it for cost savings and productivity gains. Across the industries it covers, G.E. estimates such efficiency opportunities at as much as \$150 billion.

Some industrial Internet projects are already under way. First Wind, an owner and operator of 16 [wind farms](#) in America, is a G.E. customer for wind turbines. It has been experimenting with upgrades that add more sensors, controls and optimization software.

The new sensors measure temperature, wind speeds, location and pitch of the blades. They collect three to five times as much data as the sensors on turbines of a few years ago, said Paul Gaynor, chief executive of First Wind. The data is collected and analyzed by G.E. software, and the operation of each turbine can be tweaked for efficiency. For example, in very high winds, turbines across an entire farm are routinely shut down to prevent damage from rotating too fast. But more refined measurement of wind speeds might mean only a portion of the turbines need to be shut down. In wintry conditions, turbines can detect when they are icing up, and speed up or change pitch to knock off the ice.

Upgrades on 123 turbines on two wind farms have so far delivered a 3 percent increase in energy output, about 120 megawatt hours per turbine a year. That translates to \$1.2 million in additional revenue a year from those two farms, Mr. Gaynor said.

“It’s not earthshaking, but it is meaningful,” he said. “These are real commercial investments for us that make economic sense now.”

For the last few years, G.E. and Mount Sinai Medical Center have been working on a project to optimize the operations of the 1,100-bed hospital in New York. Hospitals, in a sense, are factories of health care. The challenge for hospitals, especially as cost pressures tighten, is to treat more patients more efficiently, while improving the quality of care. Technology, said Wayne Keathley, president of Mount Sinai, can play a vital role.

At Mount Sinai, patients get a black plastic wristband with a location sensor and other information. Similar sensors are on beds and medical equipment. An important advantage,

Mr. Keathley said, is to be able to see the daily flow of patients, physical assets and treatment as it unfolds.

But he said the real benefit was how the data could be used to automate and streamline operations and then make better decisions. For example, in a typical hospital, getting a patient who shows up in an emergency room into an assigned bed in a hospital ward can take several hours and phone calls.

At Mount Sinai, G.E. has worked on optimization and modeling software that enables admitting officers to see beds and patient movements throughout the hospital, to help them more efficiently match patients and beds. Beyond that, modeling software is beginning to make predictions about likely patient admission and discharge numbers over the next several hours, based on historical patterns at the hospital and other circumstances — say, in flu season.

The software, which Mount Sinai has been trying out in recent months, acts as an intelligent assistant to admitting officers. “It essentially says, ‘Hold off, your instinct is to give this bed to that guy, but there might be a better choice,’ ” Mr. Keathley explained.

At a hospital like Mount Sinai, G.E. estimates that the optimization and modeling technologies can translate into roughly 10,000 more patients treated a year, and \$120 million in savings and additional revenue over several years.

The origins of G.E.’s industrial Internet strategy date back to meetings at the company’s headquarters in Fairfield, Conn., in May 2009. In the depths of the financial crisis, Jeffrey R. Immelt, G.E.’s chief executive, met with his senior staff to discuss long-term growth opportunities. The industrial Internet, they decided, built on G.E.’s strength in research and could be leveraged across its varied industrial businesses, adding to the company’s revenue in services, which reached \$42 billion last year.

Now G.E. is trying to rally support for its vision from industry partners, academics, venture capitalists and start-ups. About 250 of them have been invited to a conference in San Francisco, sponsored by the company, on Thursday.

Mr. Immelt himself becomes involved in recruiting. His message, he says, is that if you want to have an effect on major societal challenges like improving health care, energy and transportation, consider G.E.

An early convert was William Ruh, who joined G.E. from Cisco, to become vice president in charge of the software center in San Ramon. And Mr. Ruh is taking the same message to high-tech recruits like Ms. Paul. “Here, they are working on things they can explain to their parents and grandparents,” he said. “It’s not a social network,” even if the G.E. projects share some of the same technology.

Annexe 4 : [Making the Internet of Things a Reality : Mobility meets Big Data in the Cloud – “Triple Word Score”!](#)

Source : [Sanjay Poonen's Blog](#), directeur de la mobilité et de l'innovation chez SAP, 1^{er} octobre 2012

One aspect of working for a global company that I don't care for are 5am conference calls with Europe. But what's even more frustrating is waking up to my alarm clock at 4:30 am only to discover that the 5 am call was cancelled overnight. Well, what if my calendar could talk to my alarm clock across the Internet? The cancelled meeting would trigger my alarm clock being set back an hour, allowing me to sleep a little longer. Now imagine what my morning would be like if all of the devices in my life were synched together. The meeting cancellation resets not only my alarm clock but the coffee machine as well. Additionally, my mobile device receives a notification from my car that I'm low on gasoline. I'm informed that the trains are running 15 minutes late, and there's 10 minutes of crowded traffic on my route to the train station. All that information is fed back to my alarm clock (and coffee machine for that matter) via the Internet.

At the end of the day, on my walk to the train station, my phone receives a notification from my refrigerator that I'm low on milk and a grocery store that I'm passing has a promotion for milk (and by the way, my favorite yogurt). I'm directed via location awareness right to the aisle where the milk and yogurt are stocked, and through precision retailing, a personalized coupon for 50% discount on the yogurt is sent to my mobile device.

Here's another scenario. When my family goes on a ski trip to Tahoe, my wife and I disagree about whether to turn our home heating on or off. She wants the house warm for our kids when we return; I want to save energy. Well, what if we turned off the thermostat, but on our return drive an hour away from home, I use my phone to direct an Internet-enabled thermostat to turn the heat up in my home!

These might all seem like scenes from “Back to the Future”, but much of this is increasingly possible via what is known as the Internet of Things (IoT) and the intelligent sharing of information between Machine-to-Machine (M2M). Basically, four key elements are required for IoTs – a) Tagging Things b) Sensing Things c) Shrinking Things and d) Thinking Things. With advances in RFID, miniaturization and analytics, M2M makes the Internet of Things an increasingly tangible possibility. Think of such M2M communication as the “social collaboration” of machine-to-machine or machine-to-man.

Such technology is beginning to mature, whether it's smart thermostats from startups like Nest Labs or Honeywell, or what's being called “precision retailing”, where innovations in Big Data Analytics, combined with Mobility and GPS, allow tailored promotions to be offered to consumers on their mobile devices. One of our automotive customers once told me that there's more software in the modern car than in the first space shuttle! I learned from our manufacturing customers that if you thought today's tractors are dumb, quite the contrary, they stream all kinds of information like an Airbus 380 might, so that farmers can optimize usage, schedule maintenance and focus their time on agricultural production. Consumer companies are exploring smart vending machines that have tiny computers on a wireless network which leverage information like usage data and weather forecasts to determine replenishment schedules. If you know it's going to be a hot day, being able to get your trucks to the vending machine fast enough might be the difference in a breakout profitable quarter.

We look at all of these machines, whether wired or unwired, and see them as extensions of mobile devices; they all need to be secured, managed, and enabled to run applications in much the same way as a mobile phone. Managing this smart machine to machine (M2M) evolution requires a comprehensive architecture and technology solutions that we're working on with our partners. But at the core of M2M are three key elements: Mobility, Big Data and the Cloud. These are precisely the focus areas that we've designated as innovation vectors at SAP. And when these three elements come together in use cases like the "Internet of Things" or "Machine-2-Machine", it's like getting a "Triple Word Score" in the game of Scrabble !

So... how does SAP's Mobile Management solution fit into this vision? Stay tuned for my next blog to find out the answer !

Annexe 5 : Questionnaire pour les attachés douaniers

CGEIET – 11 mai 2012

“La logistique transfrontière et les technologies de l’Internet appliquées aux objets”.

Introduction

Le Conseil général de l’économie, de l’industrie, de l’énergie et des technologies réalise, dans le cadre d’une mission de conseil au profit de la direction générale des douanes et droits indirects, une enquête sur le recours aux technologies de l’Internet des objets dans le domaine des activités douanières.

Le présent questionnaire a pour but de mieux connaître :

- dans les domaines qui intéressent la Douane ;
- la situation et les projets ;
- concernant l’usage des applications ou des technologies issues ou connexes à l’Internet des objets.

Les domaines qui intéressent la Douane directement ou pour d’autres administrations sont :

- le contrôle des obligations des opérateurs économiques agréés et des plate-forme logistiques ;
- la vérification de la permanence de l’intégrité des objets et/ou de leurs contenants ;
- la réalisation des formalités administratives dans le régime du guichet unique ;
- la vérification des règles de protection ;
- la lutte anti-contrefaçon (via notamment l’authentification des objets, l’ADN des objets,
- l’objet-preuve...).

Les systèmes et les technologies concernés sont celles issues de l’Internet ou de l’Internet des objets ainsi que les technologies connexes - marquage des objets, traçabilité, etc.

Nous nous intéressons aux évolutions à l’horizon de 5 / 7 ans.

Les résultats globaux seront restitués aux attachés, en même temps qu’une enquête prospective, en liaison avec la Direction des relations internationales de la DGDDI.

N’hésitez pas à demander des précisions à :

- | | |
|--------------------------------|---|
| - Jean-Pierre Dardayrol | jean-pierre.dardayrol@finances.gouv.fr |
| - Claudine Duchesne | claudine.duchesne@finances.gouv.fr |
| - Loïc Lenoir de la Cochetière | loic.lenoir-de-la-cochetiere@finances.gouv.fr |

1) Le pays où vous êtes en poste dispose d'un plan ou des projets de développement de l'Internet des objets, doté d'une gouvernance et de ressources.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pouvez-vous expliquer les points forts et faibles de ce plan :

2) Ce plan ou ces projets concernent les volets fonctionnels suivants :

	Existence oui/non	Description succincte : nom, finalités, porteurs, moyens, horizon, ...
La logistique transfrontière et les opérations douanières		
La logistique à longue distance		
Les plates-formes aéroportuaires		
Les plates-formes maritimes		
La logistique urbaine		
Les contrôles administratifs - internes ou aux frontières		
La vérification des fraudes ou les contrôles sanitaires		
L'intégrité des marchandises - contenus ou contenants		
La lutte anti-contrefaçon		
La fiscalité - accises, TVA, taxes locales, ...		

Autres, à préciser		
--------------------	--	--

3) Ce plan ou ces projets concernent principalement les secteurs suivants :

	Pilotes	Projets de déploiement large	Caractéristiques
L'agro-alimentaire			
Les alcools et/ou le tabac			
La pharmacie			
L'automobile et/ou l'aéronautique			
Le luxe			
Autres à préciser			

4) Ce plan ou ces projets contiennent des projets de R&D ou des pilotes dans les domaines suivants :

	Projet de R&D oui/non	Pilotes oui/non	Grandes caractéristiques
L'intégration des systèmes multi-acteurs			
Les logiciels de gestion de plates-formes ou d'entreprises			
Les identifiants d'objets - contenants ou contenus			

Les identifiants et/ou les étiquettes			
L'architecture ou les protocoles de l'Internet des objets			

5) *A quelle autre question souhaiteriez-vous répondre ?*

Annexe 6 : Réponse des douanes de Singapour

11 May 2012

Questionnaire for Singapore Customs:

“Cross-Border Logistics and the Internet of Things Technologies”

Introduction

As part of a mission to advise the Directorate General of Customs and Excise (DGDDI), the General Council for the Economy, Industry, Energy and Technologies (Ministry of Finance) is carrying out a survey on the use of Internet of Things technologies in the field of customs work.

The aim of this questionnaire is to reach a better understanding, in fields of interest to Customs authorities, of the current situation and projects involving the use of applications or technologies derived from or related to the Internet of Things.

The fields that are of direct interest to the Customs authorities or other administrations include :

- Monitoring authorised economic operators' and logistics platforms' compliance with obligations
- Verifying the continuing integrity of objects and/or their contents
- Carrying out administrative formalities using the one-stop-shop approach
- Verification of compliance with protection rules
- Anti-counterfeiting operations (particularly via object authenticity, object DNA and objects used as legal evidence)

The systems and technologies concerned are those derived from the Internet or the Internet of Things, as well as related technologies – object markers, traceability, etc.

We are interested in developments with a 5- to 7-year horizon.

1) The country has a plan or a project for developing the Internet of Things, which has been provided with a management structure and resources.

	Agree strongly	Agree fairly strongly	Disagree fairly strongly	Disagree strongly
Do you agree with this statement?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please explain the strong and weak points of this plan:

2) The plan or project concerns the following functional areas :

	Exists yes/no	Brief description: name, goals, sponsors, resources, timeline, etc.
Cross-border logistics and customs operations	Yes	<p><u>TradeXchange</u> TradeXchange aims to be a neutral and secure platform that enables businesses to seamlessly exchange information across the supply chain. Through consultation with the industry, 3 integrated solutions were implemented on TradeXchange :</p> <ul style="list-style-type: none"> - Marine Cargo Insurance Chain where it enables businesses to save up to 90% of the time from its marine cargo insurance application; - Trade Finance Chain where it enables businesses to obtain factoring approval from bank faster and at lower rate; and - Trade Permit Chain it enables businesses to shorten its permit preparation process up to 50% of the time <p>Through TradeXchange, businesses will enjoy greater operational efficiencies, clearer supply chain visibility, faster shipment turnaround and productivity due to more timely exchanges of information and documents with their partners in the value chain. URL : TradeXchange Status : Live</p>
Long-distance logistics	Yes	<p><u>CASSANDRA – Living Lab 1 (Asia-Europe)</u> The objective of the CASSANDRA project is to enhance supply chain security through the sharing of trade data across end-to-end supply chain. Singapore Customs’ participation in the CASSANDRA Living Lab 1 project is to establish and pilot a seamless integrated data pipeline solution between Singapore and the Netherlands. The integration will be through Singapore’s TradeXchange and the Dutch port community system Portbase. A dashboard will be developed in the project CASSANDRA that will help visualize the data exchange among the businesses across the supply chain. Status : Development.</p>

Hub airports	Yes	<p><u>e-freight@Singapore</u> e-freight@Singapore is a joint initiative between the Civil Aviation Authority of Singapore (CAAS) and Infocomm Development Authority of Singapore (IDA). This project seeks to inter-connect stakeholders in the air cargo logistics supply chain, such as shippers, air freight forwarders, airport ground handlers, airlines, consignees and related government agencies. Freight forwarders will benefit from the process integration. They will receive shipments data from the Shippers electronically, reducing the need to manually re-key in data for subsequent documentations. There will be significant improvements to accuracy and speed. URL: e-freight@Singapore Status : Development</p>
Maritime hubs	Yes	<p><u>See Cassandra Project under Long Distance Logistics</u></p>
Urban logistics	No	-
Administrative controls – internal or border-based	Yes	<p><u>Radio Frequency Identification (RFID) in Cargo Clearance Processing</u> Singapore Customs is exploring the use of RFID in tracking and monitoring of goods movement between Singapore and its neighbouring country. This will help reduce clearance time at the checkpoint, reduce human error in clearance processes, and improve supply chain visibility. Status : Exploratory Stage</p>
Fraud investigation or health checks	Yes	<p><u>Customs Intelligence and Investigation System (C2IS)</u> C2IS is Singapore Customs’ next generation enforcement system. It aims to provide a one stop system for all enforcement activities, which include providing full paperless Investigation Papers online, aggregating entity information across the enterprise, and tracking of physical objects within the organisation. Status : Procurement Stage</p>
Integrity of goods – contents or containers	Yes	<p><u>Business Analytics in Cargo Risk Profiling</u> Singapore Customs is in the midst of conducting a Business Analytics consultancy study to review and identify opportunities where analytics can improve data analysis and risk profiling process. Status : Exploratory Stage</p>

Anti-counterfeiting operations	Yes	See C2IS Project under Fraud Investigation
Taxation – excise, VAT, local taxes, etc.	Yes	Revenue Management System Singapore Customs is looking into revamping the existing Revenue Management System, with focus on building and enhancing capabilities in the areas of revenue collection, debt management, case and performance management. Status : Exploratory Stage
Other (please specify)	Yes	Exploring :- 1) Cloud Computing 2) Mobile Services 3) Track and Trace 4) Intelligent Search

3) The plan or project concerns primarily the following sectors :

	Pilot phase	Large-scale projects	Characteristics
Agri-food			
Alcohol and/or tobacco			
Pharmaceuticals			
Automotive and/or aerospace		e-freight@Singapore Programme	See above
Luxury goods			
Other (please specify)			

4) This plan or project contains R&D projects or a pilot phase in the following areas :

	R&D project yes/no	Pilot phase yes/no	Main characteristics
Combining multi-stakeholder systems	No	Yes	<ul style="list-style-type: none"> • e-freight@Singapore • TradeXchange
Platform or business management software	No	Yes	<ul style="list-style-type: none"> • TradeXchange
Object identifiers – containers or contents	No	Yes	<ul style="list-style-type: none"> • RFID / GPRS tracking
Identifiers and/or labels	No	No	
Architecture or protocols for the Internet of Things	No	No	

5) Which other question would you like to answer ?

Annexe 7 : Liste des organismes rencontrés ou interrogés

DGDDI
OMD (Org. mond. des douanes)
Douane US
Douane Singapour
Douane NL
Douane UK
Douane Allemagne
Ministère de l'Intérieur
Gendarmerie
DGCIS
ADP
AFNET
ARJO SECURITY
ATOS
AXA
BONGRAIN
BRINK'S
CASSIDIAN (Gr. EADS)
CEA-LETI
CITE ON LINE
CNRFID
EDITAG
ENSME
Expert Fédé. Du cuir
Expert technologies anti-contrefaçon
Expert-Avocat TIC
Expert (JSCP)
GITEP
GS1
GYPTIS
IBM
IM2NP
INSA Rouen
INSIDE
ITEMS
KEYNECTIS
LUSIS
MGI
MICROSOFT
Mines Paris
MORPHO (Gr.SAFRAN)
ORANGE
ORIDAO
POSTE/GEOPOST
SAFRAN
SAP
SCHNEIDER ELECTR
SCS
SECF
SIGNOPTIC (Gr. ARJO)
SOGET Marseille
TAGSYS
THALES
UNIFAB
USTV Toulon
VALEO
WAITO Fondat.
WCO

Annexe 8 : Questionnaire – Version française

Ministère de l'économie, des finances et du commerce extérieur
CGEIET – 11 mai 2012

Questionnaire à retourner à : jean-pierre.dardayrol@finances.gouv.fr ou loic.lenoir-de-la-cochetiere@finances.gouv.fr, pour le 30 juin 2012.

Invariants et alternatives pour des scénarios d'appropriation des technologies de l'internet des objets par les logisticiens transfrontières et les services de Douane

Introduction

Le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies réalise, dans le cadre d'une mission de conseil au profit de la direction générale des douanes et droits indirects, une enquête sur le recours aux technologies de l'Internet des objets dans le domaine des activités douanières.

Le présent questionnaire a pour but de mieux cerner "à dire d'experts",

- dans les domaines qui intéressent la Douane,
- les points de consensus et les points de divergences ou d'incertitude,
- concernant l'usage des applications ou des technologies issues ou connexes à l'Internet des objets.

Les domaines qui intéressent la Douane directement ou d'autres administrations sont,

- le contrôle des obligations des opérateurs économiques agréés et des plates-formes logistiques,
- la vérification de la permanence de l'intégrité des objets et/ou de leurs contenants (traçabilité et identité),
- la réalisation des formalités administratives dans le régime du guichet unique,
- la vérification des règles de protection,
- la lutte anti-contrefaçon (authenticité de l'objet).

Les systèmes et les technologies concernés sont ceux issus de l'Internet ou de l'Internet des objets ainsi que les technologies connexes - ADN de l'objet, marqueurs chimiques, variables ou non, objets-preuves, etc.

Nous nous intéressons aux évolutions à l'horizon de 5 / 7 ans.

Le questionnaire est structuré en deux parties :

- les évolutions générales d'une part,
- les applications aux métiers douaniers,
- précédées d'une caractérisation du métier du répondant, d'autre part.

L'enquête est itérative : les participants recevront les réponses à un "premier tour de questionnaire" et pourront, le cas échéant, modifier leurs réponses et les justifier.

Le questionnaire s'adresse aux responsables exécutifs des entreprises et des administrations concernées ainsi qu'aux experts.

Il est fermé au sens où il sera adressé à des personnes physiques ou morales préidentifiées - notamment sur recommandation des participants.

Les réponses peuvent concerner, au choix du répondant, tout ou partie du questionnaire.

Les réponses individuelles resteront anonymes ; les résultats globaux seront adressés aux participants et présentés lors d'une table ronde.

N'hésitez pas à demander des précisions à :

- Jean-Pierre Dardayrol jean-pierre.dardayrol@finances.gouv.fr
- Claudine Duchesne claudine.duchesne@finances.gouv.fr
- Loïc Lenoir de la Cochetière loic.lenoir-de-la-cochetiere@finances.gouv.fr

Questionnaire

Votre métier - en deux questions :

Vous êtes :

- un fabricant
- un négociant
- un professionnel de la logistique
- un professionnel de la sécurité
- un professionnel des systèmes d'information ou de l'Internet
- un agent de la Douane ou d'une administration
- un acteur de la R&D ou un universitaire
- autres (à préciser)

Vous êtes :

- un "exécutif" (acteur)
 - . concepteur de technologies ici étudiées
 - . utilisateur avéré ou potentiel d'une ou plusieurs de ces technologies
- Dans ce dernier cas, vous êtes :
 - . industriel
 - . négociant
 - . prestataire de services (conditionneur, affrêteur, entreposeur, transporteur, etc.)
- un expert

Avez-vous été victime d'un mal auquel les technologies ici évoquées pourraient, du moins le pensez-vous, répondre :

- contre-façon ;
- détournement de trafic ;
- autres (précisez).

1 - Les grandes tendances du marché

Nous aborderons tout d'abord les évolutions globales de la logistique et de sa sécurité en lien avec les technologies de l'Internet appliquées aux objets à l'horizon de 5 / 7 an.

Dans cette perspective, nous souhaiterions avoir votre avis sur 17 questions ; il peut être répondu à un sous-ensemble des questions et/ou ajouter une dernière question libre.

D'ici 5 à 7 ans, selon vous,

*1) un grand nombre d'applications "internet" concernant les **objets** et reposant sur leur identification seront utilisées dans le secteur de la logistique et/ou de leur sécurité.*

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

*2) un grand nombre d'applications "internet" concernant les **contenants** des objets et reposant sur leur identification seront utilisées dans le secteur de la logistique et/ou de leur sécurité ?*

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

3) les contraintes environnementales pesant sur la logistique urbaine remodeleront l'ensemble du secteur de la logistique

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

4) les applications pour les domaines de la logistique urbaine et de la logistique à longue distance auront convergé.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

5) les solutions mises en oeuvre en Europe, en Asie et en Amérique du nord seront ouvertes et interoperables.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

6) les objets et les contenants seront identifiés de façon unique et universelle.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

7) il existera un Internet des objets ouvert dont l'architecture et les protocoles feront l'objet d'un large consensus.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

8) l'infrastructure dominante sera celle de l'Internet des objets, complétée par des intranets et des extranets fermées et spéciales à certaines catégories d'objets - armes, organes humains, etc.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

9) les problèmes de sécurité relatifs à des applications pour les objets et leur logistique auront été résolus et ne constitueront plus un obstacle au développement de l'Internet des objets ou d'intranets spécialisés.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

10) les problèmes de protection de la vie privée relatifs à des applications pour les objets et leur logistique auront été résolus et ne constitueront plus un obstacle au développement de l'Internet des objets ou d'intranets spécialisés.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

11) les problèmes de position dominante (tant en termes de prix que d'exploitation détournée des informations recueillies) relatifs à des applications pour les objets et leur logistique auront été résolus et ne constitueront plus un obstacle au développement de l'Internet des objets ou d'intranets spécialisés.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

12) la gamme des identifiants industriellement disponibles pour les objets et les contenants aura été simplifiée et fera l'objet d'un large consensus.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

13) le marché aura suscité un corpus "satisfaisant" de standards sur tous les segments des systèmes d'information et de communication.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

14) les obligations réglementaires internationales ou européennes concernant les objets - sécurité, fiscalité, protection de l'environnement, des consommateurs, etc. - seront compatibles et permettront la mise en place de systèmes d'information "communs" et de guichets uniques.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

15) les intégrateurs de systèmes, les éditeurs de logiciels et les différents industriels coopéreront pour offrir des solutions "clés en main", économiquement compétitives.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

16) en France, il n'y aura pas de "goulet d'étranglement" - ressources humaines, cadre juridique, ... - limitant le déploiement de solutions.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

17) les technologies seront communes permettant traçabilité, identification et authentification des objets.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

18) A quelle autre question souhaiteriez-vous répondre ?

2 - Les domaines douaniers

Dans cette partie, on s'intéresse aux conditions dans lesquelles les technologies de l'Internet appliquées aux objets modifieront les métiers et les processus dans les domaines douaniers. Sept questions sont abordées ; il peut être répondu à un sous-ensemble des questions et/ou ajouter une dernière question libre.

D'ici 5 à 7 ans, selon vous,

1) le contrôle des obligations des opérateurs économiques agréés et des plates-formes logistiques inclura en tant qu'élément fondamental une vérification de la capacité de ces opérateurs et de ces plates-formes à utiliser les technologies de l'Internet appliquées aux objets.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

2) la vérification de l'intégrité des objets et/ou de leurs contenants sera largement systématisée et reposera fréquemment sur l'utilisation de systèmes incluant des technologies de l'Internet.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

3) la réalisation des formalités administratives dans le régime du guichet unique et la vérification des règles de protection - protection de l'environnement et des consommateurs, ... - reposera principalement sur des systèmes incluant des technologies de l'Internet.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

4) la lutte anti-contrefaçon reposera sur des systèmes souvent fermés propres à chaque titulaire de droit.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

5) la lutte anti-contrefaçon reposera sur l'utilisation de systèmes incluant des technologies de l'Internet.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

6) en France, la Douane ne rencontrera pas de difficultés à mobiliser les ressources nécessaires à l'évolution de ses activités - ressources humaines, réglementation, ressources budgétaires, systèmes d'information, partenariats industriels, etc.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

7) en France, les autres administrations et collectivités publiques concernées - répression des fraudes, services vétérinaires, ... - ne rencontreront pas de difficultés à mobiliser les ressources nécessaires à l'évolution de leurs activités - ressources humaines, réglementation, ressources budgétaires, partenariats industriels, etc.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

7) la Douane aura été amenée à modifier de façon importante ses systèmes d'information.

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas d'accord du tout
Êtes-vous d'accord avec cette assertion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Si en désaccord (plutôt pas d'accord ou pas du tout d'accord), pouvez-vous expliquer ?

9) A quelle autre question souhaiteriez-vous répondre ?