L'Internet des objets

Briefing sur les affaires publiques de l'Internet Society

2 Août 2016

Introduction

L'Internet des objets est un terme général utilisé pour décrire des situations dans lesquelles la connectivité Internet et les capacités de calcul sont associées à des appareils, capteurs et objets de tous les jours qui ne sont pas considérés habituellement comme des ordinateurs (par exemple, biens de consommation, voitures et camions, composants industriels, moniteurs de santé portatifs et de nombreux appareils travaillant ensemble pour créer des concepts tels que « villes intelligentes » et « maisons intelligentes »). Ces objets collectent des données de leur environnement qui sont ensuite transmises et analysées à distance pour créer de nouvelles idées, fournir des services et contrôler d'autres éléments.

Les projections de l'impact de l'IoT sur l'Internet ainsi que sur l'économie sont impressionnantes : jusqu'à 100 milliards d'appareils connectés de type IoT[1] et un impact économique mondial de plus de 11 billions USD en 2025[2]. L'IoT promet des avances en automatisation industrielle, soins de santé, conservation de l'énergie, agriculture, transports, gestion urbaine ainsi que de nombreux autres secteurs et applications. Le potentiel d'une croissance vertigineuse dans l'innovation, les applications et les services constitue une reconnaissance de la nature ouverte de l'architecture et la conception de l'Internet qui ne pose de limite ni aux types d'appareils ni aux services qui peuvent s'y connecter.

En même temps, toutefois, il reste des difficultés significatives associées à l'IoT qui peuvent faire obstacle à la réalisation de ses bénéfices potentiels. Quelques-unes des difficultés et questions les plus urgentes comprennent des questions de sécurité, confidentialité, interopérabilité et de normes, de même que des questions de règlements et de droit sans oublier la préparation des économies émergentes à l'adopter.

Cette note offre une vue d'ensemble des questions clés liées à l'IoT. Ces mêmes questions sont discutées de manière plus approfondie dans le rapport de l'Internet

Souvent désigné en tant qu'*Internet des objets (IoT),* des milliards d'appareils intelligents devraient apparaître en ligne dans les dix prochaines années, apportant avec eux la promesse d'opportunités économiques mondiales et de futures innovations qui vont transformer la façon dont nous travaillons, vivons et jouons. Toutefois, les difficultés associées à l'IoT, y compris la sécurité et la confidentialité, doivent être prises en compte pour que la technologie atteigne son plein potentiel.

1 « Index de Connectivité Globale. » Technologies Huawei Co., Ltd., 2015. Web. 6 septembre 2015. http://www.huawei.com/minisite/gci/en/index.html.
2 Manyika, J. ; Chui, M. ; Bisson, P. ; Woetzel, J. ; Dobbs, R. ; Bughin, J. ; et Aharon, D. " L'Internet des Objets : Déterminer la valeur au-delà de l'engouement. " McKinsey Global Institute, Juin 2015.

Society, *L'Internet des choses : une vue d'ensemble – Comprendre les problèmes et défis d'un monde plus connecté*.

Principales considérations

Bien que l'intérêt dans les objets connectés ait décollé dans les dernières années, le concept de la connexion d'objets et éléments aux réseaux de communication et à l'Internet n'est pas nouveau. Les systèmes de communication entre machines (M2M), qui utilisent des réseaux propriétaires plutôt que l'Internet se sont développés largement dans les environnements industriels il y a plus de 25 ans. Les premiers objets quotidiens contrôlés par l'Internet sont apparus au début des années 90 et ont ouvert la voie à l'Internet des objets d'aujourd'hui.

Aujourd'hui, l'IoT représente un aspect croissant de la façon dont les personnes et les institutions interagissent avec l'Internet dans leurs vies personnelles, sociales et économiques. Il peut aussi représenter un changement dans la façon dont les utilisateurs collaborent et sont influencés par l'Internet. Par exemple, l'expérience aujourd'hui de l'utilisation de l'Internet est largement caractérisée par des utilisateurs qui téléchargent activement et génèrent du contenu par leur ordinateur et smartphone. De nombreux appareils de l'IoT, toutefois, sont conçus pour fonctionner en arrière-plan, en envoyant et recevant des données au nom de l'utilisateur avec peu d'intervention humaine ou même sans que l'utilisateur en soit conscient ; d'autres encore sont conçus pour contrôler des objets et des biens dans le monde tels que des véhicules et des bâtiments, ou pour veiller sur le comportement humain.

Si les projections et les tendances de l'IoT deviennent réalité, nous serions sages de considérer les implications d'un monde dans lequel les interactions les plus courantes avec l'Internet proviennent d'un engagement passif avec des objets connectés, plutôt que d'un engagement actif avec du contenu. Les gouvernements, par exemple, veulent s'assurer que leurs politiques restent en contact avec l'environnement qui change rapidement.

Les politiques qui font la promotion de l'infrastructure de l'Internet, l'usage efficace d'un réseau sans fil, du développement des centres de données ainsi que de la responsabilisation et le choix de l'utilisateur sont cruciales pour l'évolution de l'IoT. Et comme la somme et la nature des données collectées sur les utilisateurs et leur environnement passent par l'IoT, les politiques de confidentialité et de sécurité des données doivent être considérées pour faire face à l'évolution de la technologie et ses impacts potentiels sur les utilisateurs.

Au-delà des aspects de l'IoT concernant les infrastructures directes et les télécommunications, d'autres domaines politiques peuvent bénéficier d'une révision. Les appareils de l'IoT vont probablement toucher la plupart des aspects de notre vie, y compris des appareils pour nos maisons, lieux de travail, écoles, hôpitaux et autres espaces publics. Comme telles, les politiques de confidentialité, sécurité des données, santé, transports et les politiques de technologie et d'innovation seront vraisemblablement touchées. Cette large portée suggère que les responsables politiques auront besoin de considérer de larges implications en termes de politiques dans un vaste champ d'objectifs et d'initiatives politiques.

Bien que l'IoT ne soit pas une idée particulièrement nouvelle d'un point de vue technique, sa croissance et sa maturité présenteront à la fois de nouveaux bénéfices et de

nouveaux défis qui demanderont un changement dans les approches et les stratégies en ce qui concerne les politiques.

Difficultés

Un nombre de difficultés doit être réglé pour que les bénéfices potentiels de l'IoT soient pleinement réalisés pour les personnes, les sociétés et les économies.

- **Sécurité.** Bien que les préoccupations liées à la sécurité ne soient pas une nouveauté dans les technologies de l'information, les attributs de nombreuses implémentations de l'IoT présentent de nouveaux et uniques défis en termes de sécurité.

  Les fabricants rencontrent fréquemment des difficultés économiques et techniques en construisant et entretenant des fonctionnalités de sécurité robustes dans les appareils de l'IoT. Mais les appareils et les services possédant une sécurité faible sont vulnérables à des cyberattaques et peuvent exposer les utilisateurs à un vol de données. Parce qu'un nombre sans cesse croissant d'appareils en ligne augmente le nombre de vulnérabilités potentielles de sécurité, c'est une difficulté clé de l'IoT.

  Garantir une sécurité à vie des produits et des services de l'IoT doit être une priorité fondamentale pour conserver la confiance générale des utilisateurs dans cette technologie. Les utilisateurs doivent avoir confiance dans le fait que les appareils de l'IoT et les services de données liés sont sécurisés et intégrés dans notre vie quotidienne.

  En principe, les développeurs et les utilisateurs d'appareils et systèmes de l'IoT ont une obligation collective pour garantir qu'ils n'exposent pas les utilisateurs et l'Internet lui-même à des dommages potentiels. Les actions de l'industrie, des gouvernements, des utilisateurs et d'autres contribueront à sécuriser le développement, l'entretien et l'utilisation des appareils de l'IoT.

  L'Internet Society croit qu'une approche collaborative à la sécurité de l'IoT sera nécessaire au développement de solutions efficaces et appropriées qui soient bien adaptées à l'échelle et la complexité des problèmes.

- **Confidentialité.** De la possibilité de collecter, analyser et transformer les données dérive la plupart de la valeur des appareils et services de l'IoT, mais ces données peuvent aussi être utilisées pour croquer des profils détaillés et invasifs des utilisateurs. En effet, l'IoT redéfinit le débat sur les questions de confidentialité, parce que de nombreuses implémentations peuvent changer de manière spectaculaire la façon dont les données sont collectées, analysées et utilisées.

  Spécifiquement, l'IoT amplifie les soucis sur l'augmentation potentielle de surveillance et de suivi, et la somme de données sensibles qui peut être collectée par les appareils fonctionnant dans nos maisons, nos entreprises et les environnements publics. Quelquefois ces appareils collectent des données sur les particuliers sans qu'ils en aient connaissance ou qu'ils aient donné leur consentement informé. De plus, pendant que les données de ces appareils bénéficient au propriétaire de l'appareil, les mêmes données bénéficient aussi fréquemment au fabricant et au fournisseur. Ceci devient une véritable

préoccupation de confidentialité quand les particuliers qui sont observés par des appareils de l'IoT attendent une confidentialité différente que les collecteurs de ces mêmes données en ce qui concerne l'utilisation et la portée de leurs données.

Les appareils de l'IoT qui collectent les données sur les personnes dans une juridiction peuvent transmettre des données dans une autre juridiction pour leur stockage ou leur traitement. Des difficultés peuvent survenir si les données collectées sont jugées personnelles ou sensibles et sont soumises aux lois sur la protection des données dans de multiples juridictions.

Rendre possible la circulation de données à travers les frontières tout en protégeant la confidentialité et promouvant une certitude légale pour les utilisateurs et les fournisseurs de services de l'IoT sera la clé pour la promotion d'une croissance globale de l'IoT.

Bien que les défis de confidentialité soient considérables, ils ne sont pas insurmontables. Il convient de développer des stratégies qui favorisent la transparence, l'équité et le choix des utilisateurs dans la collection et le maniement des données, améliorent le droit à la confidentialité et les attentes des utilisateurs dans une large gamme de préférences et stimulent l'innovation dans les nouvelles technologies et les services.

- **Interopérabilité et normes.** L'interopérabilité parmi les appareils de l'IoT et les flux de données peut encourager l'innovation et procurer un rendement accru aux fabricants d'appareils et aux utilisateurs, augmentant par cela les bénéfices globaux et la valeur économique. McKinsey Global Institute estime que l'interopérabilité permettra d'augmenter jusqu'à 140 % la valeur potentielle générée par l'IoT.[3]

  Bien qu'une complète interopérabilité sur tous les produits et services ne soit pas toujours faisable ou nécessaire, les acheteurs peuvent hésiter à acquérir des produits et services de l'IoT s'ils présentent une rigidité d'intégration, une complexité de propriété, des jardins clos (plateformes ou écosystèmes fermés) et des inquiétudes sur les blocages réalisés par les vendeurs. L'interopérabilité et les considérations de normes s'étendent aussi aux données collectées et traitées par les services de l'IoT, car des formats de données propriétaires et incompatibles peuvent présenter des difficultés pour les utilisateurs recherchant des systèmes intégrés, ayant la souplesse de changer de service ou de pratiquer des analyses supplémentaires sur les données collectées. Bref, un environnement fragmenté d'implémentations propriétaires techniques et de formats de données[4] entravera la valeur de l'IoT et la souplesse pour les utilisateurs comme pour l'industrie.

  Le marché actuel offre une variété d'approches techniques à l'IoT. Certaines sociétés voient des avantages stratégiques à développer des écosystèmes propriétaires, alors que d'autres sont en train de développer leurs propres

3 ibid.
4 Pour une information sur les activités récentes du Détachement d'Ingénierie de l'Internet (IETF) et du Comité de l'Architecture de l'Internet (IAB) afin de promouvoir la standardisation et l'interopérabilité de l'IoT, voir https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf et https://www.iab.org/activities/workshops/iotsi/.

approches car des technologies communes n'existent pas encore. Une large gamme de sociétés, de groupes industriels et de chercheurs travaillent sur des approches qui créent une interopérabilité de l'IoT et des standards accrus.

L'Internet Society croit qu'une interopérabilité accrue et l'utilisation de standards génériques, ouverts, volontaires et largement disponibles en tant que blocs de construction techniques pour des dispositifs et des services de l'IoT (tel que le protocole Internet, ou IP) supporteront des bénéfices de l'usager, une innovation et une opportunité économique accrus.

- **Des questions réglementaires, légales, et de droits.** L'IoT amplifie et réintroduit de nombreuses questions réglementaires et légales. Il existe un danger que le rythme rapide des évolutions dans la technologie IoT puisse dépasser la capacité des structures politiques, légales et réglementaires associées à s'adapter.

  L'un de ces problèmes inclut le conflit potentiel entre la surveillance du maintien de l'ordre et les droits civils. Les dispositifs IoT offrent des bénéfices potentiels au maintien de l'ordre public, à la sécurité du public et à l'administration publique. Cependant, ils augmentent également les préoccupations potentielles concernant les droits civils et de l'homme en ce qui concerne l'omniprésence de la surveillance de la société, des utilisations secondaires de données par le gouvernement et d'un accès aux données à partir de dispositifs IoT personnels par le maintien de l'ordre ou comme évidences dans le cas d'actions légales, parmi d'autres questions difficiles.

  De plus, les dispositifs IoT posent des questions de responsabilité légale. Une question fondamentale est : Si quelqu'un est blessé du fait de l'action ou de l'inaction d'un dispositif IoT, qui est responsable ? La question est souvent compliquée, et dans bien des cas il n'existe pas suffisamment de jurisprudence pour soutenir une position. Étant donné que les dispositifs IoT fonctionnent d'une façon bien plus complexe que les produits autonomes, des scénarios à responsabilité bien plus complexe ont besoin d'être envisagés.

  Du fait du caractère large des défis régulateurs et politiques de l'IoT, une approche de gouvernance collaborative pour le développement des politiques qui s'appuie sur une contribution et une participation par une gamme de parties prenantes est nécessaire pour les meilleurs résultats.

- **Économie émergente et enjeux du développement.** L'IoT s'annonce très prometteur pour produire des bénéfices sociaux et économiques envers les économies émergentes et de développement dans des zones d'agriculture durable, de qualité et d'utilisation de l'eau, de soins de santé, d'industrialisation, de surveillance du climat et de gestion environnementale.

  Par exemple, des réseaux de capteurs aident villageois et chercheurs en Asie et en Afrique à améliorer la fourniture en eau salubre en surveillant la qualité de l'eau à sa source et la performance des pompes de distribution. De plus, des moniteurs du sol sans fil, du climat, et du bétail et un équipement pour l'agriculture automatisé par IoT ont été déployés dans des régions en voie de

développement pour aider des fermiers à améliorer la productivité.[3] Par ces mesures et bien d'autres, l'IoT s'annonce très prometteur en tant qu'outil pour atteindre les Objectifs du Développement Durable des Nations Unies.[4]

Les régions en voie de développement présentent également des défis uniques liés au déploiement, à la croissance, à la mise en œuvre et à l'utilisation de la technologie. Ces défis comprennent le déploiement d'un Internet adéquat et d'infrastructures de communication basiques dans des zones rurales et éloignées, des incitations pour l'investissement et une participation locale dans le développement de solutions liées à l'IoT. Pour faire en sorte que les bénéfices liés à l'IoT soient réellement globaux, les besoins et défis uniques de mise en œuvre dans des régions moins développées devront être résolus.

Principes directeurs

Du fait de l'adoption anticipée de dispositifs IoT, ses potentiels bénéfices économiques et sociétaires, et défis associés, une prise de conscience accrue du secteur public de la technologie et de l'importance des problèmes les entourant est essentielle. Les gouvernements sont instamment priés de suivre les étapes suivantes pour accommoder et soutenir le déploiement de l'IoT.

- **Promouvoir la croissance des infrastructures liées à l'Internet et aux données.** Les gouvernements doivent promouvoir à la fois l'expansion des infrastructures sans fil et filaires, y compris dans des zones rurales et éloignées, et considérer les besoins à la fois d'une utilisation du spectre avec licence et sans licence. Des barrières au développement de centres de données et de systèmes basés sur l'utilisateur pour l'analyse de données, telles que de lourdes taxes sur les équipements ou des besoins de permis, devraient être éliminées. Les gouvernements devraient revoir leurs infrastructures existantes de l'Internet à la lumière des besoins potentiels en communication de données plus larges de dispositifs IoT.

- **Favoriser le déploiement de l'IPv6.** IPv6 est une technologie habilitante pour la croissance de l'Internet, et elle deviendra encore plus critique car l'IoT fait grimper le nombre de dispositifs connectés. Les gouvernements devraient faire de l'adoption de l'IPv6 une priorité nationale et engager les parties prenantes dans leur communauté pour encourager le déploiement de l'IPv6.[5]

- **Favoriser les standards IoT ouverts volontaires.** Employer une interopérabilité plus élevée et l'utilisation de standards ouverts, volontaires et largement disponibles en tant que blocs de construction techniques pour des dispositifs IoT supportera des bénéfices de l'utilisateur, une innovation et une opportunité économique plus importants. Les gouvernements devraient s'abstenir de mandater des approches techniques à l'IoT, et, au lieu de cela, encourager l'industrie, les chercheurs et d'autres parties prenantes à travailler ensemble sur

3 Pour plus d'exemples sur comment l'IoT soutient le développement, voir « Exploitation de l'Internet des Objets pour un Développement Global », https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf.
4 Des informations sur les Objectifs du Développement Durable des Nations Unies peuvent être trouvées sur https://sustainabledevelopment.un.org/sdgs.
5 Un guidage supplémentaire pour l'IPv6 peut être trouvé dans le dossier de politique sur l'IPv6 de l'ISOC, http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.

le développement de standards basés sur le consensus, ouverts, qui supportent l'interopérabilité.

- **Adopter une approche collaborative, pluripartite pour des discussions liées à la politique de l'IoT.** L'IoT constitue un domaine particulièrement intéressant pour les décideurs, du fait qu'il constitue un environnement de développement rapide, et sa technologie recouvre de nombreuses industries et utilisations. Une approche de gouvernance collaborative, une gouvernance qui se base sur l'expertise et l'engagement d'une vaste gamme de parties prenantes, sera nécessaire pour développer des solutions efficaces et appropriées.[6] Les politiques devraient viser à promouvoir la capacité des usagers à se connecter, se parler, innover, partager, choisir et se faire confiance d'une manière qui, à la fois, promeut l'innovation et habilite les droits de l'usager.

- **Favoriser une approche collaborative envers la sécurité de l'IoT.** L'Internet Society croit que la sécurité de l'IoT est la responsabilité collective de tous ceux qui développent et utilisent les dispositifs IoT. Les participants dans l'espace IoT doivent adopter une approche collaborative en ce qui concerne la sécurité parmi sa large communauté pluripartite en assumant la responsabilité, en partageant les meilleures pratiques et leçons apprises, en encourageant le dialogue lié à la sécurité, et en mettant l'accent sur le développement de solutions de sécurité flexibles, partagées, qui peuvent s'adapter et évoluer au fur et à mesure que les menaces se modifient au cours du temps. La politique de sécurité liée à l'IoT devrait privilégier la responsabilisation des acteurs pour traiter les problèmes de sécurité là où ils se produisent, plutôt que de centraliser la sécurité liée à l'IoT sur un petit nombre, et également préserver les propriétés fondamentales de l'Internet et des droits de l'usager.[7]

- **Favoriser des pratiques de conception responsables pour les dispositifs IoT.** Les pratiques liées à la sécurité dès le stade de la conception et à la confidentialité dès le stade de la conception pour les dispositifs IoT devraient être encouragées. Soit via la régulation de la protection de la confidentialité et des données, via l'autorégulation de l'industrie volontaire, ou via d'autres moyens d'incitation ou politiques, les développeurs de dispositifs IoT devraient être encouragés à respecter la confidentialité de l'utilisateur final et les intérêts de sécurité des données, et considérer ces intérêts comme un élément central du processus de développement du produit. Les concepteurs de systèmes IT devraient également considérer le cycle de vie complet du système IoT pour s'assurer que les dispositifs obsolètes ne posent pas de risque de sécurité et sont compatibles avec une gestion environnementale responsable.

6 Une vue d'ensemble du modèle pluripartite, collaboratif pour la gouvernance de l'Internet est disponible sur http://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works.
7 Une vue d'ensemble de l'approche de sécurité collaborative dans le rapport de l'Internet Society, Sécurité collaborative : Une approche pour aborder les problèmes de sécurité de l'Internet, 2015. http://www.internetsociety.org/collaborativesecurity.

Ressources supplémentaires

L'Internet Society a publié plusieurs articles et du contenu supplémentaire en rapport avec cette question. Ils sont disponibles en libre accès sur le site Web de l'Internet Society.

- Page Web sur les ressources d'IoT, http://www.internetsociety.org/iot.
- *L'Internet des Objets (IoT) : Une vue d'ensemble – Comprendre les problèmes et défis d'un monde plus connecté.* (2015). http://www.internetsociety.org/doc/iot-overview.
- "Adoption de l'IPv6 ". (2016). http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-IPv6-20160419-en.pdf.
- Pages Web sur les ressources IPv6, http://www.internetsociety.org/deploy360/ipv6/.

Sécurité collaborative : Une approche pour aborder les problèmes de Ssécurité de l'Internet. (2015). http://www.internetsociety.org/collaborativesecurity.