STC

175 STCTTS 17 F bis
Original : anglais

Assemblée parlementaire de l'OTAN

COMMISSION
DES SCIENCES ET DES TECHNOLOGIES

L'INTERNET DES OBJETS : PROMESSES ET DANGERS D'UNE TECHNOLOGIE DE RUPTURE

RAPPORT

Matej TONIN (Slovénie)
Rapporteur
Sous-commission sur les tendances technologiques et la sécurité

TABLE DES MATIÈRES

I. INTRODUCTION

1. L'internet des objets (IdO) est une technologie qui fait beaucoup parler d'elle depuis plusieurs années, et ce à juste titre car elle pourrait bien bouleverser la vie moderne telle que nous la connaissons. La planète compte aujourd'hui davantage d'objets connectés que de personnes. En 2016, la population mondiale atteignait 7,4 milliards de personnes, pour 16,28 milliards d'objets connectés (Cisco, 2016). D'ici 2020, entre 30 et 60 milliards de dispositifs seront connectés dans le monde entier (Vermesan et al. 2015; Howard, 2016). L'impact économique de l'IdO représente déjà un total annuel d'environ 2 billions de dollars et, d'ici 2025, le marché mondial de l'IdO pourrait représenter entre 4 et 12,8 billions de dollars par an (Fischer, 2015 ; al-Fuhaqa et al., 2015).

2. La croissance rapide de la technologie de l'IdO est stimulée par quatre éléments déterminants (Zheng et Carter, 2015). Premièrement, les capteurs, les régulateurs et les transmetteurs sont de plus en plus puissants, abordables et petits. Deuxièmement, le taux de pénétration d'internet, la bande passante et la disponibilité de la connectivité sans fil connaissent une croissance rapide. Troisièmement, comme le stockage et la capacité de traitement des données augmentent et s'améliorent, il est plus facile et moins cher de stocker et d'organiser des données. Quatrièmement, l'innovation dans les domaines des applications logicielles et de l'analyse, notamment les progrès en matière de techniques d'apprentissage automatique et d'algorithmes, a permis aux gens et aux entreprises de tirer parti des mégadonnées (*Big Data*).

3. Sur la courbe d'adoption des technologies, l'IdO se situe quelque part entre la phase d'innovation et la phase d'adoption précoce (Greengard, 2015). Si cette technologie atteint un jour sa pleine maturité et donne des résultats à la hauteur de son potentiel, l'IdO transformera chaque aspect de notre quotidien. Il pourrait par exemple permettre d'accroître la productivité des employés, d'améliorer la connectivité, de réduire les coûts d'exploitation, d'enrichir l'expérience des clients et des citoyens et d'augmenter les revenus dans de nombreux secteurs économiques (Folk et al., 2015). Le tableau 1 donne un aperçu de quelques-uns des principaux secteurs qui pourraient bénéficier de l'IdO.

Tableau 1 : EXEMPLES DE FUTURS SECTEURS INTELLIGENTS
Agriculture
Gestion des villes / urbanisme
Lutte contre le terrorisme
Énergie
Lutte contre l'incendie
Sécurité alimentaire
Soins de santé
Gestion domestique
Maintien de l'ordre
Logistique
Fabrication (internet industriel/industrie 4.0)
Militaire
Exploitation minière
Mobilité/transport
Achats

4. Si l'IdO recèle un énorme potentiel, une technologie de rupture comporte pourtant toujours des défis et des risques. La multiplication des objets connectés tout autour de nous inspire aux plus optimistes le sentiment parfaitement utopique qu'ils pourraient apporter une solution à bien des problèmes de l'humanité, et aux plus pessimistes, une dystopie selon laquelle l'adoption massive de ces technologies se ferait sans la sécurité adéquate, tandis que la volonté humaine reculerait au profit du contrôle gouvernemental et de celui des machines. Aucun de ces scénarios n'est à l'heure actuelle très vraisemblable mais l'IdO fera incontestablement des gagnants et des perdants (Greengard, 2015). Il faut donc impérativement entamer un débat politique soutenu sur la façon d'en exploiter les promesses et d'en maîtriser les dangers. Le présent rapport pourrait contribuer à lancer un tel débat dans le contexte de la sécurité transatlantique.

5. Le présent document est né de l'intérêt croissant que la commission des sciences et des technologies (STC) porte au thème des technologies de rupture potentielles, qu'elle traite dans ses rapports, réunions, visites et autres activités (elle a notamment mené en 2016 une enquête à petite échelle[1]). Il s'appuie en outre sur le rapport spécial que la STC a établi en 2014 sur *Cyberespace et sécurité euro-atlantique* (AP-OTAN, 2014).

6. Le présent rapport se penche tout d'abord sur les principes essentiels de l'IdO et sur les défis qui en découlent actuellement. Il s'intéresse ensuite aux opportunités et défis que présente l'IdO pour les forces armées, puis il se concentre tout particulièrement sur les défis qu'engendre l'IdO pour les infrastructures critiques. Il s'achève enfin par une série de recommandations sur la voie à suivre.

II. QU'EST-CE QUE L'INTERNET DES OBJETS ?

A. LES PRINCIPES DE BASE

7. Il n'existe aucune définition unanimement acceptée de l'IdO. Comme le déclarait récemment avec esprit un journaliste face à la multiplicité des points de vue à ce sujet : « C'est un peu comme la parabole des trois aveugles et de l'éléphant, mais au lieu de trois personnes, il y en a mille qui touchent une sculpture en argile humide » (Michels, 2017). La définition que donne Gartner, le leader mondial de la recherche et du conseil dans le domaine des technologies de l'information représente toutefois un bon point de départ : l'IdO est « le réseau d'objets physiques dotés d'une technologie intégrée qui leur permet de communiquer et de détecter, ou encore d'interagir avec leurs états internes ou l'environnement extérieur » (Gartner, 2017). L'IdO est également « une expression à la mode décrivant l'informatisation de tout, des voitures et compteurs électriques aux jouets des enfants en passant par le matériel médical et les ampoules électriques » (*The Economist*, 2017b). Peut-être la définition la plus ambitieuse est-elle toutefois celle du « concept des 6 "tout" » : « L'internet des objets vise à permettre de connecter des objets à *tout* moment, en *tout* lieu, à *tout* objet et à *tout* individu, de préférence à l'aide de *tout* accès/réseau et de *tout* service » (Vermesan et al., 2015 ; Borgia, 2014 ; définition soulignée par le rapporteur).

8. En dehors des définitions théoriques, la distinction entre « internet » et « internet des objets » est floue. En substance, l'IdO est « une expression générique désignant tout ce qui est connecté à internet » (TechTerms, 2015). Tout au début, on pouvait considérer internet comme indissociable des ordinateurs. Toutefois, au fil du temps, les dispositifs connectés n'ont plus été seulement des ordinateurs et les chercheurs se sont attachés à trouver une façon de décrire cette évolution. C'est à Kevin Ashton, directeur exécutif de l'*Auto-ID Center du Massachusetts Institute of Technology*, que revient la paternité de l'expression « internet des objets », qu'il a utilisée en 1999 pour décrire sa vision de l'avenir de la gestion de la chaîne d'approvisionnement compte tenu

[1] Voir le rapport général 2017 de la STC *Préserver l'avance technologique de l'OTAN : adaptation stratégique et R&D en matière de défense* [174 STC 17 F bis]

de la connexion d'objets à internet grâce au système d'identification par radiofréquence (RFID, voir également ci-après). Le fait de pouvoir suivre automatiquement leur stock de portières, de moteurs et de roues, allait permettre aux entreprises automobiles d'améliorer considérablement la gestion de leur chaîne d'approvisionnement. L'expression a été adoptée mais aujourd'hui encore les entreprises continuent de rivaliser les unes avec les autres pour trouver de nouvelles expressions à la mode, parmi lesquelles : « systèmes cyber-physiques », « l'internet de tout », ou encore « le web physique ». À l'instar de l'internet des ordinateurs, qui est tout simplement devenu « internet » dans l'esprit de la plupart des gens, il se pourrait bien que l'IdO, de par son intégration croissante dans le quotidien de tout un chacun, devienne juste, une fois encore, « internet ».

9. Tout comme internet, l'IdO ne consiste pas simplement en une technologie ou en un réseau (Vermesan et al., 2015). Il s'agit plutôt d'un « archipel de dispositifs connectés » (Greengard, 2015). L'une des particularités de l'IdO est son degré élevé d'hétérogénéité : les ampoules intelligentes, dont l'intensité peut être diminuée avec un smartphone, n'ont rien à voir avec les conteneurs d'expédition étiquetés, qui peuvent faire l'objet d'un suivi dans le monde entier, ces derniers n'ayant eux-mêmes rien à voir du tout avec les voitures sans chauffeur, qui sont dotées d'une technologie de détection suffisante pour pouvoir circuler en ville.

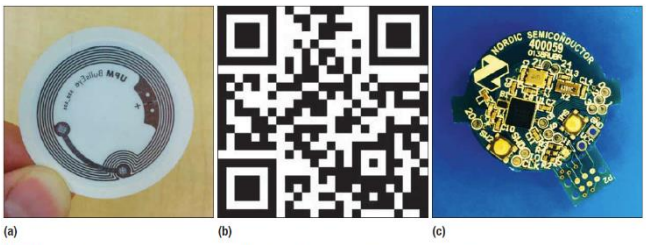
10. Examiner les éléments constitutifs de l'IdO aide à mieux cerner ce que recouvre cette expression. Au cœur de l'IdO, il y a des « objets » physiques, connectés et intelligents (Folk et al., 2015). De tels équipements collectent, transmettent, calculent et agissent en fonction des données reçues. On les appelle le « nouveau carburant » ou la « nouvelle monnaie » des économies actuelles (Vanian, 2016). Les sept processus décrits ci-dessous rattachent ces objets à l'IdO (Al-Fuhaqa et al., 2015).

11. **Identification** : pour faire partie de l'IdO, les objets doivent pouvoir être désignés et avoir une adresse, tout comme les ordinateurs peuvent être localisés et identifiés grâce à leur adresse IP (protocole internet). En d'autres termes, les dispositifs intelligents ne sont d'aucune utilité s'ils ne peuvent être directement accessibles. De nos jours, il existe une multitude d'identifiants pour les produits IdO, par exemple les identificateurs de ressources uniformes (URI), les codes produits électroniques (EPC), des codes universels et des adresses IP relevant du tout dernier protocole en vigueur (IPv6).

12. **Détection** : les capteurs permettent aux objets intelligents d'obtenir des données et donc d'interagir avec le monde physique. Les smartphones d'aujourd'hui en contiennent d'ailleurs une multitude, notamment, des détecteurs de proximité, des capteurs de lumière, des baromètres, des magnétomètres, des détecteurs de position, de vitesse et de courant, des accéléromètres, des gyroscopes, des thermomètres, des podomètres, des cardiofréquencemètres, des capteurs d'empreintes digitales et même des détecteurs de rayonnement. Les chercheurs tentent même de mettre au point des détecteurs de goûts et d'odeurs qui puissent un jour rivaliser avec le goût et l'odorat de l'utilisateur.

13. **Communication** : il faut que les données récoltées par les capteurs soient transmises à un dispositif susceptible de les analyser puis d'y réagir. Les températures relevées par des thermostats intelligents doivent être envoyées aux éléments du réseau qui sont en mesure de répondre en conséquence (monter le chauffage ou enclencher la climatisation, etc.). Il existe une diversité de technologies filaires ou sans fil – qui ont toutes des avantages et des inconvénients différents – pouvant assurer ces communications. Par exemple, l'IdO reposait à ses débuts sur l'utilisation d'étiquettes RFID (radio-étiquettes) pour le suivi de marchandises à l'échelle nationale ou mondiale. De nombreux produits de consommation en sont aujourd'hui équipés. Il existe d'autres technologies d'étiquetage, notamment les codes QR (*Quick Response*) et le Bluetooth *Low Energy* (voir figure 1), ainsi que d'autres technologies de communication, comme la communication en champ proche (NFC pour *Near-Field Communication*), le wifi, Bluetooth ou

ZigBee, ainsi que des technologies radio à bande étroite (reposant sur des services dédiés ou des systèmes de téléphonie mobile).



(a) (b) (c)

FIGURE 2. Various forms of electronic tags support the Physical Web (all about the size of a quarter): (a) a near-field communication (NFC) tag; (b) a quick response (QR) code; and (c) a Bluetooth low energy (BLE) tag. However, it is not clear which technology—each with its own affordances and problems—will become the primary IoT enabler.

Figure 1 (Want et al., 2015)

14. **Informatisation** : une fois les données récoltées et communiquées, elles doivent être informatisées, ce qui peut se faire de diverses façons. Certains produits IdO seront en mesure de traiter les données grâce à des microcontrôleurs. Il est fréquent qu'ils puissent aussi réagir aux informations qu'ils reçoivent grâce à des actionneurs. C'est ainsi qu'en l'absence de la famille, partie en vacances, des détecteurs de fumée intelligents peuvent au besoin directement appeler les pompiers. D'autres dispositifs vont toutefois envoyer leurs données à des smartphones ou à des ordinateurs situés à proximité. Dans d'autres configurations encore, il se pourrait que des réseaux informatiques locaux soient en mesure de traiter les données eux-mêmes ou qu'ils fassent office de passerelles vers des services d'informatique en nuage (*cloud computing*).

15. **Services** : une fois les données arrivées à destination, les services entrent en jeu. Une solution domotique intelligente réglera la température, le flux d'air ou l'éclairage dans une habitation. Un système logistique intelligent saura à quel moment il doit commander de nouveaux composants pour une chaîne de montage ou ordonner l'expédition d'un conteneur qui vient juste d'être rempli. Un réseau électrique intelligent analysera les données émises par ses composants et optimisera ensuite la production d'énergie ou l'utilisation de celle-ci en conséquence. En définitive, la seule limite aux possibilités de services IdO est l'imagination de l'être humain (ou des machines).

16. **Sémantique** : les chercheurs se consacrent depuis plusieurs années au « web sémantique », qui « fournit un modèle commun permettant aux données d'être partagées - et réutilisées - entre plusieurs applications, entreprises et groupes d'utilisateurs » (W3C, 2013). Le web sémantique devrait pouvoir intégrer et fusionner les données provenant de nombreuses sources hétérogènes pour que les êtres humains ou les machines puissent trier les données disponibles de façon plus intuitive. La sémantique devient donc extrêmement utile dans l'environnement IdO. Un expert affirme même qu'elle est le « cerveau de l'IdO » (Al-Fuhaqa et al., 2015).

17. Du fait de leur hétérogénéité, les **infrastructures IdO** peuvent prendre de multiples formes. Certains systèmes IdO fonctionnent principalement à l'échelon local. Les maisons intelligentes seront par exemple en grande partie autonomes. Cependant, les données recueillies à un niveau pourraient être intégrées dans un système plus vaste : il serait possible d'explorer les données provenant de toutes les maisons intelligentes d'un quartier pour mieux comprendre comment améliorer la gestion de chacune d'entre elles. D'autres systèmes fonctionnent avant tout à l'échelle macroscopique. Par exemple, un système de capteurs déployé dans le monde entier et recueillant des données environnementales pourrait alimenter directement des dispositifs d'analyse des changements ou phénomènes climatiques. Certains systèmes enverront des données à des services centralisés d'informatique en nuage. D'autres pourront s'appuyer sur des capacités informatiques locales comme le « *fog computing* », aussi appelé « *edge computing* », dont la puissance de calcul est moindre mais qui sont plus rapides. Un système de feux de circulation

intelligents, servant à signaler aux piétons qui traversent si un véhicule s'apprête à brûler le feu rouge, n'a pas le temps d'envoyer ses données vers le nuage (Bonomi et Natarajan, 2014). Il pourrait sauver des vies en s'appuyant sur l'informatique locale ou sur d'autres dispositifs intelligents de proximité (*fog / edge computing*). Certains objets intelligents communiqueront directement avec le nuage et d'autres indirectement, par exemple par l'intermédiaire de la tablette d'un utilisateur. Les systèmes IdO peuvent aussi être intégrés dans des systèmes de systèmes. Les données relatives au transport aérien, qui sont avant tout recueillies pour améliorer les flux de passagers, peuvent être associées aux données des systèmes de santé pour déterminer de quelle manière les maladies infectieuses se propagent d'une région à une autre. Certains systèmes peuvent essentiellement s'appuyer sur les communications entre machines, sans grande interférence humaine dans leur fonctionnement quotidien, alors que d'autres impliquent de nombreuses communications humains-machines. Certains objets sont avant tout des objets physiques équipés d'éléments IdO, par exemple des caisses de pièces de machines radio-étiquetées. D'autres sont essentiellement des objets numériques existant aussi dans le monde physique, par exemple les tablettes informatiques. En un mot, l'architecture du système IdO semble offrir des possibilités infinies.

B. DÉFIS TECHNIQUES ET TECHNOLOGIQUES

18. Pour pouvoir vraiment se généraliser, l'IdO doit inévitablement surmonter de nombreux défis techniques et technologiques. L'un des plus grands défis réside dans la nécessité de définir des **normes** communes. Des sociétés, par exemple, travaillent actuellement à l'élaboration de toute sorte de normes. Il est donc essentiel de fusionner ces normes, indépendamment de leur source, pour parvenir à de bons standards et garantir l'interopérabilité. C'est pourquoi les organisations internationales de normalisation et diverses autres organisations s'efforcent activement d'élaborer des normes relatives à l'IdO, tandis que des alliances entre différents acteurs commencent à se former dans le but de concrétiser cette fusion. Si la normalisation et l'interopérabilité sont à ce point indispensables c'est que la plus grande promesse de la technologie IdO réside dans la valeur ajoutée liée à la connexion de produits IdO très divers et à l'utilisation des mégadonnées qu'ils génèrent. C'est ainsi que dans un environnement urbain, les routes et feux de circulation intelligents, les systèmes intelligents de distribution de l'énergie et de l'eau auto-fourniraient tous une valeur ajoutée. Toutefois, le plus grand potentiel en matière de gestion urbaine réside dans les données provenant de chacun de ces systèmes de manière à réduire les coûts et à améliorer l'efficacité, la qualité de vie et la sécurité. Une analyse va même jusqu'à affirmer que « 40 % de la valeur économique potentielle de l'internet des objets dépendra de l'interopérabilité » (Baily et Manyika, 2015). En juin 2015, la commission a en effet identifié les possibilités de tels systèmes complexes à partir de l'initiative LMSI (*Lower Manhattan Security Initiative*) des services de police de la ville de New York ; la LMSI intègre caméras, détecteurs, archives nationales et autres sources de données et elle permet de disposer d'images de la ville en temps réel ou d'archives (AP-OTAN, 2015).

19. La généralisation de l'IdO soulève d'autres questions techniques et technologiques essentielles (dont les questions de sûreté, de sécurité et de protection de la vie privée qui sont examinées dans la sous-section suivante) :

- **Infrastructures IdO** : comment les produits intelligents, dont le nombre ne cesse d'augmenter, seront-ils connectés à (des parties de) l'IdO ? Où s'effectuera le traitement des données : au sein de petits réseaux locaux, de dispositifs décentralisés de *fog computing* ou de dispositifs centralisés d'informatique en nuage ?
- **Détection du contexte** : est-il possible de mettre au point des dispositifs capables de détecter le contexte dans lequel ils se trouvent afin de prendre de meilleures décisions ? Un smartphone peut-il par exemple automatiquement se mettre sur silencieux lorsqu'il détecte qu'il se trouve dans un cinéma ?

- **Connectivité des produits de faible technologie** : comment intégrer des produits IdO de faible technologie, par exemple des poignées de porte intelligentes, dans des réseaux dans lesquels ils vont être en présence de produits de haute technologie ayant une puissance de calcul largement supérieure ?
- **Recherche de produits** : comment les utilisateurs de l'IdO – qu'il s'agisse de machines ou d'humains – retrouveront-ils certains produits IdO lorsqu'il y en aura des milliards de par le monde ? Il existe déjà des bases de données interrogeables sur les produits IdO mais serait-il possible de les étendre et de les rendre conviviales ?
- **Latence** : comment s'assurer que les données arrivent à destination à temps ? Par exemple, les systèmes à bord des voitures autonomes pourraient-ils réagir suffisamment vite pour empêcher des accidents ?
- **Mobilité** : comment s'assurer que les produits IdO s'intègrent sans effort dans les réseaux qu'ils rencontrent lorsqu'ils sont en mouvement, par exemple des voitures connectées se déplaçant en Europe ? Quels investissements d'infrastructures les autorités doivent-elles réaliser pour garantir une couverture transnationale adéquate ?
- **Extensibilité** : pourrait-on mettre au point des applications susceptibles de contrôler des produits très variés étant donné qu'il ne sera pas possible, dans la pratique, de télécharger une application pour chaque petit service IdO ?
- **Analyse des mégadonnées** : comment les services informatiques traitent-ils les mégadonnées, qui se caractérisent par leur volume important, leur vitesse et leur diversité, et qui proviennent de produits souvent distribués à grande échelle ?
- **Coûts** : à mesure que la complexité des produits et des services augmente, les fournisseurs peuvent-ils maîtriser les coûts de façon à ce que l'IdO se généralise ?
- **Besoins énergétiques** : est-il possible de gérer durablement les besoins énergétiques découlant de la prolifération des produits IdO ?
- **Enjeux environnementaux** : si les articles IdO se généralisent, quel sera l'impact sur la gestion des déchets électroniques produits ?

20. Conscients qu'il faut surmonter ces défis ou les gérer si la révolution de l'IdO est appelée à devenir une réalité, les chercheurs, le secteur industriel et les pouvoirs publics s'emploient sans relâche à trouver des solutions à ces problèmes. Un grand nombre de technologies émergentes pourraient y contribuer (du moins en partie), et libérer tout le potentiel de l'IdO.
Le tableau 2 présente certaines de ces technologies.

Tableau 2 : TECHNOLOGIES HABILITANTES POUR L'IDO
Fabrication additive
Systèmes de fabrication avancés
Matériaux avancés
Intelligence artificielle
Biotechnologie
Blockchain
Exploration de données complexes
Nanotechnologie
Photonique
Technologie quantique
Robotique

C. L'AVENIR DE L'IdO : ARGUMENT ÉCONOMIQUE, SÉCURITÉ ET VIE PRIVÉE

21. La vitesse à laquelle se généralise l'IdO dépend de tout un éventail de facteurs allant au-delà des défis techniques et technologiques. Bien que le potentiel d'adaptation du secteur public soit énorme, le secteur privé progresse plus rapidement dans l'offre de produits et de services IdO. Ce seront donc les prestataires commerciaux et les consommateurs qui forgeront l'avenir de l'IdO.

22. Les entreprises doivent être convaincues de l'argument économique. La valeur ajoutée de l'IdO est vraiment évidente dans de nombreux secteurs, par exemple la gestion de la chaîne d'approvisionnement. De grandes sociétés comme Amazon et Walmart ont beaucoup à gagner en utilisant l'IdO. Pour d'autres secteurs, ce n'est en revanche pas aussi évident. La principale question est de savoir si les entreprises peuvent tirer de l'IdO une valeur suffisante pour pouvoir procéder aux investissements nécessaires. Après tout, l'IdO n'est pas une fin en soi pour elles ; elles doivent trouver le moyen de gagner des parts de marché et d'accroître leur profit (IBM, 2015). Les détracteurs affirment d'ores et déjà que le modèle économique de l'IdO ne fonctionne pas, en partie à cause du manque de valeur fonctionnelle de nombreux produits IdO et de la hausse des coûts (IBM, 2015).

23. Il faut par ailleurs convaincre les clients de la valeur ajoutée des produits IdO. Si les clients ne sont pas convaincus qu'un grille-pain connecté améliore leur vie, ils ne l'achèteront pas. Ils tiennent également compte d'autres facteurs clés, tels que la fiabilité et la facilité d'utilisation des produits et services IdO. Selon un groupe de chercheurs, « nous devons faire en sorte que tout utilisateur puisse, avec quelque smartphone ou tablette que ce soit, interagir avec n'importe quel produit IdO dont il s'approche (sans application spéciale) » (Want et al., 2015).

24. Comme pour tout ce qui concerne le cyberespace en général, des questions majeures se posent en matière de sécurité et de vie privée. Si les fournisseurs ne peuvent pas garantir que les produits IdO sont sûrs et qu'ils protègent la vie privée de leurs clients – ou si les clients ne font pas confiance aux sociétés sur ce plan – l'IdO ne sera ni rapidement ni largement adopté. Il existe trois grandes catégories de risques :

- **Les risques pour la vie privée :** on peut citer à titre d'exemple récent le mode « *fake off* » secret que la CIA aurait installé en 2012 et 2013 sur certains modèles de téléviseurs intelligents de la marque Samsung (Calore, 2017). Cette révélation a fait suite à la publication par WikiLeaks de documents provenant soi-disant du gouvernement des États-Unis. Ces documents laissent entendre qu'en cas d'activation de l'outil de collecte de renseignements, le téléviseur, qui semble être éteint, peut recueillir des données audios et éventuellement vidéos sur ce qui se passe autour de lui.
- **Le risque systémique :** à titre d'illustration, en 2016, le « botnet Mirai », réseau regroupant 145 000 caméras et enregistreurs vidéo numériques (DVR), a servi à mener une attaque contre un serveur crucial de noms de domaines, ce qui a entraîné l'interruption d'un certain nombre de services et la paralysie de plusieurs sites web majeurs. Cette attaque a globalement impliqué jusqu'à un million d'appareils connectés à Internet (Agawu & Bate, 2016).
- **Les autres risques associés à des appareils IdO mal sécurisés** : voir Section IV sur l'Infrastructure critique et l'IdO.

25. Les réseaux IdO sont difficiles à sécuriser. Il existe notamment un risque de dysfonctionnement des produits IdO, d'utilisation accidentelle de ces produits et d'attaques ciblées (primitives ou sophistiquées) (Evans, 2015 ; Lewis, 2016). Voici quelques exemples de risques potentiels :

- Lorsqu'il était vice-président des États-Unis, Dick Cheney a fait désactiver la fonction sans fil de son pacemaker de crainte que des hackers n'infligent une décharge fatale à son cœur (Zetter, 2015).
- En 2015, une vidéo virale montrait de quelle façon des hackers étaient parvenus à détourner le système embarqué d'une Jeep et à désactiver le volant et les freins (Valasek & Miller, 2015).
- Un rapport de 2015 signalait que les réseaux Wi-Fi à bord des avions étaient vulnérables aux attaques de hackers susceptibles de prendre le contrôle d'un avion en plein vol (Hern et agences, 2015).
- En 2017, un organisme gouvernemental allemand a lancé un avertissement contre une poupée parlante. À cause d'un périphérique Bluetooth non sécurisé, sa technologie intelligente pouvait dévoiler des données à caractère personnel. En théorie, des hackers étaient en mesure d'écouter un enfant et de lui parler pendant que celui-ci jouait avec la poupée (BBC News, 2017).

26. Internet étant déjà répandu, l'adoption généralisée de l'IdO rendra la connectivité quasi omniprésente et mènera à une grande densité de partage de l'information sur les réseaux filaires et sans fil. Les questions fondamentales de sécurité et de protection de la vie privée dans le cadre de l'IdO ne sont pas bien différentes de celles qui se posent dans le reste du cyberespace. La principale différence, toutefois, tient au fait que de nombreux produits IdO, qui sont par nature de très faible technologie – du moins en l'état actuel et à moyen terme –, ne convergent souvent que sur des réseaux *ad hoc* et pendant de courtes périodes. Équiper des interrupteurs, des rayons de supermarché ou des tracteurs intelligents des mêmes normes de sécurité et de protection de la vie privée que les ordinateurs, les smartphones ou les tablettes pourrait ne pas être faisable d'un point de vue économique. Alors comment garantir une protection adéquate ?

27. Les chercheurs développent des solutions technologiques pour la protection de la sécurité et de la vie privée. Les concepteurs de produits IdO même de faible technologie développent des soi-disant solutions de sécurité fondées sur les systèmes. Les appareils de faible technologie pourraient ainsi se connecter à internet via un contrôleur plus sophistiqué assurant une sécurité approfondie que ne peuvent offrir ces appareils. Un nouveau paradigme – la sécurité centrée sur les données – gagne du terrain. Il s'agit d'une approche plus pragmatique de la sécurité, qui reconnaît que – même en utilisant les meilleurs outils de cybersécurité – des intrus trouveront toujours le moyen de pénétrer les systèmes (Mullins, 2016). Suivant cette approche, c'est la protection des données (les plus précieuses) qui devient l'objectif prioritaire. Les défenseurs doivent donc comprendre les infrastructures, flux et risques liés aux données, classifier les données sensibles, tout en surveillant et en contrôlant leur utilisation.

28. La grande question en matière de sécurité IdO et de protection de la vie privée qui se pose consiste à savoir s'il faut « implanter » des dispositifs de protection efficaces dans les produits dès le départ ou s'il faut d'abord attendre que le marché de l'IdO décolle avant de venir « greffer » de tels dispositifs sur les produits (Lindsay et al. 2016). Pour ses partisans, la première solution permettrait aux autorités de réglementation d'éviter certains des écueils du développement d'internet, qui avait été conçu initialement pour des réseaux de faible envergure reliant des ordinateurs de confiance et pas comme un marché de masse rempli de cybercriminels. Le concept le plus répandu est celui qui fait d'une telle « sécurité par défaut » le but même de la conception de produits et de services IdO. Les partisans d'une « greffe » ultérieure de sécurisation supplémentaire craignent à l'inverse qu'installer des fonctions de sécurité coûteuses n'étouffe ce marché émergent. Un expert affirme qu'il n'est pas nécessaire que tous les produits IdO aient le même niveau élevé de sécurité et de protection de la vie privée (Lewis, 2016). Il propose de tenir compte de trois paramètres : la valeur des données recueillies, la criticité de ces données et la modularité en cas de défaillance. En d'autres termes, la protection doit être la plus élevée si les produits et services IdO recueillent et transmettent des données extrêmement utiles et/ou

sensibles et/ou si une défaillance dans une partie risque d'entraîner, en cascade, une défaillance généralisée.

29. La sécurité absolue n'est pas possible. Comme l'a récemment affirmé un magazine d'actualité : « Le risque de fraude, celui d'un accident de voiture et le risque météorologique ne peuvent jamais non plus être totalement éliminés. Mais les entreprises ont trouvé des moyens de gérer un tel risque, que ce soit en s'appuyant sur la réglementation gouvernementale ou en faisant jouer la responsabilité juridique et les assurances pour susciter un comportement sûr » (*The Economist*, 2017a). Le tableau 3 montre un exemple de principes stratégiques appliqués à un niveau national. Quoi qu'il en soit, les autorités de réglementation devraient probablement s'efforcer d'adopter une approche équilibrée permettant d'éviter aussi bien une ruée sur le marché qu'une prudence excessive. Comme le démontre la prochaine section, il serait en outre prudent de sécuriser bien davantage les parties les plus cruciales de l'IdO, à savoir celles qui concernent les forces armées et les infrastructures critiques, plutôt que les biens de consommation.

Tableau 3 **PRINCIPES STRATÉGIQUES** **DE SÉCURISATION DE L'INTERNET DES OBJETS** **(DÉPARTEMENT DE LA SÉCURITÉ INTÉRIEURE DES ÉTATS-UNIS)** **(DHS, 2016)**
Incorporer la sécurité dès la phase de conception
Promouvoir les mises à jour de sécurité et la gestion de la vulnérabilité
S'appuyer sur les pratiques de sécurité reconnues
Prioriser les mesures de sécurité en fonction de l'impact potentiel
Promouvoir la transparence dans l'intégralité de l'IdO
Se connecter prudemment et délibérément

D. QUEL RÔLE POUR L'OTAN ET L'UE ?

30. Fort heureusement, la plupart des responsables politiques prennent ces défis au sérieux. En ce qui concerne l'IdO, l'Union européenne (UE) s'est par exemple lancée dans une série d'initiatives et d'activités politiques visant à en utiliser le plein potentiel. La vision qu'a l'UE de l'IdO repose sur trois grands piliers : un marché unique pour l'IdO, un écosystème IdO prospère, et une approche de l'IdO axée sur l'être humain. En mars 2015, la Commission européenne a lancé l'Alliance pour l'innovation dans le domaine de l'internet des objets (AIOTI, *Alliance for Internet of Things Innovation*), qui vise à mettre en place un écosystème IdO dynamique, à booster l'innovation et le déploiement et à encourager l'interaction entre les acteurs concernés. Également en 2015, la Commission a adopté la stratégie pour un marché unique numérique, qui met l'accent sur la nécessité d'éviter la fragmentation et de favoriser l'interopérabilité au sein de l'IdO. Les grands domaines de la stratégie de l'IdO sont, pour l'UE, l'agriculture intelligente, les villes intelligentes, les secteurs industriels intelligents ainsi que les systèmes durables de logistique inverse, la gestion intelligente de l'eau et les réseaux électriques intelligents. Entre 2014 et 2017, l'UE avait notamment prévu d'investir 192 millions d'euros dans la recherche et l'innovation dans le domaine de l'IdO. Le programme en cours « Horizon 2020 » a fixé des objectifs concrets en matière de recherche et d'innovation dans le domaine de l'IdO, et la Commission européenne a lancé un appel à projets-pilotes à grande échelle pour l'IdO dans les domaines suivants : technologies portables, assistance à domicile, véhicules connectés, villes intelligentes, agriculture intelligente et gestion de l'eau. Cet appel est désormais clos et des fonds sont alloués aux projets retenus (au total, cinq projets pilotes à grande échelle et deux activités de collaboration et de soutien). Avec l'Alliance pour l'innovation dans le domaine de l'internet des objets, la Commission européenne travaille actuellement à un projet de nouvelle législation sur la création d'un processus de certification des produits IdO qui garantirait une protection aux utilisateurs. Il s'agit là d'une série d'exigences de base en matière de sécurité et de vie privée (Commission européenne et

Alliance pour l'innovation dans le domaine de l'internet des objets, 2017). Elle souhaite encourager les entreprises à réfléchir à un système d'étiquetage des objets connectés à internet à la fois approuvés et sûrs (Stupp, 2016).

31. L'OTAN, qui mène peu d'activités directement liées à l'IdO en dehors de celles qui consistent à mieux en comprendre les tenants et les aboutissants, commence tout doucement à entreprendre des travaux dans ce domaine. Par exemple, la Commission Technologie des systèmes d'information de l'Organisation OTAN pour la science et la technologie (STO) appuyée par son Bureau de soutien à la collaboration (CSO) a créé en 2016, pour trois ans, un groupe de travail sur les applications militaires de l'IdO.[2] Celui-ci a pour mission de prouver la valeur militaire de l'IdO moyennant des démonstrations de faisabilité, de définir une ou plusieurs architectures militaires potentielles IdO, de déterminer les risques possibles, les mesures d'atténuation et les défis non résolus liés à l'utilisation de la technologie IdO commerciale dans les forces armées, et de créer un réseau IdO à l'échelle de l'OTAN, de l'UE et de diverses communautés nationales.

32. Comme le montre le présent rapport, il reste bien des défis à surmonter en termes de sécurisation de l'IdO. Il est ressorti d'une enquête réalisée en 2015 que « 71 % des cadres estiment que les mesures nécessaires pour sécuriser les produits IdO ont entre 12 et 24 mois de retard sur le déploiement de ces produits » (Tripwire, 2015). Il est donc essentiel que les Alliés renforcent leurs politiques de cyberdéfense et de sécurité, dans le domaine civil aussi bien que dans les forces armées. Les initiatives visant à améliorer la sécurité des infrastructures critiques doivent également figurer parmi les travaux prioritaires. Fort heureusement, les pays de l'Alliance, l'OTAN en tant qu'organisation ainsi que l'UE prennent ces défis très au sérieux. L'OTAN et l'UE ont renforcé leurs politiques en la matière en 2016. Au sommet de Varsovie, en 2016, l'Alliance a une fois de plus consolidé sa politique de cyberdéfense. Les chefs d'État et de gouvernement ont réaffirmé le mandat défensif de l'OTAN et rappelé que la cyberdéfense relève de la tâche fondamentale de l'Alliance qu'est la défense collective, et que l'OTAN est prête à invoquer l'article 5 en réponse à une importante cyberattaque. En outre, l'Alliance est allée un peu plus loin en reconnaissant le cyberespace « en tant que domaine d'opérations dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait dans les airs, sur terre et en mer » (OTAN, 2016). En octobre 2016, l'OTAN a signé un mémorandum d'entente avec les autorités responsables de la cyberdéfense dans ses 28 pays membres, en vertu duquel des dispositions ont été prises en matière d'échange d'informations, de prévention des cyberincidents, ainsi que de capacité de résilience et de réaction. Pour sa part, l'UE a finalisé sa directive sur la sécurité des réseaux et des systèmes d'information, ce qui a représenté le premier texte de législation européenne sur la cybersécurité. Qui plus est, en février 2016, l'OTAN et l'UE ont signé un arrangement technique sur la coopération en matière de cyberdéfense afin de renforcer leur coopération dans ce domaine, et en particulier pour ce qui a trait à l'échange d'informations, à la formation, à la recherche et aux exercices. Il faut impérativement que cette volonté politique positive perdure étant donné que les défis liés à l'IdO ne feront qu'aller croissant au fil du temps.

[2] La nation cadre est la Pologne et les nations participantes sont l'Allemagne, la Belgique, les États-Unis, la Finlande (en qualité de pays partenaire), les Pays-Bas, la Roumanie et le Royaume-Uni. L'Agence d'information et de communication de l'OTAN est une organisation participante. Pour plus de détails, voir : https://www.cso.nato.int/activity_meta.asp?act=8647.

III. LES FORCES ARMÉES ET L'IdO

33. Le département de la Défense des États-Unis joue habituellement un rôle fondamental dans le développement des diverses technologies – capteurs, mise en réseau informatique et communications – qui sont à la base de l'IdO d'aujourd'hui (Zheng et Carter, 2015). Hélas, l'adoption de l'IdO par le secteur militaire n'en est qu'à ses débuts. Toutefois, comme la commission l'a appris au cours de sa visite dans les locaux de Leonardo-Finmeccanica en octobre 2016 (AP-OTAN, 2017), les entreprises du secteur de la défense et les forces armées ont hâte de se préparer pour l'IdO, d'en comprendre les tenants et les aboutissants et d'en tirer parti (Seffers, 2015). L'Agence états-unienne des systèmes d'information de la défense, par exemple, affirme que l'IdO « entraînera une explosion des capacités sur nos réseaux sensibles non classifiés et classifiés » (Seffers, 2015). Elle ajoute : « qu'il s'agisse d'améliorer le suivi logistique, d'optimiser la sécurité des bâtiments et les contrôles environnementaux ou de surveiller la santé de chaque soldat, l'internet des objets aura des incidences sur tout ce que nous faisons ».

A. LE POTENTIEL DES TECHNOLOGIES IdO POUR LES FORCES ARMÉES

34. Les produits connectés peuvent être bénéfiques aux forces armées d'aujourd'hui car ils peuvent leur permettre de renforcer leur efficacité et leur efficience, et de réduire les coûts (Zheng et Carter, 2015). L'IdO militaire faciliterait la modernisation et peut-être même révolutionnerait-il la guerre moderne. Les produits et services IdO peuvent recueillir des données de plus en plus nombreuses, de plus en plus complexes, puis les analyser plus rapidement ; ils font appel à une automatisation accrue et permettent de réduire l'erreur humaine, de livrer des capacités militaires plus précises et plus efficientes, et de diminuer les coûts en personnel.

35. Les États-Unis, première puissance militaire du monde, jouent un rôle précurseur dans l'adoption de l'IdO par le secteur militaire. Ils incorporent déjà des technologies IdO dans quatre domaines (Zheng et Carter, 2015), à savoir :

- **Les capteurs :** les forces armées des États-Unis se concentrent principalement sur le potentiel de l'IdO pour les applications en situation de combat et les capteurs déployés dans les différents systèmes C4ISR (commandement, contrôle, communication, informatique, renseignement, surveillance et reconnaissance). Par exemple, les plateformes de détection aéroportées, les satellites de surveillance, les véhicules aériens sans pilote, les systèmes embarqués et les stations au sol aussi bien que les soldats sur le terrain collectent des données qui sont ensuite communiquées au système commun reparti au sol DCGS (*Distributed Common Ground System)*. Celui-ci recueille et analyse les données puis transmet des informations en amont et en aval de la chaîne de commandement (AP-OTAN, 2016). Certains experts encouragent vivement les États-Unis à s'orienter vers une infrastructure en nuage intégrale pour le combat et à s'affranchir des réseaux distincts existants pour mettre en place un centre de données unifié (Wind, 2015).

- **Les systèmes de contrôle de la puissance de feu :** le déploiement de bout en bout de capteurs mis en réseau et de systèmes d'analyse numérique permet d'apporter des réponses entièrement automatisées à diverses menaces en temps réel et d'appliquer la puissance de feu avec une grande précision. Sont par exemple déjà en service le système de combat *Aegis* de la marine des États-Unis, les véhicules aériens sans pilote *Predator* ou encore le missile d'attaque terrestre *Tomahawk*.

- **Les technologies mobiles :** les forces armées des États-Unis ont lancé des programmes pilotes pour mettre en œuvre des technologies mobiles pour ses soldats et ses civils. C'est ainsi que le programme NETT Warrior vise à équiper les unités d'infanterie de smartphones Samsung Galaxy Note modifiés et reliés à la radio Rifleman, qui est capable de transmettre des données. Les soldats sur le terrain peuvent avoir accès à tout un éventail d'applications,

comme des cartes en 3D, un système de suivi des forces amies, des services de traduction et les profils des objectifs de grande importance. Toutefois, l'absence de connectivité, une fonctionnalité limitée et une expérience utilisateur médiocre sont autant d'obstacles qui subsistent au déploiement généralisé de ces dispositifs.

- **La gestion logistique :** les produits IdO ont été adoptés dans le cadre de la gestion logistique pour les tâches suivantes : suivi des envois, gestion des stocks, formation, simulation et gestion relatives aux systèmes énergétiques intelligents (comme l'initiative de l'OTAN en matière d'énergie intelligente [AP-OTAN, 2013]). Néanmoins, dans l'ensemble, le déploiement de ces produits et leur intégration sont encore limités.

36. Il existe plusieurs lacunes et difficultés en ce qui concerne la réussite du déploiement et du développement des technologies IdO au sein des forces armées des États-Unis (Zheng et Carter, 2015). Peu de systèmes font appel au plein potentiel de l'IdO, qu'il s'agisse de capteurs en réseau, de solutions d'analyses numériques ou de réponses automatisées. En outre, le secteur militaire a adopté une approche décentralisée des technologies IdO, c'est-à-dire que les différentes armes développent et déploient des technologies très différentes, ce qui rend celles-ci difficiles à sécuriser et qui limite la capacité à communiquer entre systèmes ou à faire des économies d'échelle et des synergies à partir de divers types de données. D'autres experts font toutefois valoir qu'une approche holistique au niveau de l'ensemble des forces armées pourrait s'avérer complexe, fastidieuse et en fin de compte contre-productive. Les systèmes de collecte et de traitement des données sont en outre sous-performants et l'automatisation fait défaut. Il y a d'autres facteurs restrictifs, comme l'absence de connectivité et l'infrastructure réseau nécessaire au traitement de la quantité de données générées par l'IdO militaire. Il faudrait procéder à des investissements considérables dans les infrastructures et les logiciels d'analyse pour transférer, stocker et analyser les données générées. Établir des normes et des protocoles communs afin d'assurer l'interopérabilité pose un autre défi.

37. Les barrières culturelles sont également un obstacle à l'adoption généralisée de la technologie IdO dans l'ensemble des forces armées (Zheng et Carter, 2015). Les hauts responsables ne comprennent pas suffisamment les nouvelles technologies et ils hésitent souvent à remplacer les pratiques habituelles, à adopter des solutions innovantes et à appliquer celles-ci à la résolution des défis traditionnels. De nombreux dirigeants militaires sont réticents à s'en remettre exclusivement à la technologie et à se fier à la communication entre machines. Alors que les applications IdO offrent la possibilité de faire des économies sur le long terme, les forces armées sont souvent peu enclines à investir en raison des coûts d'acquisition initiaux élevés et des récentes contraintes budgétaires. Par ailleurs, les processus d'acquisition militaires sont empreints d'une culture du secret et de la stratégie politique, démarche qui se heurte à la culture d'essais et erreurs relativement ouverte du secteur technologique privé (Zheng et Carter, 2015 ; AP-OTAN, 2017). Les sociétés technologiques privées sont aussi parfois moins désireuses de travailler avec le département de la Défense en raison des restrictions en matière de droits de la propriété intellectuelle et des contrôles des exportations.

B. LES RISQUES LIÉS AUX APPLICATIONS IdO DANS LES FORCES ARMÉES

38. Le recours à des produits et applications IdO dans les forces armées peut également présenter des risques de sécurité considérables, en particulier en matière de guerre électronique et de cyberguerre (Zheng et Carter, 2015). À mesure que les forces armées déploieront des produits et applications IdO, le nombre de points d'entrée pour les cyberattaquants ne fera que croître. Les menaces internes et les erreurs des utilisateurs sont également problématiques. Par ailleurs, comme la plupart des technologies IdO reposent sur la communication sans fil par fréquences radio, elles sont exposées au risque de guerre électronique, notamment au brouillage des signaux ou à la détection de la position des troupes.

39. Les risques de sécurité sont particulièrement répandus dans trois domaines : la sécurité des véhicules, les soins de santé et la chaîne d'approvisionnement (Campbell, 2016). Comme indiqué au préalable, les hackers ont la possibilité de prendre le contrôle de véhicules et de les diriger. Le système militaire de soins de santé présente aussi diverses vulnérabilités, notamment le contrôle à distance de dispositifs de santé et de sécurité, par exemple la manipulation des niveaux de dosage des pompes à perfusion et celle des moniteurs cardiaques et des défibrillateurs. Les chaînes d'approvisionnement militaires peuvent également être compromises étant donné que les produits IdO sont faits de composants fabriqués et assemblés dans différentes régions du monde. Qui plus est, il ne faut pas sous-estimer le risque que des adversaires puissent diffuser de fausses informations au sein des réseaux de l'Alliance pour perturber les processus et les opérations. Enfin, les nombreux dispositifs dont se sert le personnel militaire peuvent fournir de précieuses données aux attaquants. Par exemple, l'appareil photo d'un smartphone peut divulguer des informations sur la sécurité d'un avant-poste militaire.

C. LES FORCES ARMÉES ET LE SECTEUR COMMERCIAL

40. Comme indiqué dans la précédente section, le secteur privé stimule le développement et le déploiement des technologies IdO. Pour mieux exploiter les possibilités de l'IdO, les forces armées auront besoin d'adopter de nouvelles procédures en matière d'acquisitions et d'appels d'offres (Zheng et Carter, 2015 ; AP-OTAN, 2017). Il pourrait être judicieux de commencer par des domaines qu'il sera plus facile d'équiper avec des technologies IdO et pour lesquels des produits sont déjà disponibles sur le marché. Un domaine dans lequel les applications IdO ont un énorme potentiel d'économies est celui de l'amélioration de la gestion logistique, par exemple la maintenance conditionnelle et la gestion des flottes, des stocks, des bases ou de l'efficacité énergétique. En outre, afin de fournir une couverture internet dans des zones reculées, les forces armées pourraient investir dans des satellites commerciaux pour les communications militaires. Une autre technologie porteuse est celle des relais de communication de haute altitude, pour lesquels sont par exemple employés des véhicules aériens sans pilote opérant hors de portée des armes. Les forces armées pourraient également réfléchir à la possibilité de déployer des nanosatellites, pesant 1,33 kg (appelés « CubeSats »), pour créer des constellations de réseaux compatibles. Elles pourraient en outre s'attacher à mettre au point des systèmes complémentaires de sécurité pour les produits et applications commerciaux. Enfin, comme indiqué plus haut, des normes et protocoles communs sont nécessaires à l'adoption rapide et à l'intégration de l'IdO.

41. Les technologies IdO commerciales évoluent constamment et rapidement. Or, les processus d'acquisition militaires sont longs et complexes. Pour avoir accès à l'innovation, les forces armées doivent accroître leur collaboration avec le secteur privé (AP-OTAN, 2017). Les experts ont suggéré d'adopter une approche ascendante et d'organiser, dans la Silicon Valley, des salons ouverts à tous, consacrés à l'acquisition de technologies militaires afin de solliciter des solutions créatives aux problèmes que rencontrent les forces armées et de répondre à la nécessité d'attirer des innovateurs (Zheng et Carter, 2015). Il a également été suggéré de créer des bancs d'essai spécialisés dans le recensement et l'expérimentation des technologies dont les forces armées pourraient tirer parti, d'adopter les méthodes « Agiles » de développement logiciel qu'emploie le secteur privé et de confier la gestion de données à des prestataires commerciaux.

IV. LES INFRASTRUCTURES CRITIQUES ET L'IdO

42. Les installations et services associés aux infrastructures critiques sont des éléments ou des systèmes qui sont « indispensables au maintien des fonctions sociétales vitales » (Commission européenne, 2017). Si les infrastructures critiques subissent des perturbations, des dommages ou sont détruites, le fonctionnement de la société en pâtira considérablement (AP-OTAN, 2014). Les infrastructures critiques se rencontrent habituellement dans le secteur public, le secteur

énergétique, les transports, les services financiers, le secteur alimentaire et ceux de l'information et de la communication.

43. La numérisation des processus liés aux infrastructures critiques offre de nombreux avantages économiques aux opérateurs et aux consommateurs, mais elle ouvre également la porte à d'importants risques. Une cyberattaque bien menée contre une infrastructure critique, ou même une panne accidentelle, pourraient avoir des conséquences terribles, voire mortelles. Par exemple, l'arrêt intentionnel d'un service ou l'altération de données pourraient entraîner des coupures de courant et plonger des villes entières dans le noir, compromettre le fonctionnement des générateurs d'hôpitaux et les niveaux de toxicité de l'eau, et interrompre les communications, empêchant toute intervention d'urgence (Nadboy, non daté). Le lien entre protection des infrastructures critiques et l'IdO mérite donc que les décideurs politiques lui accordent une attention toute particulière.

44. À mesure qu'augmentera le nombre de produits, systèmes et services IdO, la cybermenace – déjà sérieuse – pesant sur les infrastructures critiques augmentera elle aussi considérablement. Les risques sont en hausse car a) les dispositifs connectés sont de plus en plus utilisés dans la gestion et l'entretien des infrastructures critiques et b) la probabilité que des infrastructures critiques entrent en contact avec des dispositifs et services connectés non sécurisés ira croissante. En un mot, l'étendue des cyberattaques et des cyberaccidents augmentera de façon sensible.

45. Si les fournisseurs d'infrastructures critiques ne parviennent pas à atteindre un niveau suffisant de cybersécurité, les conséquences seront bien plus importantes que dans d'autres secteurs. Ils sont de plus en plus connectés les uns aux autres et, surtout, ils passent tous par les principales infrastructures de télécommunications et les réseaux internet. On estime en effet que les opérateurs de services téléphoniques et informatiques sont les plus menacés car ils permettent à toutes les autres infrastructures critiques de fonctionner. Une attaque contre le réseau d'une infrastructure critique peut donc avoir de sérieuses répercussions sur les autres (*The Economist*, 2016). La cyberattaque menée contre l'Estonie en 2007, jusqu'alors inédite de par son ampleur et sa précision, en est un exemple significatif. Elle a été perpétrée par des cyberattaquants étrangers inconnus, juste après un différend entre l'Estonie et la Russie à propos du déplacement d'un monument commémoratif. Les institutions étatiques, mais aussi toutes les grandes banques commerciales, les entreprises de télécommunications, les organes de presse et des serveurs essentiels ont été ciblés. L'attaque n'a pas causé d'importants dommages matériels ou économiques, mais elle a poussé l'Estonie à réexaminer en profondeur la sécurité de ses services d'e-gouvernance et à renforcer les mesures de sécurité.

46. L'un des éléments fondamentaux de la plupart des infrastructures critiques – et donc une cible de premier ordre – est le système de contrôle industriel (ICS), qui comprend des systèmes de contrôle et d'acquisition de données (SCADA) et d'autres types de systèmes de contrôle chargés de suivre les processus et de contrôler les flux d'informations (Simon, 2017). Habituellement, un ICS est un système isolé physiquement, non vulnérable aux cyberattaques. De nos jours, toutefois, de plus en plus d'ICS sont connectés à internet, ce qui les rend plus vulnérables à divers types d'attaques (Simon, 2017). Dans bien des cas, les infrastructures critiques dépendent de systèmes ICS et SCADA anciens, dépourvus des contrôles de sécurité importants dont bénéficient les réseaux informatiques modernes.

47. Les cyberattaques passant par des objets connectés peuvent avoir des répercussions matérielles non négligeables. En 2008, des hackers non identifiés ont attaqué l'oléoduc Bakou-Tbilissi-Ceyhan, dont on pensait qu'il était l'un des plus sûrs au monde. Ils se sont infiltrés dans le système de contrôle de l'oléoduc via un réseau sans fil et ont manipulé les systèmes, provoquant une explosion (Simon, 2017). En 2015 et 2016, l'Ukraine a fait l'objet d'une série de cyberattaques contre ses infrastructures énergétiques et financières. Des hackers ont notamment

attaqué un réseau électrique situé dans l'ouest de l'Ukraine, privant d'électricité des milliers de personnes et causant, la première panne d'électricité officiellement due à un piratage (Polityuk, 2016).

48. Les cyberattaques visant les infrastructures critiques prennent diverses formes. Les menaces incluent des attaques utilisant l'électronique, les fréquences radio ou l'informatique pour atteindre les composants informatiques qui contrôlent les infrastructures critiques. Les attaquants peuvent déployer des programmes malveillants, pratiquer l'ingénierie sociale, surcharger les processeurs, exploiter les faiblesses du matériel et des logiciels, procéder à des attaques physiques et à des attaques électromagnétiques. Il peut notamment s'agir d'attaques par déni de service distribué, de trojans, d'injections SQL (*Structured Query Language*), d'attaques botnet et d'attaques *Zero-Day* (Castellon et Frinking, 2015). Dans la chaîne de la cybersécurité, les gens sont souvent le maillon le plus faible. C'est ainsi que le programme malveillant Stuxnet, qui a infecté la centrale nucléaire iranienne Natanz en 2010, a pu pénétrer le réseau fermé via des clés USB.

49. Les infrastructures critiques deviennent une cible courante pour des individus aussi bien que pour des adversaires cautionnés par des États (Simon, 2017). L'équipe du département de la Sécurité intérieure des États-Unis (DHS) chargée des interventions en cas de cyberurgence sur les systèmes de contrôle industriel est par exemple intervenue dans 295 cyberincidents liés aux infrastructures critiques durant l'exercice 2015, soit une augmentation de 20 % par rapport à l'année précédente. Dans le secteur manufacturier, qui est essentiel, le nombre a pratiquement doublé pour atteindre le record de 97 incidents, suivi de 46 incidents dans le secteur énergétique et 25 dans le secteur des systèmes de distribution de l'eau et de traitement des eaux usées. D'autres incidents ont été signalés dans les systèmes de transport, les sites gouvernementaux et les secteurs des soins de santé et des communications. Dans 37 % des cas, il s'agissait de campagnes d'harponnage (*spear phishing :* escroqueries qui leurrent leurs cibles pour qu'elles ouvrent un contenu malveillant) et dans 11 % des cas de scannage et d'exploration de réseaux (DHS, 2016a).

50. Les infrastructures critiques sont une cible de choix car leur perturbation a de sérieuses conséquences économiques, politiques et sociales (Simon, 2017). Les protagonistes de ces attaques sont notamment des hackers, des cybercriminels, des « hacktivistes », des concurrents, d'autres États et des amateurs (Castellon et Frinking, 2015). Les compétences requises pour mener de telles attaques se sont décentralisées et sont plus facilement accessibles.

51. Compte tenu de l'importance que revêt la sécurisation des infrastructures critiques, les gouvernements, les organisations internationales et le secteur privé travaillent assidûment au renforcement de leur sécurité. Des systèmes de sécurité de plus en plus efficaces sont mis au point, comme les signatures numériques, la cryptographie, la sécurité biométrique, les pare-feu, les systèmes de prévention des intrusions et les systèmes de contrôle d'accès (Simon, 2017).

52. Par ailleurs, la coopération entre les pouvoirs publics et le secteur industriel est indispensable pour faire progresser la cybersécurité et prévenir les cyberattaques. Il sera primordial de s'accorder sur des normes communes, des directives et des pratiques visant à garantir la protection des infrastructures critiques. Les éléments suivants seront également d'une grande importance : une sensibilisation accrue, des capacités avancées de détection des menaces, la formation et l'entraînement des employés ainsi qu'une meilleure résilience face à une attaque menée à bien ou en cas d'accident.

V. CONCLUSIONS

53. L'édition de juillet 2016 du baromètre de Vodafone sur l'IdO dévoile quelques chiffres stupéfiants. Parmi les entreprises qui ont répondu au questionnaire, 28 % déploient déjà des technologies IdO et pas moins de 76 % estiment que l'IdO sera « essentiel à la réussite future de toute organisation dans leur secteur » (Vodafone, 2016). Comme l'affirme Erik Brenneis, directeur IdO chez Vodafone, « ce qui compte maintenant, ce n'est pas de savoir si une entreprise va adopter ou non l'IdO mais comment » (Vodafone, 2016). En résumé, l'adoption généralisée des technologies IdO dans le secteur commercial aura lieu tôt ou tard. Des pouvoirs publics innovants, aux échelons locaux, régionaux et nationaux, ont déjà de nombreux projets en cours ou en préparation. Les forces armées avancées commencent tout doucement à prendre conscience elles aussi des avantages des technologies IdO.

54. Le présent rapport a toutefois également montré les nombreux défis qu'engendre le déploiement étendu de l'IdO. Les décideurs politiques, notamment les parlementaires nationaux, doivent commencer à façonner activement un environnement IdO qui reste ouvert, innovant et sûr. Il faut trouver le bon équilibre. Cependant, ils doivent garder à l'esprit quelques principes généraux pour toute politique relative à l'IdO :

- Les cadres réglementaires et autres politiques cherchant à façonner l'environnement IdO doivent trouver le bon équilibre entre rendre l'IdO fiable, sûr et privé et suffisamment inciter les entreprises à investir dans ces technologies.

- Il faut promouvoir énergiquement la normalisation des technologies IdO.

- Le financement de la recherche et du développement concernant l'IdO doit être suffisant pour permettre l'adoption de l'IdO à grande échelle.

- Les pouvoirs publics et en particulier les forces armées doivent revoir la manière dont ils s'adaptent aux technologies émergentes compte tenu du fait que le secteur privé stimule le développement de nombreuses technologies IdO. En outre, ils doivent se préparer à réaliser des investissements à long terme pour récolter à l'avenir tous les bénéfices de l'IdO.

- Les pouvoirs publics doivent également redoubler d'efforts en matière de cyberdéfense, de sécurité et de protection des infrastructures critiques vu le nombre croissant de produits et services IdO qui sont déployés.

BIBLIOGRAPHIE SÉLECTIVE

(Pour des informations plus exhaustives sur les ressources utilisées, veuillez-vous adresser au directeur de la commission)

Agawu, Emefa Addo and Laura Bate, *Cybersecurity Awareness Month... Now with Added Facts!*, New America, 2016

Al-Fuhaqa, Ala, et al., "Internet of Things: A Survey on Enabling technologies, Protocols, and Applications", *IEEE Communication Surveys & Tutorials*, vol. 17, no 4, 2015

AP-OTAN, *Préserver l'avance technologique de l'OTAN : adaptation stratégique et R&D en matière de défense* [174 STC 17 F], rapport général 2017 de la STC

AP-OTAN, *rapport de mission de la visite en Italie*, du 3 au 7 octobre 2016 [035 STCTTS 17 F]

AP-OTAN, *rapport de mission de la visite dans le Connecticut et New York, États-Unis*, du 1er au 4 juin 2015 [151 STC 15 F]

AP-OTAN, *Cyberespace et sécurité euro-atlantique* [209 STC 14 F bis], rapport spécial de la STC, 2014

AP-OTAN, *L'avenir des capacités alliées de renseignement, surveillance et reconnaissance aéroportées*, [174 STC 16 F bis] rapport général de la STC, 2016

AP-OTAN, *Nouvelles idées pour les armées alliés en matière d'énergie : responsabiliser, réduire la demande, sécuriser l'approvisionnement* [159 STCEES 13 F bis], rapport de la STCEES, 2013

Baily, Martin Neil and James M. Manyika, *Reassessing the Internet of Things*, Project Syndicate, 2015

BBC News, *German Parents Told to Destroy Cayla Dolls over Hacking Fears*, 17 février 2017

Bonomi, Rodolfo and Preethi Natarajan, "Fog Computing: A Platform for Internet of Things and Analytics", in: Bessis, N and C. Dobre (eds.), *Big Data and Internet of Things: A Roadmap for Smart Environments*, Studies in Computational Intelligence 546, Switzerland: Springer International Publishing, 2014

Borgia, Eleonora, "The Internet of Things Vision: Key Features, Applications and Open Issues", *Computer Communications*, vol. 54, 2014

Calore, Michael, *Worried the CIA Hacked Your Samsung TV? Here's How to Tell*, 7 mars 2017

Campbell, Shawn, *"Military Security in the Age of the Internet of Things"*, *Signal*, 1 février 2016,

Castellon, Nicolas and Erik Frinking, *Securing Critical Infrastructures in the Netherlands: Towards a National Testbed*, The Hague Security Delta, 2015

Cisco, *VNI Complete Forecast 2016*, 2016

Commission européenne, *Critical Infrastructure*, 2017

Commission européenne / AITI, *Report on Workshop on Security & Privacy in IoT*, 2017

CSO (Bureau de soutien à la collaboration), *Military Applications of Internet of Things (IST-147)*, undated

DHS, *NCCIC/ICS-CERT Year in Review: FY 2015*, 2016.

DHS, *Strategic Principles for Securing the Internet of Things (IoT): Version 1.0*, 2016

Evans, Dave, *IoT Threat Environment*, Cisco, 2015,

Fischer, Eric A., *The Internet of Things: Frequently Asked Questions*, Washington DC: Congressional Research Service, 2015

Folk, Chris et al., *The Security Implications of the Internet of Things*, AFCEA International Cyber Committee, 2015

Gartner, *Internet of Things*, 2017

Greengaard, Samuel, *The Internet of Things*, Cambridge: The MIT Press, 2015.

Hern, Alex and Agencies, "Wi-Fi on Planes Opens Door to In-Flight Hacking, Warns US Watchdog", *The Guardian*, 15 avril 2015

Howard, Philip, *Ideas to Retire: A Closed-Platform Internet of Things*, Brookings Institution, 2016

IBM, *Device Democracy: Saving the Future of the Internet of Things*, IBM Institute for Business Value, 2015

Infineon, NXP, ST and ENISA, *Common Position on Cybersecurity*, décembre 2016

Lewis, James Andrew, *Managing Risk for the Internet of Things*, Center for Strategic and International Studies, 2016
Lindsay, Greg, Beau Woods and Joshua Corman, *Smart Homes and the Internet of Things*, Atlantic Council Issue Brief, 2016,
Michels, Dave, "The Future of IoT: Where It's Heading, What to Expect", *Network World*, 30 mai 2017
Nadboy, Michelle, *Industrial Internet Of Things (IoT): Identifying The Vulnerabilities Of Field Devices*, Water Online, undated
OTAN, *Communiqué du Sommet de Varsovie*, 9 juillet 2016
Polityuk, Pavel, Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid, Reuters, 20 décembre 2016,
Seffers, George I., *"Defense Department Awakens to Internet of Things"*, *Signal*, 1 janvier 2015
Simon, Tobby, *Critical Infrastructure and the Internet of Things*, Global Commission on Internet Governance, Paper Series, no 46, 2017
Stupp, Catherina, *Commission Plans Cybersecurity Rules for Internet-Connected Machines*, *Euractiv*, 5 octobre 2016
TechTerms, *Internet of Things*, 2015
The Economist, *Securing the Digital City: Cyber-Threats and Responses*, 2016
The Economist, *The Myth of Cyber-Security*, 8 avril 2017a
The Economist, *Why Everything is Hackable*, 8 avril 2017b
Tripwire, Enterprise of Things, 2015,
Vanian, Jonathan, "Why Data Is the New Oil", *Fortune*, 1er juillet 2016
Vermesan, Ovidiu et al., "Internet of Things beyond the Hype: Research, Innovation and Deployment", in: Vermesan, Ovidiu and Peter Friess (eds.), *Internet of Things – From Research and Innovation to Market Deployment*, European Research Cluster on the Internet of Things (IERC), Gistrup: River Publishers, 2015
Vodafone, *Vodafone IoT Barometer 2016*, 2016
W3C, *W3C Semantic Web Activity*, 2013
Want, Roy, Bill N. Schmitt and Scott Jenson, "Enabling the Internet of Things", *Computer*, vol. 48, no. 1, 2015
Wind, *The Internet of Things for Defense*, 2015
Zetter, Kim, "Medical Devices that are Vulnerable to Life-Threatening Hacks", *Wired*, 24 novembre 2015
Zheng, Denise E., Carter, William A., *"Leveraging the Internet of Things for a More Efficient and Effective Military"*, Center for Strategic and International Studies, 2015